文章编号:1673-1522(2019)02-0228-06 DOI: 10.7682/j.issn.1673-1522.2019.02.009

某型导弹技术准备人因安全性分析

陆巍巍,徐 涛,韩建立

(海军航空大学,山东 烟台 264001)

摘 要:某型导弹技术准备过程具有涉及操作人员多,人员间以及人与设备之间交互多的特点,系统级的安全性分析结果表明,人为致因因素是导致安全问题的重要因素。因此,文章研究了一种基于行为模型的人因安全性分析方法(Extended STPA with Behaviour Model,BME-STPA)。BME-STPA方法基于行为模型思想,对STPA控制器模型进行扩展,使其更加适用于人为致因因素分析,解决了STPA方法对人因安全性分析针对性不强的问题,具有较强的可操作性。以导弹加注过程中溢出灌增压作为BME-STPA的应用案例,证明了该方法的实用性和有效性。

关键词:导弹技术准备;安全性分析;安全性分析系统;加注

中图分类号:TP301.6 **文献标志码:**A

在某型导弹技术准备过程中,涉及人员、岗位多,协作、交互多,对装、设备的操作也多,具备复杂系统的典型特征[1];操作人员的精力主要集中在协调控制不同系统设备,因而承担了更多压力,这导致产生人为错误的可能性较高。

鉴于人因在系统安全性中的重要性,本文基于行为模型的概念,对STPA(系统理论过程分析方法)的人员控制器模型进行扩展[2],构建了一种基于行为模型的人因安全性分析方法(Extended STPA with Behaviour Model,BME-STPA),该方法将人的行为纳入系统运行过程中,实现人因分析中致因因素的定位,确定不安全行为在特定工作环境中出现的原因。

1 BME-STPA人因安全性分析方法

1.1 基于STPA的分析过程

Nancy Leveson提出的STAMP模型,目的是查找更多类型的事故致因因素,包括人为差错、组织结构、设计缺陷以及非故障组件之间不良交互作用等[3]。STAMP模型将复杂系统当成含有多个层次的分层结构,用以揭示上层对下层的约束和下层向上层的反馈信息,并构建控制关系模型[4]。

STPA是建立在STAMP模型基础上的安全性分析方法,它通过构建由作动器、控制过程和传感器等构成的反馈控制回路,分析输入、输出信号在性能、时间或逻辑上的不合理情况,识别存在的不安全控制行为并构建事故场景,其通用控制器模型如图1所示,其中包含人员控制器和自动控制器[5]。

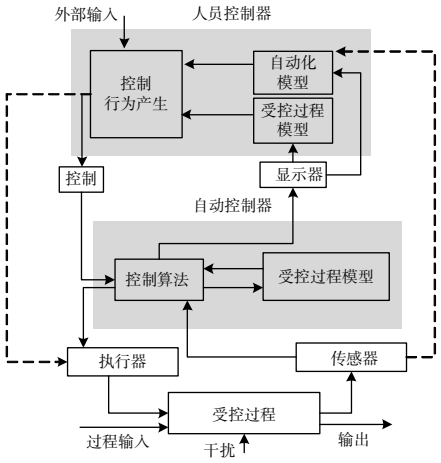

图1 STPA的通用控制器模型

Fig.1 Common controller model of STPA

可以看到,人员控制器的过程模型与自动控制相比,除了包括受控过程的模型,还包括自动控制系统模型,这2种过程模型用来生成动态的人员控制行为,从而主导整个操作流程[6]。来自人员控制器控制过程和自动控制器的反馈信息(以视觉、听觉、触觉等形式)直接或间接(通过人机接口)输入至人员控制器,从而对控制行为的生成产生影响。控制行为产生后,会通过人员控制器的控制机构送至自动控制器,或者直接送至执行器,进而对受控过程产生影响。

1.2 基于行为模型的人员控制器模型改进

各种行为模型主要是对人的信息处理过程、形成决策和人与设备交互过程的描述。而人因安全性分析不但需要知道人是怎么思考的,还要知道他们如何

收稿日期: 2019-01-24; **修回日期:** 2019-03-22

作者简介: 陆巍巍(1983-),男,讲师,硕士。

以及为何会打破系统的安全约束[7]。

因此，在STPA的安全性分析中，须将人的思维模型与基于控制理论的安全分析技术有机结合起来。这种模型不需要过多地涉及人的行为模式的细节问题，应当主要关注整个系统中操作人员与其他组件的互动[8]。本文基于此，给出了一种适用于STPA的行为模型架构如图2所示，并构建了一种基于STPA的人因安全分析方法：BME-STPA方法。对比图1和图2可以看到不同之处在于：

1）控制器模型由“态势感知”、“态势理解”、“行为决策”、“行为实施”等组建的新行为模型取代了原来的“过程模型－控制算法”模型。

2）外源因素（指非控制系统本征因素，即传感器、控制器、执行器之外的因素）取代了环境输入和规程输入。

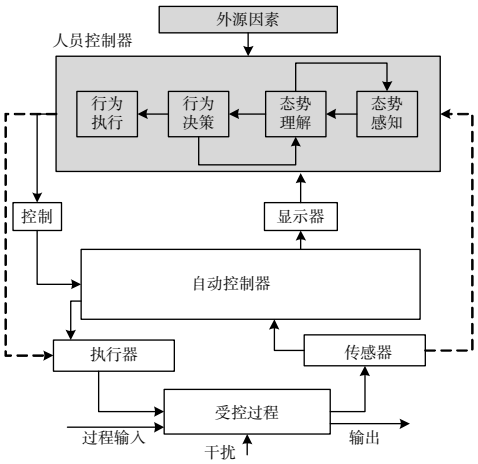

图2 改进的控制器模型

Fig.2 Improved controller model

1.3 改进的控制器模型

1）态势感知。反馈信息到达控制器后，在被控制行为产生影响前，首先会经过“感知”模型的处理。操作人员能够正确处理和理解来自人机接口、传感器和自身感觉系统的反馈信息，是做出正确的反应和操作的前提。这里的“正确处理和理解”指的是操作人员对反馈信息的理解没有出现偏差和误解[9]。在STPA中，如果反馈信息没有被正确的接受和理解，操作人员可能会因此做出错误的控制行为，进而引发事故。

2）态势理解。反馈信息被控制模型感知后，会触发操作人员对当前态势信息模型的产生或者刷新，这一点与STPA控制器模型相同。态势理解是行为决策的决策依据，其输入是态势感知模块产生的态势信息，态势理解模块将对输入信息进行再处理，内化形成操作人员对态势信息认知的表示[10]。在态势感知和态势理解之间还存在一个反向的箭头，表明态势理解有时会进一步要求态势感知阶段更新信息，或输入更多的信息，以满足操作人员对当前态势掌握的需求。

3）行为决策。行为决策模型会根据态势信息来产生控制行为。在行为决策与态势理解之间也存在着交互。行为决策需要态势感知的支持，而当人员进行决策时，如果发现当前获取的态势无法为控制行为的选择提供足够的信息支持，则会要求通过态势感知和态势理解进一步获取更全面的态势信息[11]。

4）行为执行。决策模型确定好控制行为后，操作人员须要将其付诸实施。如果操作工具设计有缺陷（比如用户友好性差），操作人员就可能无法即时做出动作，或做出错误的动作，从而在某种条件下导致事故的发生[12]。与基本的STPA人员控制器类似，控制行为实施后，会通过人员控制器的控制机构送至自动化控制器，或者直接送至执行器，进而对受控过程产生影响。

2 人因安全性分析用例—加注

本文以某型导弹技术准备中加注过程的部分操作为分析对象，介绍BME-STPA方法的应用过程。

2.1 加注操作流程

加注操作涉及的人员包括：0号手——负责指挥协调，下达操作指挥口令，并负责工作把关，检查各号手的工作；1号手——操作控制台，观察仪表显示，读数；2号手——加注罐有关操作；3号手——溢出罐有关操作；4号手 —— 对接和拆除加泄连接器；5号手——报告和记录有关数值。另有消防、救护、抢险人员在现场保障[13]。工作流程如图3所示。

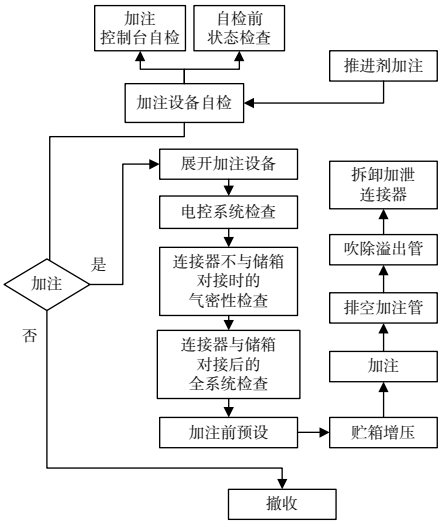

图3 推进剂加注流程图

Fig.3 Flow chart of propellant filling

2.2 事故场景、典型事故类型与安全约束分析

1)事故场景。对照危险严重性等级标准[14],划分可能的事故等级:Ⅰ-燃料泄漏导致的人员中毒;Ⅱ-操作不当(搬运设备)导致的人员受伤;Ⅲ-操作不当导致的设备损伤;Ⅳ-轻于Ⅲ的损伤。

2)典型事故类型。加注过程可能导致燃料泄漏的典型事故类型如表1所示(默认加注前准备工作检查完毕,当前状态正常)。

3)系统安全约束分析。根据发现的系统危险,给出对应的安全约束如表2所示,这也是识别不安全控制行为的依据。

表1 加注过程典型事故类型

Tab.1 Typical accidents during the fueling

序号	步骤	系统危险	可导致事故
1	连接器对接	加注口连接器未连好下溢口连接器未连好 上溢口连接器未连好	Ⅰ
2	全系统气检及氮气置换	未做好气密性检查	Ⅰ
3	加注罐溢出罐就位	搬运动作不规范	Ⅱ(人员受伤)、Ⅲ(损坏台秤)
4	加注量设定	设定值超过限定值	Ⅰ
5	溢出罐增压	增压过小	Ⅰ(管路冲击载荷大)
6	加注罐增压	增压过大	Ⅰ(管路冲击载荷大)
7	加注	气路操作失误增压 加注罐意外增压	Ⅰ(连接点可能泄露)
8	加注罐泄压	连接器未连好	Ⅰ
9	排空加注管	连接器未连好	Ⅰ
10	吹除加注管、溢出管	连接器未连好	Ⅰ
11	拆连接器	动作不规范有残留燃料	Ⅰ、Ⅲ、Ⅳ
12	撤收	动作不规范	Ⅲ、Ⅳ

表2 加注过程系统级安全约束

Tab.2 System security constraints during the fueling

系统危险		安全约束	
H1	加注口连接器未连好	SC1	必须将加注口连接器连接好
H2	下溢口连接器未连好	SC2	必须将下溢口连接器连接好
H3	上溢口连接器未连好	SC3	必须将上溢口连接器连接好
H4	气检未做气密性检查	SC4	必须做好全系统气密性检查
H5	加注罐溢出罐搬运动作不规范	SC5	必须严格按照操作规范搬运
H6	加注量设定值超限	SC6	加注量的设定必须准确无误
H7	溢出罐增压过小	SC7	溢出罐增压必须及时准确
H8	加注罐增压过大	SC8	加注罐增压必须及时准确

2.3 安全控制结构

本文选取溢出罐增压操作作为安全分析的对象。溢出罐增压过程的安全控制结构如图4所示,涉及的操作人员包括0号手(指挥)、1号手(加注台操作)、3号手(溢出罐操作);设备包括溢出罐和加注台,其中溢出罐是受控对象,加注台兼具控制器和传感器的功能。

溢出罐增压操作以3号手为核心,涉及与0号手、1号手,以及与控制器和传感器的交联,0号手向1号手、3号手下达增压指令后,3号手通过观察压力表,感知溢出罐增压状态,当溢出罐增压满足要求时,3号手向0号手报告,0号手向1号手下达"S2A置'中'位"指令,1号手根据指示灯显示完成"S2A置'中'位"后,向1号手报告。3号手继续观察溢出罐压力情况,如无异常,溢出罐增压操作结束。

由此可以看出,在溢出罐增压操作过程中,人员的作用就非常重要,人因贯穿在整个操作过程中,在设备正常的情况下,人因是导致不安全控制行为的主要因素。

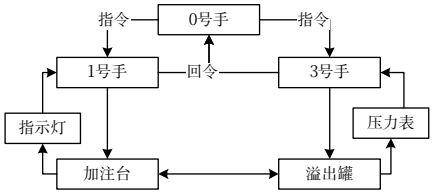

图4 溢出罐增压过程安全控制结构

Fig.4 Safety control structure during overflow tank supercharging

2.4 溢出罐增压中基于BME-STPA的人因分析

2.4.1 不安全控制行为(UCA)分析

UCA产生的4种情形为[15]:

情形1:安全约束需要的控制行为没有施加;

情形2:施加的错误控制行为导致安全危害;

情形3:安全控制行为提供的过早、过晚或者次序错误;

情形4：控制行为过早或者过晚的停止。

据此分别对溢出罐增压涉及的3名操作人员进行UCA分析，分析结果如表3所示。

表格的第1列为涉及的操作人员，第2列为与安全约束SC7相关的控制行为，第3~6列为对应的UCA。以UCA3-2为例，3表示3号手，2表示当前号手UCA的序号。

表3 加注过程系统级安全约束

Tab.3 System security constraints during the fueling

操作人员	控制行为	情形1	情形2	情形3	情形4
3号手	报告压力	–	UCA3-1： 报告了错误值	UCA3-2：未及时报告压力值 UCA3-3：未按流程依次报告压力变化	–
1号手	S2A置“中”位	UCA1-1：未将S2A置“中”位	UCA1-2： 将S2A置其他位	UCA1-3：未及时将S2A置“中”位	–
0号手	下达“报告压力”指令	UCA0-1：未下达“报告压力”指令	UCA0-2： 下达了错误指令	UCA0-3：未及时下达指令	–
0号手	下达“S2A置“中”位”指令	UCA0-5：未下达S2A置“中”指令	UCA0-6： 下达了错误指令	UCA0-7：未及时下达指令	–

2.4.2 人因致因因素分析

完成UCA分析后，即可以每一个UCA或者多个UCA为出发点，进行人因致因因素分析。下面以UCA3-1、UCA3-2、UCA3-3为例，对3号手进行人为致因因素分析，3号手报告压力时的行为模型如图5所示。进行安全分析时，在考虑外源因素影响下，按照行为执行、行为决策、态势理解、态势感知的顺序进行[16]。

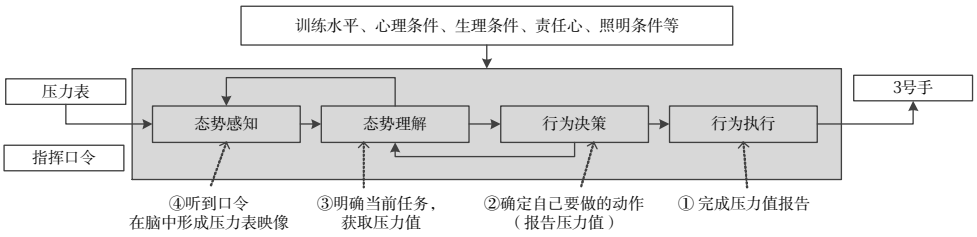

图5 行为模型

Fig.5 Behavior model

1）行为执行。首先，假定3号手已经读出了压力值，但是在报告时出现了失误，报告了错误的数字。此时，考虑各种可能的外源因素，可以得出以下致因因素[17]：① 人体工学因素：由于心情紧张报错数字；由于注意力不集中报错数字；由于疲劳报错数字。② 知识因素：由于发音不标准导致报出了会被误解的数字；由于工作经验和知识面不足，报出了不准确的数字。

2）行为决策。接下来分析为何号手会做出错误的行为选择。在报告压力这一动作中，3号手的选择空间为：报告或者不报告当前数值。行为决策失误的根源首先可能来自错误的态势理解，这一点将在“态势理解”中进行分析。在态势理解正确的前提下，可能的致因因素为：① 号手急于完成当前操作，导致没有依次报告压力变化；② 号手对规程的遵从意识不强，导致没有及时报告压力值；③ 号手训练水平不够，没有形成相应的操作记忆，导致没有及时或者没有依次报告压力；④ 号手由于情绪紧张或者注意力不集中等原因，导致没有及时或者没有依次报告压力。

3）态势理解。根据前文所述，态势信息可以分为受控过程状态、受控过程行为和操作环境3个部分，可能存在的致因因素为：① 对受控过程状态的理解错误：由于注意力不集中，训练水平不够等原因，号手对自己当前号位认识错误（训练中每个受训人员往往会轮流担任不同的操作号手）；号手对压力表数值的判读错误：对压力表不熟悉导致读数错误；将当前压力表的指示默认与其他仪表混淆，导致读数错误等；由于注意力不集中，训练水平不够等原因，号手对指挥号手（0号手）下达的口令记忆错误。② 对受控过程行为的理解错误：由于训练水平不够等原因，号手对当前应当执行的任务存在误解。例如，不确定自己应当报告哪些数值；由于对压力变化的误判，导致压力报告的时机错误。③ 对任务环境的理解错误：对任

务的严肃性和违规操作后果的严重性没有正确认识；认为其他号手的工作能够弥补自己的过失。

4)态势感知。来自传感器、环境和其他操作人员的信息汇集到操作人员，但这些信息未能全部被操作人员接收到或者正确理解，态势感知中可能存在的致因因素主要有[18]：① 设备或者系统缺陷导致的错误：3号手站位距离压力表太远，导致读数错误；压力表表盘受污导致读数错误；0号手与3号手之间距离太远，导致3号手不能听清口令。② 外源因素导致的错误：照明条件不好导致读数错误；环境噪音过大导致号手不能听清口令；号手由于伤病等原因导致听力或者视力受损。

2.4.3 分析结果评价

针对“溢出灌增压”这一操作，采用BME-STPA方法进行了人为致因因素分析。分析过程以行为模型为依据，分别从行为执行、行为决策、态势理解、态势感知4个阶段入手，并且在每个阶段涵盖了外源因素导致的致因因素。

与STPA方法相比，由于BME-STPA对人因分析更具针对性，给出的分析指南也更加详尽和全面，因此能定位出更为准确、全面和深层次的致因因素。例如，在分析态势理解中的致因因素时，BME-STPA方法分别从“受控过程状态”“对受控过程行为”“任务环境”3个方面，结合操作人员的心理条件、训练水平等外源因素，得出8条致因因素，这是STPA方法难以做到的。

3 结束语

本文根据STAMP理论，研究了一种基于STPA的人因安全性分析方法BME-STPA方法：用简洁的行为模型替代STPA的控制器模型，并将外源因素作为分析方法的重要因素之一，用人的行为模型替代STPA的控制器模型，构建了基于行为模型的BME-STPA方法；以“态势感知”、“态势理解”、“行为决策”、“行为实施”和“外源因素”5个基本要素为基础，给出了人为致因因素的分析指南，解决了STPA方法对人因安全性分析针对性不强的问题；最后，以末修加注中的溢出罐增压操作为分析用例，证明了BME-STPA方法的实用性和有效性。

参考文献：

[1] 霍阳. 战略导弹贮存安全性模型与可靠性备件率研究[D]. 西安：西安电子科技大学，2014.
HUO YANG. The research of security model and reliability rate of spare parts in strategic missile storage[D]. Xi'an：Xidian University，2014.（in Chinese）

[2] LEVESON N G. Engineering a safety world：systems thinking applied to safety[M]. Boston：MIT Press，2012：15-17.

[3] LEVESON N G. A new approach to hazard analysis for complex systems[C]//International Conference of the System Safety Society. Ottawa，Canada，2003：20-30.

[4] LEVESON N G. A new accident model for engineering safer system[J]. Safety Science，2004，42(4)：203-210.

[5] LEVESON N G. A system model of accidents[C]//International Systems Safety Society. Unionville，USA，2002：15-40.

[6] FLMING C，PLACKE M，LEVESON N. STPA analysis of next gen interval management components：ground interval management and flight deck interval management[R]. Boston：MIT，2013：17-20.

[7] 高远，樊运晓，王鹏，等. 基于STPA的特种设备安全违规致因模型研究[J]. 工业安全与环保，2017，43(5)：49-52.
GAO YUAN，FAN YUNXIAO，WANG PENG，et al. Research on the safety violation cause model for special equipment based on STPA[J]. Industrial Safety and Environmental Protection，2017，43(5)：49-52.（in Chinese）

[8] BAO YINGKAI，TANG JUNXI，WANG YIFEI，et al. Quantification of human error probability in power system based on SLIM[C]//IEEE PES Asia-Pacific Power and Energy Engineering Conference. Kowloon，Hong Kong：IEEE，2014：7-10.

[9] 吴志强. 面向服务质量保障的态势感知技术研究[D]. 重庆：重庆大学，2015.
WU ZHIQIANG. Research of situation awareness technology oriented service quality guarantee[D]. Chongqing：Chongqing University，2015.（in Chinese）

[10] 廖鹰，易卓，胡晓峰. 基于深度学习的初级战场态势理解研究[J]. 指挥与控制学报，2017，3(1)：67-70.
LIAO YING，YI ZHUO，HU XIAOFENG. Battlefields situation elementary comprehension based on deep learing[J]. Journal of Command and Control，2017，3(1)：67-70.（in Chinese）

[11] 张东俊，张涛，王石. 基于潜艇声探测能力预测的感知行为决策方法[J]. 声学技术，2018，37(4)：309-312.
ZHANG DONGJUN，ZHANG TAO，WANG SHI. A perceptual behavior decision method based on acoustic detectability prediction of submarine[J]. Technical Acous-

tics,2018,37(4):309-312.(in Chinese)

[12] 李鹏程,陈国华,张力,等.人因可靠性分析技术的研究进展与发展趋势[J].原子能科学技术,2011,45(3):329-335.
LI PENGCHENG, CHEN GUOHUA, ZHANG LI, et al. Research review and development trends of human reliability analysis techniques[J]. Atomic Energy Science and Technology,2011,45(3):329-335.(in Chinese)

[13] 周红梅,陆巍巍,王斌.战略导弹火工品与测试[M].烟台:海军航空工程学院,2015.
ZHOU HONGMEI, LU WEIWEI, WANG BIN. The eed testing of the strategic missile[M]. Yantai: Naval Aeronautical Engineering Academy,2015.(in Chinese)

[14] 中国航空综合技术研究所.系统安全性通用大纲:GJB 900A-2012[S].北京:航空航天工业部,1991:1-36.
CHINA AERO POLYTECHNOLOGY ESTABLISHMENT. General program the system safety: GJB 900A-2012[S]. Beijing: Ministry of Aerospace Industry, 1991: 1-36.(in Chinese)

[15] 田思明,史振中.武器装备危险源辨识与风险分析方法研究[J].中国安全生产科学技术,2007,3(2):111-113.
TIAN SIMING, SHI ZHENZHONG. The research on distinguishing the hazard source of weapon equipment and the methods of risk controlling[J]. Journal of Safety Science and Technology,2007,3(2):111-113.(in Chinese)

[16] FERJENCIK M. An itegrated approach to the analysis of incident causes[J]. Safety Science, 2011, 49(6): 1133-1146.

[17] ISHIMATSU T, LEVESON N G, THOMAS J P, et al. Hazard analysis of complex spacecraft using systems-theoretic process analysis[J]. Journal of Spacecraft and Rockets,2014,51(2):509-520.

[18] SALMON P M, CORNELISSEN M, TROTTER M J. Systems-based accident analysis methods: a comparison of accimap, HFACS, and STAMP[J]. Safety Science, 2012,50(4):1160-1167.

Personnel Safety Analysis of the Preparing Technology of a Certain Type of Missile

LU Weiwei, XU Tao, HAN Jianli

(Naval Aviation University, Yantai Shandong 264001, China)

Abstract: A certain type of missile technology preparation process has many features. It involves many personnel, and many interaction between personnel and equipments. The safety analysis results from system level shows that the human factors are important factors leading to security issues. Therefore, in this paper an extended STPA with Behavior Model, (BME-STPA) was invented. The BME-STPA method was based on the behavior model idea, and the STPA controller model was extended to make it more suitable for the analysis of cause factor analysis. The problem that STPA was not targeted to human safety analysis and had very strong maneuverability. The application case of BME-STPA was presented in this paper, which proved the practicability and effectiveness of this method.

Key words: missile technology preparation; security analysis; security analysis system; fueling