

导弹系统安全性分析中的引发事件鉴别方法*

王冬¹, 蒋平², 程志君², 郭波²
(1. 军事经济学院 装备经济管理系, 湖北 武汉 430035;
2. 国防科技大学 信息系统与管理学院, 湖南 长沙 410073)

摘要:引发事件鉴别是基于事故机理安全性分析的首要任务。鉴别结果是否全面、完整直接影响最终分析结果的有效性。导弹系统安全风险涉及面广、影响因素多,需要系统的可操作方法来指导引发事件的鉴别工作。针对导弹工作特点,提出考虑导弹任务剖面,运用主逻辑图对导弹进行系统性的层次化描述,对引发事件进行整理和归纳。将危险与可操作性分析引入导弹系统安全性分析中进行引发事件鉴别,结合故障模式影响分析,支持对单一故障类和参数异常类引发事件的鉴别。结果表明,所提框架为解决导弹系统安全性分析中引发事件鉴别的系统性完整性提供了可行的思路。

关键词:导弹安全性;引发事件鉴别;故障模式影响分析;危险与可操作性分析

中图分类号:E917 **文献标志码:**A **文章编号:**1001-2486(2017)01-115-05

Initiating event identification method for systematic missile safety analysis

WANG Dong¹, JIANG Ping², CHENG Zhijun², GUO Bo²

(1. Department of Equipment Economic Management, Military Economics Academy, Wuhan 430035, China;
2. College of Information System and Management, National University of Defense Technology, Changsha 410073, China)

Abstract: Initiating event identification is the primary task in safety analysis based on accident mechanism. The comprehensiveness and the completion of identification have a direct effect on final results. Due to the width of related facets and multitude of impact factors, an operable systematic method is required to guide the identification process. Aiming at the properties of missile weapon, the MLD (master logic diagram) was proposed to provide a systematic hierarchical description of missiles. It was also utilized to collect and classify identified initiating events. For the first time, the HAZOP (hazard and operability analysis) was introduced in missile system safety analysis to identify the initiating events. Combined with FMEA (failure modes and effects analysis), this framework provided support for the identification of initiating events which were caused by single failure or parameter abnormality. Results show that the proposed framework provides a practical way to ensure the comprehensiveness of initiating event identification for system safety analysis of missile weapon.

Key words: missile safety; initiating event identification; failure modes and effects analysis; hazard and operability studies

当前,基于导弹事故机理的安全性分析方法已得到广泛认可,其中概率风险评价(Probabilistic Risk Analysis, PRA)方法已广泛应用于核工业^[1]、航天工业^[2]和民用工程^[3],为导弹的系统安全性分析提供了借鉴和参考。一般地,事故机理如图1^[4]所示。

国内导弹安全性分析工作主要关注特定的危险源。例如,王涛等^[5]对导弹战斗部炸药部件安全性进行分析,分别建立了炸药部件在运输、贮存和使用过程中发生爆炸事故的故障树,定性地分析各种危险因素对炸药部件安全性的影响程度。

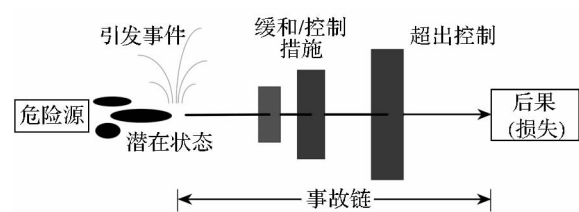


图1 事故机理
Fig. 1 Accident mechanism

陈广南^[6]对固体火箭发动机运输、贮存、维护及使用等过程中可能遇到的各种激励作用进行了研究,给出了相关安全性理论分析和计算方法。但

* 收稿日期:2015-08-11
基金项目:国家自然科学基金资助项目(71371182,61573370)
作者简介:王冬(1989—),男,重庆合川人,博士研究生,E-mail:wonderfulwinter@sina.com;
蒋平(通信作者),男,讲师,博士,E-mail:jiangping@nudt.edu.cn

与此同时,GJB900-90《系统安全性通用大纲》^[7]所要求的程序和技术方法在导弹安全性分析实践中并没有得到彻底的贯彻。对引发事件的鉴别通常单纯依靠历史经验而缺乏系统性的方法。

一方面,很大一部分导弹事故由故障导致,故障引发的安全风险是系统最常见的风险^[8]。另一方面,导弹本身具有“长期贮存,一次使用”的特点。由于导弹系统内部复杂的交互关系,不符合要求的输出很可能影响其他分系统,进而影响整个导弹系统,导致事故发生。基于此,本文提出建立利用主逻辑图(Master Logic Diagram, MLD)对导弹进行系统性的层次化描述,对引发事件进行整理和归纳。首次将过程工业中常用的危险与可操作性分析(HAZard and OPerability Studies, HAZOP Studies)引入到导弹武器装备的安全性分析中,结合故障模式影响分析(Failure Modes and Effects Analysis, FMEA),打破了传统方法只关注具体设备和特定危险源而忽略设备间交互关系的局限。由此,更加全面系统地进行引发事件的鉴别,进而得到更为完整的引发事件列表。

1 引发事件鉴别方法的综合运用

1.1 方法简介

MLD 是一个对风险事故发生必要条件进行分级描述的层次结构图,其广泛应用于概率风险评价^[2]中。从系统任务或一个不希望出现的重大事故出发,自上而下建立从任务到完成各个任务所需功能再到功能所对应的分系统、设备的结构层次,为进一步的鉴别引发事件提供系统化的分级描述。

FMEA 对系统进行分解,对各组成部分、元素进行分析。采用此分析方法,可以找出系统中各组成部分及元素可能发生的故障及其类型。实施 FMEA 的主要工作是给出可能的故障类型结论和根据分析结果说明故障原因类型和等级,形成故障模式及影响分析表。

HAZOP 分析最早由英国帝国化学工业(Imperial Chemical Industries, ICI)首先在 20 世纪 60 年代开发应用。它的基本思想是任何偏离预先设定操作条件值的现象都可能引起事故,最终导致损失。方法以描述“要素”偏离设计目的的“引导词”作为分析指导,通过分析确定潜在过程危险和运行中可能出现的问题。

1.2 综合应用思路

将以上三种方法相结合进行导弹系统安全性分析中引发事件鉴别的主要思想是:采用 MLD 对

导弹进行层次化描述,确保分析的完整性和系统性。运用 FMEA 对系统中的主要设备进行分析;运用 HAZOP 分析方法对导弹工作过程进行系统安全分析,针对各级系统间的输入/输出要素关系,在分系统与分系统、设备与设备之间建立有效的联系,从而使分析更加系统、完整、有效。三种方法综合运用的总体思路如图 2 所示。

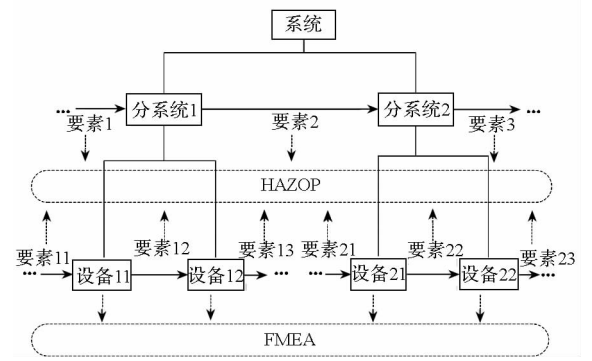


图 2 引发事件鉴别方法综合运用思路

Fig. 2 Integration of initiating event identification methods

1.3 引发事件鉴别步骤

导弹系统安全性分析中的引发事件鉴别流程按照图 3 所示步骤逐步展开。

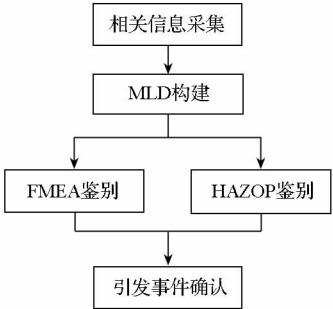


图 3 引发事件鉴别流程

Fig. 3 Initiating event identification process

步骤 1:采集相关信息。需要了解导弹配置与工作状态(各任务阶段上系统的功能组合和物理配置),明确导弹组成结构、功能、任务环境剖面、危险源信息(包括危险品的类型、数量和危险级别)等。

步骤 2:采用 MLD 对导弹进行分级描述,对液体导弹任务、功能、系统进行层次化图形展示。

步骤 3:运用 FMEA 对单一故障类引发事件进行鉴别。

步骤 4:运用 HAZOP 对参数异常类引发事件进行鉴别。

步骤 5:对鉴别的引发事件进行筛选,确认最终的引发事件列表。筛选可依照风险指数法(Risk Assessment Code, RAC)^[4]等定性方法按发生的可能性和后果的严重性两个方面进行。

2 主逻辑图构建

导弹典型的主逻辑图层次结构如图 4 所示。

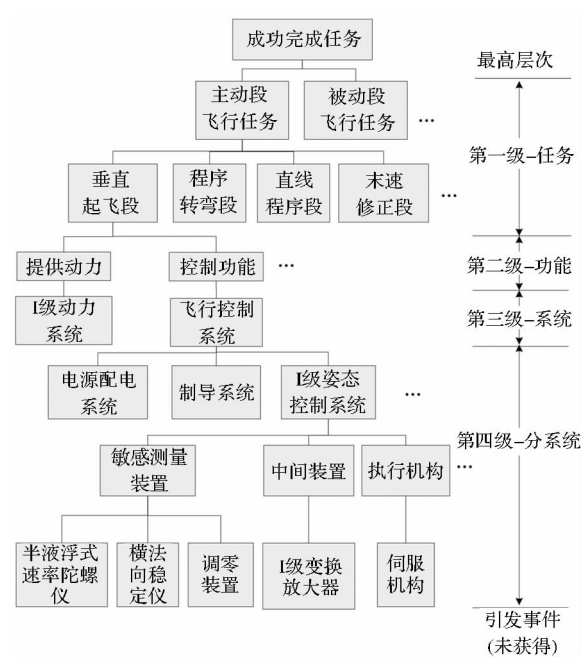


图 4 典型主逻辑图
Fig. 4 General master logic diagram

3 运用 FMEA 鉴别引发事件

FMEA 技术在可靠性分析中应用广泛,是一种行之有效的分析技术。在实际运用中,各行业、机构存在多种指导 FMEA 工作的标准,根据导弹安全性分析实际情况,可采用 GJB 1391 - 2006 《故障模式、影响及危害分析指南》^[9]。根据此标准得到的典型 FMEA 结果如表 1 所示。

由 FMEA 表格中“产品或功能标识”和“故障模式”两列可获得可能的引发事件。如对产品或功能标识“点火信号输出电路”和故障模式“提前发出点火信号”可得到引发事件“点火信号输出电路提前发出点火信号”。在分析过程中可根据实际需要筛选出严酷度类别较高的故障模式。针对每一个分系统,需要关注其所在 FMEA 分析中所在约定层次。事实上,FMEA 实施的第一步即是进行约定层次的划分,已建立起的主逻辑图可为划分方式提供参考。

将 FMEA 结果体现在图 4 所展示的 MLD 中可以得到图 5 所示结果。

表 1 典型 FMEA 结果
Tab. 1 General FMEA results

初始约定层次	约定层次	序号	产品或功能标识	功能	故障模式	故障原因	任务阶段与工作方式	故障影响			严酷度类别	故障检测方法	设计改进措施	使用补偿措施	备注
								局部影响	高一层次影响	最终影响					
X 型导弹	I 级姿态控制系统	110016	伺服机构 活塞杆 活套杆	传递拉力 带动摇摆 发动机 摆动	断裂	强度不够	导弹垂直起飞段	控制不到位	姿态控制异常	导弹发射失败	I	机械性能检测 磁粉探伤 静力试验	使用高强度材料	视情况检查	

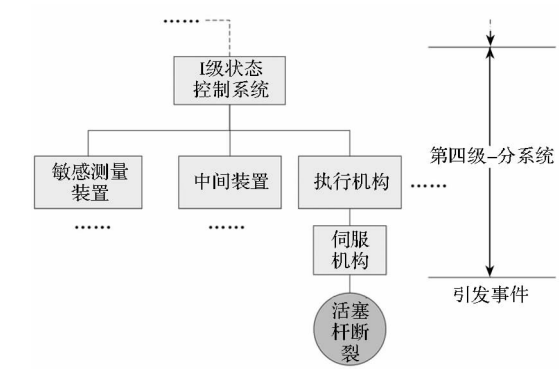


图 5 FMEA 所得引发事件
Fig. 5 Initiating event obtained using FMEA

需要注意的是,在运用 FMEA 方法进行安全性评估中引发事件鉴别时应考虑所掌握的信息和资料情况。在硬件资料相对缺乏时可运用产品功

4 运用 HAZOP 鉴别引发事件

HAZOP 最初主要应用在过程工业,近年来 HAZOP 技术逐渐推广开来,应用领域扩展到核电站安全分析^[10]、事故原因调查^[11]等。特别地,已有 HAZOP 方法主要针对武器装备的改进和应

用^[12-13]。HAZOP 主要优势在于可以对预定的流程、过程进行有效的安全分析。而导弹武器装备在运作过程中涉及大量的物料输送(如液体燃料的加注)、数据(如制导信号)传输。在整个运作过程中系统各部分的输入输出是否正常决定了导弹系统的安全状况。将各部分的输入输出作为 HAZOP 分析的要素可以有效识别其中的缺陷。

HAZOP 以“引导词”作为分析引导,找出分析要素状态变化,然后再继续分析造成偏差的原因、后果及可采取的对策。这里的引导词是针对导弹各单元运行时可能出现的偏差而设定。偏差即是各单元输入输出要素对设计意图或正常条件的背离,其形式通常是“参数+引导词”,如“输出电压过高”=“输出电压+过高”。这里应选取设备输出中对安全性影响较大的参数指标,其中可能的参数包括流量、电流和电压等。设备级参数可参考文献[8]进行设定。HAZOP 方法最初分析的重点是工艺单元。在针对导弹的应用中把导弹设备或设备功能作为工艺单元处理。在此基础上,确定各设备的输入输出要素。进而确定需要进行分析的要素参数。

在具体方法的实施上,国际上使用 HAZOP 技术的主要依据之一是为国际电工委员会(International Electrotechnical Commission, IEC)制定的应用导则。当前国内的 HAZOP 方法运用尚处于起步阶段,国家安全生产监督管理总局于

2011 年参照 IEC 标准发布了《危险与可操作性分析(HAZOP 分析)应用导则》^[14],标准主要针对适用于石油、化工、电子等工业的 HAZOP 分析。下面参照标准对“Ⅰ级姿态控制系统”中“调零装置”进行 HAZOP 分析。为保证导弹在井下发射或塔架发射时,不出现导弹碰壁或碰架,在导弹稳定系统中设置了调零装置,它与综合放大器、伺服机构组成一个闭合的调零回路。图 6 给出了调零功能实现的基本原理。

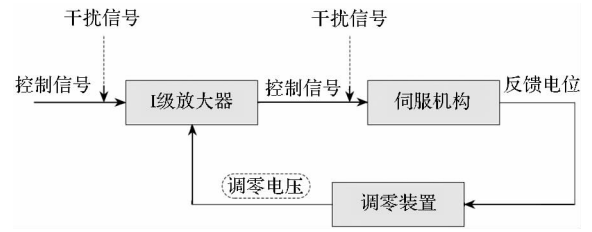


图 6 调零功能原理

Fig. 6 Principle of zero adjustment function

当Ⅰ级放大器的输入控制信号为零时,由于干扰的作用造成伺服机构零位输出,发动机出现零位偏角,伺服机构输出相应的反馈电压,控制调零装置也自动地输出一个相应的调零电压,经过放大器,使发动机零位偏角减小,消除零位干扰,保证导弹安全起飞。由上面的分析可以看出,“调零电压”作为“调零装置”的输出,其是否满足要求是影响导弹发射安全的一个重要因素。将“调零电压”设为分析“要素”,HAZOP 分析最终结果如表 2 所示。

表 2 典型 HAZOP 分析结果

Tab. 2 General HAZOP analysis result

分析 题目	分析 部分	序 号	产品或 功能名称	要 素	引导 词	偏 差	可能原因	后果	安全措施	注 释	建议安全措施	执行人
Ⅰ级 姿态 控制 系统	敏感 测量 装置	10564	Ⅰ级姿态 控制系统 调零装置	调零 电压	少 Less	低电压	调零装置损坏,伺服反馈电位计故障	伺服机构零位输出,发动机出现零位偏角	单元测试;垂直测试中进行控制系统分系统测试	—	对调零装置和伺服反馈电位计的零位、输出极性、最大输出值、正负灵敏度进行测试	

将 HAZOP 中“可能原因”一项体现在图 4 所展示的 MLD 中可以得到图 7 所示结果。

应注意的是,通过对调零电压这一个要素的分析,得到了两个引发事件。涉及两个分系统,即调零电压这一关键参数的影响因素不仅在于其直接相关的调零装置,还涉及伺服机构。这样的分析思路与以元件为中心的 FMEA 方法不同,两种思路能够得到相互补充的分析结果。

5 结论

鉴别引发事件是基于事故机理的安全性分析

方法的首要任务。针对当前引发事件鉴别缺乏系统性的问题,提出了采用主逻辑图统领下 FMEA 与 HAZOP 相结合的引发事件鉴别方式。

FMEA 和 HAZOP 的目的主要都是调动装备操作人员、安全技术人员、安全管理人员和相关装备设计人员的想象性思维,使其能够找出导弹中的危险因素,即潜在的引发事件。FMEA 是以元件为中心的分析方法,而 HAZOP 本质上是以系统为中心的分析方法。FMEA 由一个元件可能发生的故障开始,进而分析整个系统的故障后果,因此,FMEA 是从原因到后果的单向分析。HAZOP

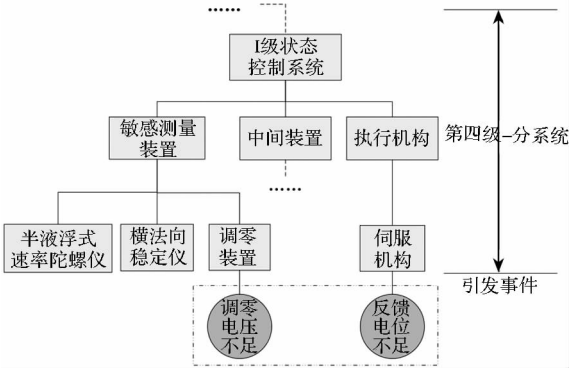


图 7 HAZOP 所得引发事件

Fig. 7 Initiating event obtained using HAZOP

识别导弹系统偏离设计目的的可能偏差,然后从两个方向进行分析,一个方向查找偏差的原因,一个方向推断其后果。FMEA 分析的对象是导弹系统的元部件,是对整个导弹系统中的“点”进行分析,而 HAZOP 是对导弹的工作程序、流程进行的分析,主要是对“线”的分析。采用 MLD 作为分析的“面”对导弹进行系统性的层次化描述,考虑导弹任务剖面,对鉴别出的引发事件进行整理和归纳,增加引发事件鉴别的系统性,分析工作组成一个完整的系统。三种方法的综合运用,不仅可以更全面合理地找出可能的引发事件,还为导弹系统安全分析提供了一种新的途径,为最终有效预防和减少事故发生提供了理论支持。此外,所涉及的方法当前已有相应的执行规范,可根据导弹安全性分析的需要进行相应的修改,方法具有较强的可操作性。

参考文献 (References)

[1] Keller W, Modarres M. A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late professor Norman Carl Rasmussen [J]. Reliability Engineering and System Safety, 2005, 89(3): 271 - 285.

[2] Stamatiatos M, Dezfuli H, Apostolakis G, et al. Probabilistic risk assessment procedures guide for NASA managers and practitioners version 2.0 [R]. Washington D.C.: Office of Safety and Mission Assurance, NASA Headquarters, 2011.

[3] Meng Q, Qu X, Wang X, et al. Quantitative risk assessment modeling for non-homogeneous urban road tunnels [J]. Risk Analysis, 2011, 31(3): 382 - 403.

[4] 周经伦, 龚时雨, 颜兆林. 系统安全性分析[M]. 长沙: 中南大学出版社, 2003.

ZHOU Jinglun, GONG Shiyu, YAN Zhaolin. System safety analysis[M]. Changsha: Central South University Press,

2003. (in Chinese)

[5] 王涛, 余文力, 王效廉. 导弹战斗部炸药部件安全性分析[J]. 质量与可靠性, 2008(4): 29 - 31.

WANG Tao, YU Wenli, WANG Xiaolian. Safety analysis of explosive device in missile warhead [J]. Quality and Reliability, 2008(4): 29 - 31. (in Chinese)

[6] 陈广南. 固体火箭发动机机械撞击载荷作用下安全性研究[D]. 长沙: 国防科学技术大学, 2005.

CHEN Guangnan. Investigation of the safety for solid rocket motor under mechanical impact [D]. Changsha: National University of Defense Technology, 2005. (in Chinese)

[7] GJB 90 - 1990. 系统安全性通用大纲[S]. 北京: 国防科学技术工业委员会, 1990.

GJB 90 - 1990. General program for system safety [S]. Beijing: Commission on Science, Technology, and Industry for National Defense, 1990. (in Chinese)

[8] 蒋平, 邢云燕, 王冬, 等. 复杂系统故障安全风险评价方法[J]. 国防科技大学学报, 2014, 36(6): 117 - 122.

JIANG Ping, XING Yunyan, WANG Dong, et al. Failure safety risk evaluation approach for complex systems [J]. Journal of National University of Defense Technology, 2014, 36(6): 117 - 122. (in Chinese)

[9] GJB/Z 1391 - 2006. 故障模式、影响及危害性分析指南[S]. 北京: 中国人民解放军总装备部, 2006.

GJB/Z 1391 - 2006. Guide to failure mode, effects and criticality analysis [S]. Beijing: PLA General Armament Department, 2006. (in Chinese)

[10] Hashemi-Tilehnoee M, Pazirandeh A, Tashakor S. HAZOP-study on heavy water research reactor primary cooling system [J]. Annals of Nuclear Energy, 2012, 37(3): 428 - 433.

[11] Kletz A T. Accident investigation; keep asking “why?” [J]. Journal of Hazardous Materials, 2006, 130(1/2): 69 - 75.

[12] 姜光楠, 戎梅, 冯畅, 等. 安全性方法——HAZOP 的改进及在武器装备等复杂系统上的应用[C]//大型飞机关键技术高层论坛暨中国航空学会 2007 年学术年会论文集, 深圳, 2007.

LOU Guangnan, RONG Mei, FENG Chang, et al. Safety method—improvement of HAZOP and its application in weapon system [C]//Proceedings of High Level Forum on Key Technology of Large Aircraft and the China Aviation Society 2007 Academic Annual Meeting, Shenzhen, 2007. (in Chinese)

[13] 焦健, 王薇, 赵廷弟, 等. 面向装备使用安全的 HAZOP 方法[J]. 兵工自动化, 2009, 28(9): 58 - 60.

JIAO Jian, WANG Wei, ZHAO Tingdi, et al. HAZOP study for weapon system operational safety [J]. Ordnance Industry Automation, 2009, 28(9): 58 - 60. (in Chinese)

[14] AQ/T 3049 - 2013. 危险与可操作性分析 (HAZOP 分析) 应用导则[S]. 北京: 国家安全生产监督管理总局, 2013.

AQ/T 3049 - 2013. Hazard and operability studies (HAZOP studies) application guide [S]. Beijing: State Administration of Work Safety, 2013. (in Chinese)