

# 人为失误的分析方法及其应用

张春来

大连海事大学 轮机工程学院, 辽宁 大连 116026

**摘要:**讨论了人为失误研究的几种方法在生产安全研究中的重要性及其适用范围,并通过具体实例对各种方法进行了分析和验证,可为相关部门提供生产安全评估和检验的理论依据。

**关键词:**人为失误;故障树;综合评判;火灾;人类工程学

**中图分类号:**U698 **文献标识码:**A **文章编号:**1001-2265(2000)07-0014-04

## Means and application of human element analysis

Zhang Chunlai

**Abstract:** This paper intends to introduce human reliability assessment techniques that can be applicable to risk assessment of the fire accident in the working-room, to identify the most critical top events, intermediate and basic events, error type and relevant root causes, and to assess their influence on technical, manning, training, management, and work environment issues, and thus advances ways to improve and eliminate these problems.

**Key words:** human error; fault trees; synthetic assessment; fire; ergonomics

## 1 引言

人在由“人-工作系统-环境”构成的大系统中处于中心的地位,对事故的发生和发展起着至关重要的作用,来源不同的相关统计分析资料和数据表明:大多数人认为80%左右的事故是由于人为失误所造成的。因此,研究人为失误,及时客观地识别人员操作失误的风险并积极采取相应的预防措施,对于降低事故发生率、促进生产安全有着重要的意义。

通过对人为失误的研究,可以有效地促进生产安全管理水平的提高。安全本身是一个模糊的概念,生产系统不发生事故并不表明该系统是安全的,系统在人员的操纵下没有发生事故,也不表明人的行为就是安全的,安全检查的目的就是发现隐患、消除潜在的危险。通过对人为失误研究获得的成果来改变以往的安全检查仅仅是对设备或系统的硬件进行是否符合“规范”的检验,达到对“人”的检验,最终达到有效地促进安全管理水平的提高之目的。

由于影响生产安全的人为失误众多,以海事船务为例,目前国际上通常把人为失误分为五个方面进行研究,即:(1)技术方面的研究(包括:设计、人类工程学、制造/结构、安装、认证、保养、修理、改装、更新等);(2)人员状况方面的研究(包括:任职资格、船员人数、船员组成、个人文化背景、工作语言、医疗状况等);(3)培训方面的研究(包括:基本安全培训、熟练程度、技能、扩充安全培训、个人陆地培训等);(4)管理方面的

研究(包括:政策、安全意识、动机、责任、主管权力、工作计划、意外事故计划、应急措施、工作手册、指导书、工作方法、检查清单等);(5)工作环境/工作条件方面的研究(包括:有毒物质、工作场所的人员防护方法、伤害、工作时间、休息时间、疲劳、生存条件、人机界面等)。这几个方面既有其内在的联系又有各自的不同特点,故所采用的研究方法亦应符合其特点。

## 2 人为失误的分析方法

### 2.1 故障树分析法

故障树分析法是可靠性所有分析方法中最主要且最常用的一种方法,通过对可能造成系统失效的各种人为因素进行分析,画出逻辑框图(即故障树),确定系统失效原因的各种可能组合方式或系统失效发生概率,具有直观性强(在清晰的故障图形下表达了系统的内在联系及单元与系统失效之间的逻辑关系),适用面广(能反映各种外部因素对系统故障的影响),分析方便(既可进行定性分析又可进行定量分析)的特点,特别适用于大型复杂系统的可靠性分析,而且既可进行定性分析,又可定量分析。

定性分析的任务就是求出故障树的全部最小割集。由于全部最小割集反映了系统的全部故障模式,所以全部最小割集的集合又称之为系统的故障谱。通过对故障谱的分析,可以找出系统的薄弱环节,提高系统的可靠性与安全性。

定量分析的意义在于利用故障树这一逻辑图形作为模型,估计顶事件发生的概率;可以对系统的可靠性、安全性进行评价;求解每个底事件的发生对促成顶事件发生的重要程度,为采取相应的措施提供理论依据。用最小割集求解底事件阶次重要度  $I(i)$  的计算公式为:

$$I(i) = D_{i \text{ } k_j} \frac{2}{2^r - 1}$$

式中  $i$  ——基本事件的序数 ( $i = 1, 2, 3, \dots, n$ )  
 $j$  ——最小割集的序数 ( $j = 1, 2, 3, \dots, k$ )  
 $D$  ——最小割集的序数,  $D = 1/N_k$ ,  $N_k$  为最小割集数。  
 $r$  ——基本事件所在最小割集的阶数<sup>[1]</sup>

用故障树分析法进行人为失误研究时,由于在进行定量分析时,需要有各个相关因素的失效概率数据,必须依赖“大量统计和试验”的相关数据,而目前普遍缺乏相应的人为差错率统计数字,而其它领域所做的相关统计资料尚不能真实反映人员操作行为的可靠性,故该方法主要用于以系统或设备失效为主的人为失误研究。

### 2.2 模糊综合评判方法<sup>[2]</sup>

该方法是用模糊风险值评价系统安全程度,并将复杂的评价计算过程自动化。建立评价模型的程序为:(1)评价指标体系的设计与确定;(2)各评价指标权重确定;(3)评价指标隶属度确定;(4)模型建立与应用。若设  $U = \{U_1, U_2, U_3, \dots, U_n\}$  为  $N$  种因素构成的因素集或指标集;设  $V = \{V_1, V_2, V_3, \dots, V_m\}$  为  $M$  种决断所构成的评判集;则由  $U$  和  $V$  之间的模糊关

系  $R = (r_{ij})_{n \times m}$  就可得出模糊综合评判的模型为:

$$R = \begin{bmatrix} r_{11} & r_{12} & \dots & r_{1m} \\ r_{21} & r_{22} & \dots & r_{2m} \\ \dots & \dots & \dots & \dots \\ r_{n1} & r_{n2} & \dots & r_{nm} \end{bmatrix}$$

该评判模型的特点:(1)评价对象多变,难以保证各位专家对评价对象都能充分了解;(2)评判可能在短时间内快速进行,很难即时展开大范围专家调查;(3)评判对象的部分指标随时变化,即时进行专家调查很难适应指标变化;(4)评价行动可能人员工作中进行,可供选择的专家人数会受较大限制。因此该评判模型特别适用于对独立承担工作任务人员的安全作业水平和工作人员队伍所具备的安全质量进行系统化、量化的评估。

### 2.3 人类工程学的研究方法

一个设计很差的界面容易导致错误,而这种错误无法通过加强培训和管理予以完全避免。先进的技术可能因为其具有更复杂的人的操作界面而存在更为严重的事故隐患。人类工程学是从人的科学中产生并总结出来的,它可以使工作、系统、产品和环境同人的体力、智力和极限相适应。

人类工程学可以分成两类:微人类工程学和宏人类工程学,这两类都涉及到人的生理和心理因素。微人类工程学着重于个体工作中的“人-机”界面关系;宏人类工程学着重于整个工作系统、主要的子系统结构与过程的设计。

过去,普通工业产品并不在设计时采用人类工程学,现在人们已经认识到提高生产安全性的一个积极的措施就是采用人类工程学的设计,因为一个设计良好的工作环境可以自然产生一些操作上的便利,降低工作强度和失误率。

### 3 人为失误分析方法的应用

以包含有可燃物的生产场所发生火灾为例,应用上述方法对该生产场所进行安全评估,并对可能导致火灾发生的各种人为失误进行定性和定量的分析。

#### 3.1 故障树的建立

##### 3.1.1 顶事件的选择

顶事件是系统不希望发生的事件,其选择依据应考虑致命的、高度可能的主要事件。从生产场所安全可靠运行的角度来看,“发生火灾事故”为可能发生且较为值得关注的希望发生的事故,这里选择“发生火灾事故”作为建立故障树的顶事件。

##### 3.1.2 边界条件及假设

合理确定边界条件,以便确定故障树的范围。这包括确定系统的初始状态,确定可以忽略不计的小概

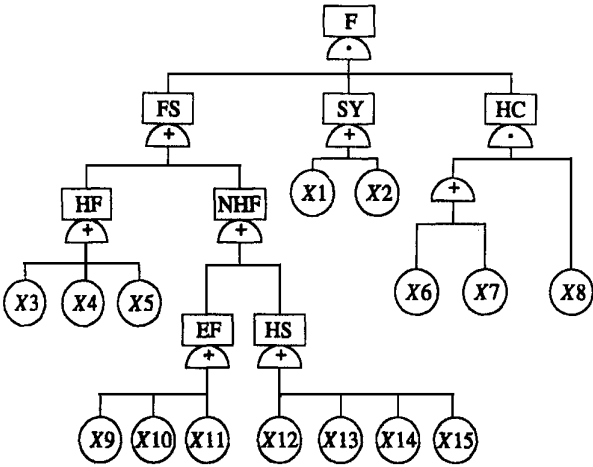


图1 失火故障树

$X_1$  - 未采取措施;  $X_2$  - 报警及消防系统失效;  $X_3$  - 吸烟;  $X_4$  - 电气焊;  
 $X_5$  - 其他人为火源;  $X_6$  - 废弃油污;  $X_7$  - 设备或管道泄露燃油;  $X_8$  - 排风系统失效;  $X_9$  - 电气系统发生短路;  $X_{10}$  - 电气系统产生电弧或电火花;  $X_{11}$  - 电气设备绝缘被击穿;  $X_{12}$  - 正常运转设备产生的热表面;  $X_{13}$  - 大功率灯;  $X_{14}$  - 过电流引起的设备或线路过热;  $X_{15}$  - 其他原因产生的热表面

率事件,确定在一定条件下的必然事件等。

本文分析中主要考虑了由人为失误引起的基本故障事件,于此,假设所分析系统的各组成部分是二状态,即只有正常工作状态及故障状态;假设各组成部分的基本故障事件是相互独立的,并忽略由系统环境和不可抗力引起的事件。

3.1.3 故障树的建立

采用手工建树的方法,由顶事件出发循序渐进地寻找每一层事件发生的所有可能的原因,并一直分解到基本的底事件为止,得到图 1 的故障树。

3.2 定性分析

定性分析的任务就是求出故障树的全部最小割集。由于全部最小割集反映了系统的全部故障模式,所以全部最小割集的集合又称之为系统的故障谱。通过对故障谱的分析,可以找出系统的薄弱环节,提高系统的可靠性与安全性。利用富塞尔方法求得“失火故障树”的最小割集为:

$\{x_1, x_3, x_6, x_8\}; \{x_1, x_4, x_6, x_8\}; \{x_1, x_5, x_6, x_8\}; \{x_1, x_3, x_7, x_8\}; \{x_1, x_4, x_7, x_8\}; \{x_1, x_5, x_7, x_8\}; \{x_2, x_3, x_6, x_8\}; \{x_2, x_4, x_6, x_8\}; \{x_2, x_5, x_6, x_8\}; \{x_2, x_3, x_7, x_8\}; \{x_2, x_4, x_7, x_8\}; \{x_2, x_5, x_7, x_8\}; \{x_1, x_6, x_8, x_9\}; \{x_1, x_6, x_8, x_{10}\}; \{x_1, x_6, x_8, x_{11}\}; \{x_1, x_6, x_8, x_{12}\}; \{x_1, x_6, x_8, x_{13}\}; \{x_1, x_6, x_8, x_{14}\}; \{x_1, x_6, x_8, x_{15}\}; \{x_1, x_7, x_8, x_9\}; \{x_1, x_7, x_8, x_{10}\}; \{x_1, x_7, x_8, x_{11}\}; \{x_1, x_7, x_8, x_{12}\}; \{x_1, x_7, x_8, x_{13}\}; \{x_1, x_7, x_8, x_{14}\}; \{x_1, x_7, x_8, x_{15}\}; \{x_2, x_7, x_8, x_9\}; \{x_2, x_7, x_8, x_{10}\}; \{x_2, x_7, x_8, x_{11}\}; \{x_2, x_7, x_8, x_{12}\}; \{x_2, x_7, x_8, x_{13}\}; \{x_2, x_7, x_8, x_{14}\}; \{x_2, x_7, x_8, x_{15}\}。$

以上共计 40 组,当这些最小割集任何一个发生时,顶事件必然发生,这有助于我们掌握事故发生的规律,为预防事故的发生提供了全面而可靠的信息,并根据这些信息采取积极有效的预防措施,达到杜绝或减少事故发生的目的。

3.3 定量分析

定量分析的意义在于利用故障树这一逻辑图形作为模型估计顶事件发生的概率;可以对系统的可靠性、安全性进行评价;求解每个底事件的发生对促成顶事件发生的重要程度,为采取相应的措施提供理论依据。在本文中由于底事件较多,为能方便地比较各底事件在故障树中的重要性,特别是人为失误的影响程度,仅对结构重要度进行分析。经计算得:

$I(1) = I(2) = I(6) = I(7) = 0.067$   
 $I(3) = I(4) = I(5) = I(9) = I(10) = I(11) =$   
 $I(12) = I(13) = I(14) = I(15) = 0.017$   
 $I(8) = 0.133$

排列顺序为:

$I(8) > I(1) = I(2) = I(6) = I(7) > I(3) =$   
 $I(4) = I(5) = I(9) = I(10) = I(11) = I(12) = I$   
 $(13) = I(14) = I(15) I$

3.4 人为失误的原因分析

在火灾事故中,我们依据上述分类原则,把引发顶事件发生的 15 个基本事件中的人为失误归纳在表 1 中,其中  $Y_1$ —技术方面;  $Y_2$ —人员状况方面;  $Y_3$ —培训方面;  $Y_4$ —管理方面;  $Y_5$ —工作环境/工作条件方面; 1—有关系; 0—无关系。

表 1 基本事件与人为因素的关系表

基本事件	人为失误	$Y_1$	$Y_2$	$Y_3$	$Y_4$	$Y_5$
$X_1$	易燃物未专门处理	1	0	0	1	0
$X_2$	报警消防系统失效	1	0	1	1	1
$X_3$	吸烟	0	0	1	1	1
$X_4$	电气焊	0	0	1	1	1
$X_5$	撞击摩擦产生明火	0	0	1	1	1
$X_6$	油污处理	1	0	1	1	0
$X_7$	燃油泄露	1	0	0	1	0
$X_8$	通风失效	1	0	0	1	0
$X_9$	电气短路	1	1	0	1	0
$X_{10}$	电气火花	1	0	1	1	0
$X_{11}$	绝缘破坏	1	1	1	1	0
$X_{12}$	设备发热	1	0	0	0	0
$X_{13}$	灯泡发热	1	0	0	0	0
$X_{14}$	过流发热	1	1	1	1	0
$X_{15}$	其他过热	1	0	0	0	0

引发顶事件(失火)发生的 15 个基本事件,又可以继续分解为由人为因素组成的 39 个基本事件。其中,技术方面的因素 12 项,占 31%;人员状况方面的因素 3 项,占 7.6%;培训方面的因素 8 项,占 21%;管理方面的因素 12 项,占 31%;工作环境/工作条件方面的因素 4 项,占 10%。

3.5 减少人为失误的可行方法

$X_8$ —排风系统失效;  $X_2$ —报警及消防系统失效,在重要度分析中显示为最重要,所涉及的人为失误有:技术方面的因素(系统的设计、安装、保养、维修等);管理方面的因素(保证系统正常工作所需的责任、计划、方法、检查及安全意识)。培训方面的因素(具有基本的消防常识);管理方面的因素(保证系统正常工作所需的责任、计划、方法、检查及安全意识);工作环境/工作条件方面的因素(系统应符合人类工程学的基本原理)。

减少人为失误的可行方法,以消防阀控设计在易于接近的位置上操作为例:为使阀容易被所有可能的人员接近和操作,有几个主要的因素应考虑:(1) 安装位置应位于操作者站立平面上(或下)的适宜的高度;

(2) 阀手柄正确排列(即与操作者站立平面平行或垂直);(3) 阀手柄一周要有足够的间隙以便于操作者能摸到阀;(4) 阀的操作力量;(5) 阀的操作机构(是手轮还是直手柄);(6) 手轮的大小(决定了阀的操作是靠一只手还是两只手);(7) 阀位指示器的位置和排列(如果装备了阀位指示器)。这几个主要的因素使操作者决定了阀的可操作性。根据人类工程学的研究结果建议在阀控设计时:(1) 手轮直径小于 152mm 的阀,其手轮应被设计和定位成手操作式;手轮直径大于 152mm 的,其手轮应按双手操作式被设计和定位。(2) 用于应急的阀不应位于其他盖子后面(除非盖子被标识且不需移走其他固定件即可打开);位于站立平面之下的阀,手柄应垂直或平行于站立平面且手柄的抓握平面不低于站立平面 304mm;位于站立平面以上的阀,手柄应被定向以便于操作者仅用推(或拉)即可开(或关)阀;大于 508mm 英寸的阀,手轮或手柄不应高于操作者站立平面 1951mm;带手柄的阀(如:球阀),靠近人行道时应被定向以便于当它关闭时其手柄不插入人行道。(3) 操作者站在前面操作的阀,在阀手柄前应有至少 608mm 的间隔;阀的位置应是不必站在管子、电缆

架、扶手、设备或其它物体上就可接近阀手柄;阀手轮或手柄周围至少要有 76mm 的间隔以便于操作者的手能进入。(4) 手轮应是逆时针开,顺时针关。

## 4 结束语

安全生产中的人为失误和人类工程学应用的研究是目前安全系统工程研究的重点,对分析和预测由于人为失误引起的危险,识别潜在事故隐患具有重要的意义。

### 参考文献

- [1] 黄祥瑞. 可靠性工程. 北京:清华大学出版社,1990,68~80
- [2] 黄燕品. 海事预防中人为失误风险的量化评估. 大连海事大学学报 1998(3):1~4
- [3] ABS《Guidance note on the application of ergonomics to marine systems》Co. American Bureau of Shipping,1998,299-318

收稿日期:2000-04-21

作者简介:张春来(1962-),男,天津人,大连海事大学讲师,硕士。

(编辑 江 复)

(上接第 6 页)

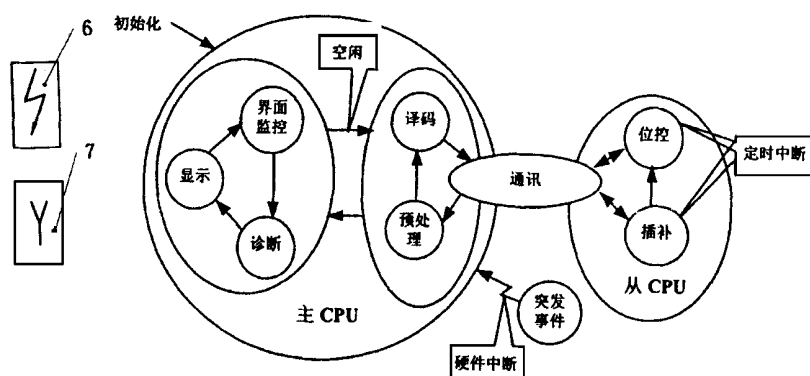


图 4 并行多任务调度模型

对于一些突发事件,如刀具碰撞等,一旦发生将中断所有对象的执行。上述不同优先级的对象之间采用抢占式的调度策略,同等优先级的对象之间采用基于时间片的循环轮转调度策略,并行多任务调度模型如图 4 所示。

## 5 结束语

采用 OO 技术建立数控软件通用模型是提高数控软件可重用性和可重构能力的有效方法,也是实现开放式、全软件数控的必要前提。本文在分析数控软件功能模型的基础上,提出通过建立数控软件通用类库的方法来实现数控软件模块的可重用,并建立了基于客户/服务器的通信模型和并行多任务调度模型。该

思想已经在车床数控系统和铣床数控系统中得到应用,实现了译码、预处理、插补、诊断等模块的可重用和多任务并行处理。

### 参考文献

- [1] ESPRIT III OSACA. Open system architecture for controls within automation systems. OSACA Final Report, April 30 1996, <http://www.os-aca.org>
- [2] G. Pritschow, Ch. Daniel. Open System Controller - A Challenge for the Future of the Machine Tool Industry. Annals of the CIRP, 1993 (42): 1
- [3] 吴祖育,秦鹏飞编.《数控机床》第二版,上海:上海科学技术出版社,1998
- [4] 吴涵生等编.《面向对象的开发技术及其应用》第一版.上海:上海科技文献出版社,1995
- [5] 胡俊. 基于 Windows95 新型车床数控界面系统的研究. 合肥工业大学硕士学位论文,1999
- [6] 王宇晗等. 开放结构数控系统的行为建模研究. 中国纺织大学学报(英文版),2000(1)
- [7] 左静等. 数控系统软件芯片的研制和开发. 中国机械工程,1999(10):4

收稿日期:2000-03-06

作者简介:王宇晗(1966-),男,江苏阜宁人,上海交通大学讲师,硕士。

(编辑 江 复)