第13卷第11期 中国安全科学学报 Vol.13No.11
2003年11月 China Safety Science Journal Nov.2003

复杂工业系统中人因失误根本原因分析

戴立操 工程师 张 力 黄曙东
(南华大学人因所)

学科分类与代码:620.2040
基金项目:国家自然科学基金资助项目(70271016);国防军工技术项目(Z012002A001)。

【摘 要】 在现代大规模复杂人-机-环境系统中,人因失误诱发的故障或事件呈上升趋势。人因事件的根本原因分析,对于防范复杂系统中事故的发生是非常必要的。人因事件根本原因的分析包括:需要分析的人因事件的确定;对事实进行调查、分析调查结果;确定根本原因;制定纠正措施;完成最终报告。人因事件的分析最终需要找出失效屏障并提出修补的方法,笔者采用事件与原因因子分析技术来进行分析。在分析过程中,需要绘出事件和原因因子图(E&CF图),而E&CF图可以显示出从开始到结束全过程中事件发生的正确次序,通常包括失效屏障,预先存在的条件、次级事件、不恰当的动作和形成事件的原因因子。形成人因事件的原因因子在复杂工业系统中,可以分成12个部分。笔者给出了核电厂蒸汽发生器(SG)主给水阀门泄漏的人因事件的分析实例,确认了该实例中失效的屏障和事件的根本原因并提出了纠正措施。

【关键词】 复杂人机环境 人因失误 事件和原因因子图(E&CF图) 屏障分析

Analysis of Fundamental Causes of Man-made Errors in Complex Industrial System

Dai Licao, Engineer Zhang Li Huang Shudong
(Institute of Human Factor, Nanhua University)

Abstract: In modern large-scale complex man-machine-environment system, failures and events caused by human errors show an increasing trend. Analysis on fundamental causes of man-made errors is necessary in preventing accidents. The analysis includes determination of the man-made event to be analyzed, fact investigation, analysis on investigation results, determination of fundamental causes, deciding the rectifying measures and accomplishing the finalized report. The final aim of the analysis is to find out the failure barrier and the way of remedy. The authors conduct this analysis by event & cause factor (E&CF) chart. In the analysis, E&CF chart needs to be drawn to show the correct sequence of the happenings in whole process, including failure barrier, pre-conditional factors, sub-events, inappropriate actions and the final human elements forming 12 categories of cause factors. The authors present an analysis case of main water supply valve leakage of the steam generator in a nuclear power plant. The failure barrier, the fundamental causes of the event are also presented, and then the rectification measures are suggested.

Key words: Complex man-machine-environment Man-made error E&CF(Event & cause factor)chart Screen analysis

1 引 言

在现代大规模复杂的人-机-环境系统中,随着科技的发展与进步,系统软、硬件可靠性不断提高,引起的事故比例逐渐下降,而人因失误诱发的故障或事件却呈上升趋势。人因失误已成为大规模复杂系统失效或事故最重要的原因之一。对人因失误的研究与防范也更为突出与重要[1]。对于典型的系统事故分析方法有:失误模式、影响及严重度分析(FMECA, Failure Mode, Effects and Criticality Analysis)、故障树分析(FTA, Fault Tree Analysis)法等。对于人的失误,由于其生理、心理、社会、精神等特性,具有极大可塑性和难以控制性,如何分析和预防人因事件成为复杂系统事故分析的重点和难点。

复杂工业系统本身的人因特征是:人机界面复杂,人机

接口多样,环境不确定性,需要处理信息复杂动态特性多样及操作人员行为的复杂性[2]。由于以上特征,要消除人因失误几乎是不可能的,但可以最大限度地设法减少它。减少的办法就是研究人因失误的根本原因,并提出改进措施加以防范[3]。笔者借鉴故障树分析方法的思路和程序,从人因事件的表征出发,寻找引发人因事件的根本原因。

2 人因事件根本原因分析程序

人因事件根本原因分析包含6个步骤:

① 确定需要分析的人因事件;

② 对事实进行调查;

③ 分析调查结果;

④ 确定根本原因;

⑤ 制定纠正措施;

⑥ 完成最终报告。

其分析程序如图1所示。

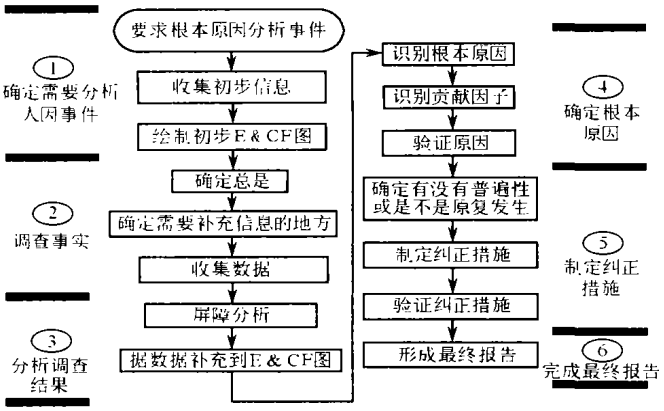

图1 人因事件根本原因分析程序

2.1 确定需要分析的人因事件

确定需要分析人因事件的目的是:确定人因事件发生的主体、发生地点、发生时间、具体发生情况和规模,由此确定事件的调查范围。其过程如下:

(1) 对相关人员(具有或可能具有相关知识和经验的人)进行调查和讨论,收集初步信息;

(2) 绘制人因事件的事件和原因因子图(E&CF:Event & Cause Factor)。采用倒推的方法,排出引起问题发生的次序,同时获取相关数据。提问程序为:

① 什么事——发生了什么事,什么设备受到影响,发生了什么不恰当行为,如果有,那么违反了哪些要求。确定究竟发生了什么事,并与文件、规程或政策要求进行比较,从中可以找出可能的线索。

② 时间——问题发生的时间,发现问题的具体时间(年、月、日、时)。

③ 地点——发生问题的地点,发现问题的具体地点。

④ 多少——确定问题的严重程度以及普遍程度(影响)。

2.2 对事实进行调查

对事实进行调查的目的是:通过调查确定事件是怎么发生的。其过程如下:

(1) 查找系统内的相关经验,查找相关问题的档案和文件,如趋势分析数据库、系统运行经验反馈等。

(2) 从初步的E&CF图中,确定需要收集的进一步信息。

(3) 确定可能的原因种类。根据WANO(World Association of Nuclear Operators)手册,人因事件归属于12个类型的原因因子[5](见3.3节)。

2.3 分析调查结果

分析调查结果的目的是:分析调查结果、在事件和原因因子图中把信息补充完整。其过程如下:

(1) 在E & CF图中,添加在调查过程中新发现的信息:所有事件的次序、作为证据的所有事实的来源、所有结论的原因、所有假设的基础、所有文件的资源。用收集到的补充信息重新审查E & CF图。

(2) 调查必须反复进行,在分析中必须包含新的信息和证据。

2.4 确定根本原因

确定根本原因的目的是:分析调查结果,确定事件为什么会发生。其过程如下:

(1) 对于人因因素相关问题,使用E&CF图来确定潜在的原因因子(对于设备性能问题,可以用故障树分析法来确定原因因子或贡献因子)。人因因素根本原因的分析必须一直持续到超出系统的控制范围。

(2) 完成E&CF图。在最终的E&CF图中,对调查中确定的每一个问题(主要结果/不恰当动作)确定其根本原因和贡献原因。原因因子图及其定义可以用来确定根本原因和贡献原因。

2.5 制定纠正措施

针对发生问题的原因来制定纠正措施,防止问题重复发生。

2.6 完成最终报告

最终报告需要永久保存。在以后的趋势分析,问题的解决和纠正行动的审核中可以随时查验。

3 事件与原因因子分析技术

复杂工业系统中,人因事件根本原因分析的主要方法是采用原因因子(E&CF)图。由于人因事件的分析最终需要寻找出失效的屏障并提出修补的方法,E&CF图必须与屏障分析图结合进行分析。

3.1 绘制 E&CF 图

(1) E & CF 图可以清楚表明事件的先后次序及引起事件的原因。复杂系统中的人因事件通常不是单个人因屏障失效的结果，而是经过一段时间发展以及包括多个作业组、系统、作业任务和人员组织机构及相关设备的复杂条件引起的。

(2) E & CF 图可以显示出从开始到结束这一过程中事件发生的正确次序，包括失效的屏障、预先存在的条件、次级事件、不恰当动作和形成事件的原因因子。

(3) 在绘制 E&CF 图的过程中，可能的原因因子将变得很明显。

3.2 屏障分析

屏障分析是找出应用于某一状态的所有的实体和行政管理控制并对他们的有效性进行评价的过程。

(1) 屏障是一种行政管理控制或者是实体控制，用来改善人员和设备的可靠性能和防止不恰当行动的发生。行政管理屏障(如文件、培训等)保证人员表现的可靠性，实体屏障(如设备联锁、设计裕度)是用来保护人员和设备以及增强人－机接口的安全及性能的设施。

(2) 由于复杂系统包括许多个作业组，系统、作业任务和设备条件复杂，屏障是多重的和多样的而不是单一的。所有的屏障依次失效才会导致不希望的事件的发生。最接近主要后果的屏障是分析的焦点。

(3) 屏障分析必须把事件和原因因子图结合在一起使用，这样就可以确定事件次序中屏障的位置(综合方法)，来确定和评估该状态中所有的已知的行政管理上或实体的屏障。

(4) 为了防止事件的重复发生、屏障需要强化、更换和补充。

3.3 原因因子判定

对复杂系统根本原因的确认，需对原因因子进行深入调查和完善，直到出现下列条件之一：①原因已超出复杂系统员工的控制范围；②防止该原因的纠正措施的代价超出允许的范围；③主要的影响得到完整解释；④没有其他的原因可以解释要评估的影响；⑤进一步的原因及影响分析将不会为纠正主要问题提供更多的益处。

复杂工业系统中人因事故原因因子可分成12 个部分：

(1) 书面交流：信息不准确，内容缺陷，无书面文件；

(2) 接口设计或设备状态：人和机器联系机制缺陷，设备状态缺陷；

(3) 人员工作实践：错误探测实践，文件应用实践，设备、材料应用实践，人员准备实践；

(4) 管理方法：管理目标，管理监督，管理评价，责任，纠正措施；

(5) 口头交流；

(6) 工作进度表；

(7) 资源管理；

(8) 监督方法；

(9) 培训/资格；

(10) 环境条件；

(11) 变更管理；

(12) 工作组织、计划。

4 分析实例

核电厂是属于高风险的复杂工业系统。据统计，核电厂的系统失效其中20％～90％与人有关，而人因事件直接或间接引起事故的比率为 70％～90％[3]。笔者给出核电厂系统中一起人因事件的实例分析。

4.1 事件描述

核电厂蒸汽发生器(SG，Steam Generator)主给水调节阀泄漏，很难控制 SG 液位，值长决定关闭一个手动给水隔离阀，用给水旁通阀控制 SG 液位。接班人员在电站启动期间提升功率，在液位问题被诊断和纠正前，发生了低液位紧急停堆。通过对主控室操纵员及相关技术人员调查与访谈，得出这一事件的细节如下：

(1) 水调节阀已修理好，但由于机组启动的压力，放弃了对此阀的泄漏试验；

(2) 运行人员启动机组；

(3) 给水调节阀泄漏，值长决定隔离此阀，并使用 2 号旁路阀；

(4) 这一信息没有记入运行日志，也没有在设备上挂牌，并且在交接班时也没有向下一值交代；

(5) 接班的运行人员继续启动机组；

(6) 功率继续上升，直到产生的蒸汽超过了给水旁路阀的给水能力，SG 低液位而停堆。

4.2 事件 E&CF 图

核电厂 SG 人因事件 E&CF 图如图 2 所示。

4.3 事件屏障分析图

图 3 是核电厂 SG 人因事件屏障分析图。这起事件中下列屏障失效：

(1) 规程——违反安全操作规程，未按照规程要求记下电站的异常设备情况；

(2) 交接班——没有告诉下一值的操作员或值长关于隔离阀的事；

(3) 运行日志——使用旁路阀未在运行日志上记录；

(4) 挂牌——没有挂牌标明阀门已关闭；

(5) 挂牌日志——没有使用；

(6) 泄漏试验——未执行，规程允许在值长认为必要的时候可以不进行该试验；

(7) 系统巡检——在把主给水调节阀投入运行前没有进行巡检(在这个电站，系统巡检是规范化做法)；

(8) 流量指示——当给水流量无法增加时，操作员没有

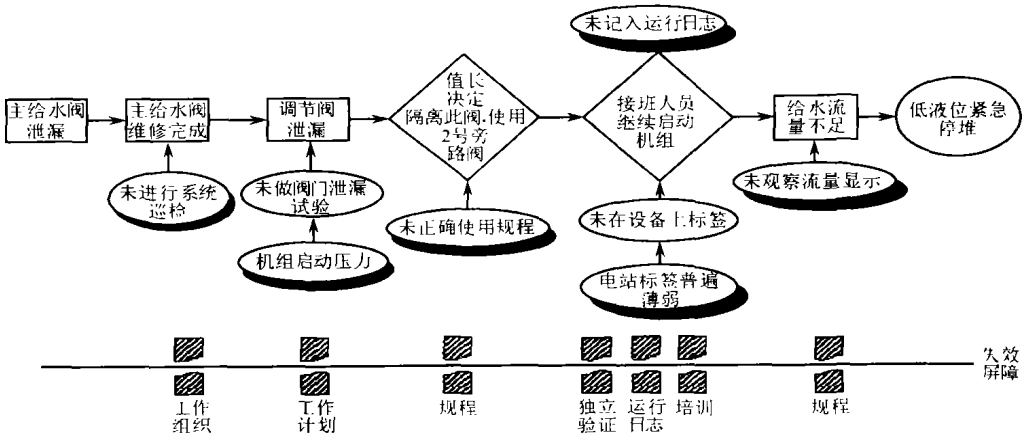

图 2 核电厂 SG 人因事件 E&CF 图

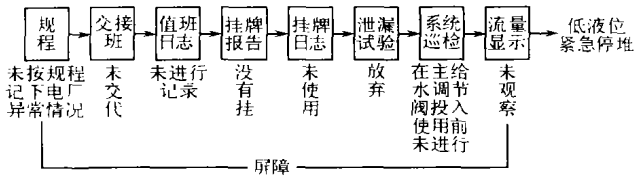

图 3 核电厂 SG 人因事件屏障分析图

进行观察。

4.4 确认根本原因

根据上述分析从以下角度确认事件发生的根本原因：书面交流，接口设计或设备状态，人员工作实践，管理方法，监督方法，工作组织、计划。

4.5 制定纠正措施

通过上述分析，可以提出对失效屏障的修补方法，预防同类事故的重复发生。例如：

(1) 强化安全管理。通过安全管理措施，建立多重安全屏障，能有效地减少人因失误的可能性。

(2) 改善人机接口，提高设备安全性能。

(3) 加强人员技能培训，提高操作人员水平。

(4) 加强企业安全教育，提升安全文化[4]。

(5) 应用先进的事故分析技术寻求事故的根本原因和其相关因素，采用最优的防范策略，预防同类事故的再度发生。

5 结束语

复杂工业系统中人因事故根本原因的分析对于防范复杂系统中人因事故的发生是非常必要的。对于这种系统中人因事故的防范，采取以往基于多米诺骨牌原理[5]的策略可能是无助的，而采用 E&CF 图结合屏障分析的方法对人因事故进行分析，是基于复杂工业系统本身的特点(多任务、多系统、复杂人员组织机构和相关设备条件)采取的一种行之有效的方法[6]。通过寻找根本原因，建立多层重叠设置的安全防护系统构成多道防线，使得即使某一防线失效也能被其他防线弥补或纠正。

将技术手段与组织手段、文化手段相结合，从管理决策、组织、技术、事故分析与减少、反馈等过程和层面构建主动型人因事故纵深防御系统，主动去探查与辨识可能的人因事故，并采取技术、组织和文化相结合的措施去减少和预防。这种方法已经在国际复杂工业系统(民航、核电、化工等)人因事故分析和事故防范中广泛采用[7]。

(收稿：2003 年 6 月；作者地址：湖南省衡阳市常胜西路；南华大学人因所；邮编：421008)

参 考 文 献

1 张力等. 人因分析：需要、问题和发展趋势[J]. 系统工程理论与实践，2001，21(2)：167～172

2 张力等. 复杂人－机系统中的人因失误[J]. 中国安全科学学报，1996，6(6)：35～37

3 张力，黄曙东等. 人因可靠性分析方法[J]. 中国安全科学学报，2001，11(3)：6～16

4 陈宝智、王金波主编. 安全管理[M]. 天津：天津大学出版社，1999.9

5 张力等. 人因事故纵深防御系统模型. 南华大学学报，2001，2(1)：31～34

6 Swain A D, Guttmann H E. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application[S]. NUREG/CR－1278, 1983

7 Mark Kearney, Michael Llewellyn, WANO Event Investigation Training, WANO OE Central Team, WANO-Paris Center[S], 2001