



核电厂事件序列的分阶段分析

玉 宇,童节娟,刘 涛,赵 军,张阿玲

清华大学核能与新能源技术研究院,北京 100084

摘要 概率安全评价(PSA)常用的技术手段是事件树(ET)结合故障树(FT)的分析方法,由于 ET/FT 都是以布尔逻辑为基础的静态分析技术,对于事件发生时间不同所引起事故进程的变化缺乏足够的处理能力。然而,事件发生的准确时间对确定事故情景的发展有时是十分关键的。本研究针对压水堆核电厂丧失主给水后辅助给水系统失效时间对事故进程的影响,采用可靠性框图和事件树方法,分阶段对该事故序列进行评价,结果表明,此事故进程中,提高操纵员执行 U1 规程的可靠性有利于降低本事故情景下发生堆芯损坏的可能性。简要分析了该方法的适用性。

关键词 分阶段;事故序列;系统可靠性;故障树;事件树

中图分类号 TL364+.4

文献标识码 A

文章编号 1000-7857(2009)15-0083-04

Accident Analysis by Phase-mission Methods in Nuclear Plant

YU Yu, TONG Jiejuan, LIU Tao, ZHAO Jun, ZHANG Aling

Institute of Nuclear and New Energy Technology, Tsinghua University, Beijing 100084, China

Abstract Probabilistic Safety Assessment (PSA) is a systematic engineering evaluation technology, widely used in the nuclear power plant safety evaluation. In PSA, the Event Tree (ET) and Fault Tree (FT) are commonly used. However, it is common that a mission in different phases is executed by different systems or function modules in an engineering project. Conventional ET/FT are static analysis methods based on Boolean logic technology, not flexible enough to handle the dynamic problems directly, e.g. to change the accident scenario evolution at different stages. Sometimes the accurate timing of the events is important for the accident sequence development. The method to evaluate the accident sequence in different phases can be used to solve the problem. The basic idea of this method is to convert the multi-phase system to several single-phase systems to be analyzed separately, and then the results are combined to get the final consequence. Reliability diagram and event tree are two of the important analysis methods for phased analysis. In this paper, they are used to analyze the accident of loss of the main feed water in different phases. It is shown that to

improve the reliability of execution process, U1 can help to reduce the probability of core damage in this accident. At last, the applicability of the two methods are discussed briefly. In the reliability diagram, since the real condition of the accident cannot be reflected completely, the illogical cut set should be deleted by hand. In the event tree, since the logical order can be partially reflected, the illogical cut set can be avoided. The two methods are both based on FT or ET eventually, so the accident development with the time cannot be described entirely, and the result is conservative. When the mission time is short, this deviation can be accepted.

Keywords phased analysis; accident event sequence; system reliability; fault tree; event tree

0 引言

目前,概率安全分析技术(Probabilistic Safety Assessment, PSA)作为一种系统化的安全分析技术,已在核电站安全评价中得到了广泛应用。事件树/故障树分析方法作为其常用的技术手段,已发展得相当成熟。在实际工程中,事故处理不同阶段的任务由不同系统、不同人员响应组合完成的情况是一种常见现象。而传统的故障树与事件树都是以布尔逻辑为基础的静态分析方法,对于事件发生时间不同所引起事故进程的变化缺乏足够的处理能力。事件发生的准确时间对确定事故情景的发展有时是十分关键的。因此,研究这种在事故发展的不同阶段需要不同的人员响应或系统响应的情况是有意义的。然而,针对此种情况,目前并无成熟的分析方法。相关文献^[1-4]中提出的针对在不同阶段需由不同单元完成系统

收稿日期:2009-06-05

作者简介:玉宇,助理研究员,研究方向为概率安全评价,电子信箱:yu-yu@mail.tsinghua.edu.cn



任务的分阶段处理方法,基本方法是分阶段建立可靠性框图或故障树,然后进行求解。其基本思想^[5-6]是将多阶段系统转化为多个独立的单阶段系统,用单阶段分析方法逐一求解后再做综合;而传统的事件树分析方法^[7],也可用于分阶段求解。以上分阶段求解的分析方法在航空、军事等领域^[8-9]已有相当的发展和运用,其思路具有借鉴意义,但在核电厂的实际事故处理过程中,人员行为或系统响应是随着事故过程的演变而发展变化的,因此后续阶段的逻辑模型与这一阶段起点的系统状态有关,上述方法应用于核电厂的事故处理过程分析时,需要根据实际情况适当修正。本研究采用以上方法对核电厂事故序列进程评价,并对结果适当分析修正。

1 事故序列

丧失主给水是压水堆核电厂较常见的一类始发事件,三哩岛事故后,人们对此类事故更加重视。为了对核电厂事故序列中在事故发展不同阶段,需要不同人员响应或系统响应这一特性进行分析,本研究以此事故序列为例进行说明。丧失主给水事件发生后,有下列缓解手段:① 辅助给水系统(ASG)运行,事故缓解;② 辅助给水系统在某时刻 t_1 前运行失败,执行规程 H2,安全注入系统(RIS)运行且稳压器安全阀开启,事故缓解;③ 辅助给水系统在某时刻 t_1 后运行失败,执行规程 U1,安全注入系统运行且稳压器安全阀开启,事故缓解。

2 可靠性框图分析

本事故分析中,辅助给水系统失效,则必须通过人员执行充-排操作,事故才能得到缓解。而辅助给水系统失效发生的时间不同,人员响应不同(执行 H2 规程或 U1 规程)。为分析方便,将缓解步骤抽象为几个单元:① 始发事件:单元 I;② 辅助给水系统:单元 A;③ 执行 H2 规程:单元 H;④ 执行 U1 规程:单元 U;⑤ 安全注入系统运行:单元 R;⑥ 稳压器安全阀打开:单元 S。对上述过程,建立可靠性框图(图 1)。

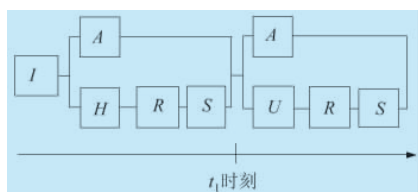


图 1 丧失主给水事故序列可靠性框图
Fig. 1 Reliability diagram for accident sequence of loss of the main feed water

采用文献[2]介绍的方法,首先将图 1 中事件 I 发生后的缓解功能转化为系统任务故障树,0 时刻始发事件发生,此后到 t_1 时刻为第 1 阶段(phase 1), t_1 时刻以后为第 2 阶段(phase 2)(图 2)。

将图 2 所示的多阶段系统转化为多个独立的单阶段系统,用单阶段分析方法逐一求解后再做综合^[2],其过程如下:
① 任务割集消减:如果当前阶段与此后阶段包含同一最小割

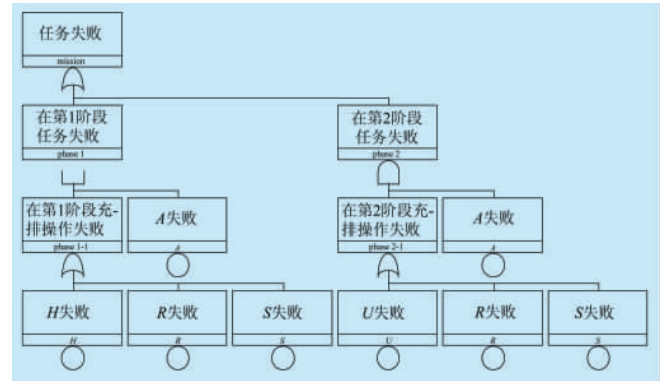


图 2 系统任务故障树

Fig. 2 Fault tree of the system mission

集,则将当前阶段中的割集消除;② 基本事件转化:用一组基本事件 $C_{K1}, C_{K2}, \dots, C_{Kj}$ 代替阶段 j 中的基本事件 C_K ;③ 转化后得到一个等效的单阶段系统,该系统包含新的逻辑序列,原系统各阶段成为该系统的子系统;转化后第 1 阶段任务故障树中的基本事件 A 由 A_1 代替, A_1 表示在第 1 阶段事件 A 发生,转化后的系统任务故障树见图 3;④ 求新故障树的最小割集。最后由常用的故障树定量评估方法从各阶段的最小割集得到全系统的不可靠度。

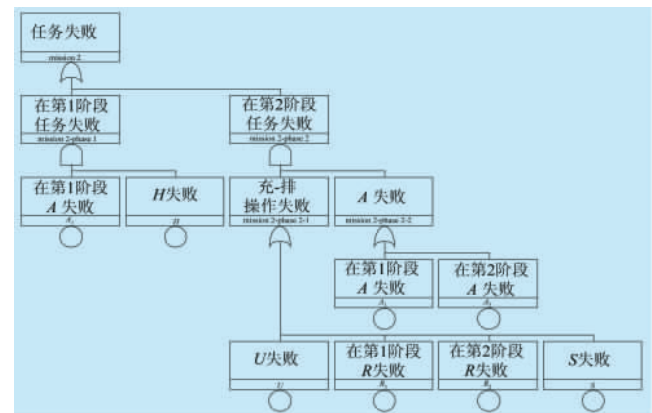


图 3 转化后的系统任务故障树

Fig. 3 Fault tree of system mission after transform

由于单元 A、R、S 都是系统,而故障树方法的任务时间是固定的,所以上述故障树无法一步计算,只能先分别计算出 A_1, A_2, R_1, R_2, S 的值;再代入转化后的系统任务故障树中,得到系统任务失效概率为 8.58×10^{-6} ,得到的 9 个割集为 $\{A_2, U\}$, $\{A_1, U\}$, $\{A_1, H\}$, $\{A_2, R_2\}$, $\{A_1, R_2\}$, $\{A_2, R_1\}$, $\{A_1, R_1\}$, $\{A_2, S\}$, $\{A_1, S\}$;再结合始发事件频率,得到堆芯损坏频率 CDF 为 4.3×10^{-6} (堆·年)。显然,结果中存在不合理的割集 $\{A_1, U\}$,这是由于图 1 与图 2~图 3 中的逻辑反映的是只要单元 A 失败,在第 2 阶段中就要执行分支 $\{U, R, S\}$,这并不能完全真实地反映事件序列的发展,因为如果 A 是在第 1 阶段中失败的,则在第 2 阶段并不需执行单元 U。

而分阶段分析方法通常假设系统在特定阶段的逻辑模

型是不改变的^[7],因此在此处分析中,需要去掉该不合理割集,结果修正为 $CDF=2.57\times 10^{-6}/(\text{堆}\cdot\text{年})$,但此结果未能考虑到共用系统的影响。

由于单元 A 与 R 存在共用系统, 下面先针对割集 $\{A_2, R_2\}$ 、 $\{A_2, R_1\}$ 、 $\{A_1, R_2\}$ 、 $\{A_1, R_1\}$ 进行逻辑计算

$$\{A_2, R_2\} + \{A_2, R_1\} + \{A_1, R_2\} + \{A_1, R_1\} = \{A, R\}$$

再对割集 $\{A, R\}$ 采用故障树进行计算, 得割集发生概率为 6.92×10^{-6} , 再与另外 4 个割集 $\{A_2, U\}, \{A_1, H\}, \{A_2, S\}, \{A_1, S\}$ 相加, 得系统任务失败概率为 1.16×10^{-5} , CDF 为 $5.8 \times 10^{-6}/(\text{堆} \cdot \text{年})$; 其中, 割集 $\{A_2, U\}$ 的贡献大于 50%, 即丧失辅助给水后操作员执行 U1 规程失败是该事故序列中导致堆芯损坏的主要贡献因素。因此, 提高操纵员执行 U1 规程的可靠性有利于该事故情景下降低堆芯损坏概率。

3 事件树分析

采用事件树方法对事故序列进行分析, 事件树图如图 4 所示, 简化后的事件树图如图 5 所示。

对图 4 中事件树求解,共得到 7 个割集: $\{A_1, H\}$, $\{A_1, R_1\}$, $\{A_1, R_2\}$, $\{A_1, S\}$, $\{A_2, U\}$, $\{A_2, R_2\}$, $\{A_2, S\}$ 。该方法求得的割集中就不存在不合理的割集 $\{A_1, U\}$ 和 $\{A_2, R_1\}$ 。但需注意,由于 A_1 , A_2, R_1, R_2 的任务时间不同,该事件树仍然不能直接计算,而需要分别计算以上 4 个元素的值,再进行综合。这里的 $P(A_2)$ 不能直接建立故障树计算,因为 A_2 并不是指 A 在第 2 阶段投入,而是指 A 在第 2 阶段失效的概率(A 是在 0 时刻就投入的),即 A 在第 1 阶段启动、运行成功,而在第 2 阶段运行失效的概率,所以不能把 A 的任务时间改为 t_1 时刻至 24 h 这一阶段的时间直接用故障树计算,而是

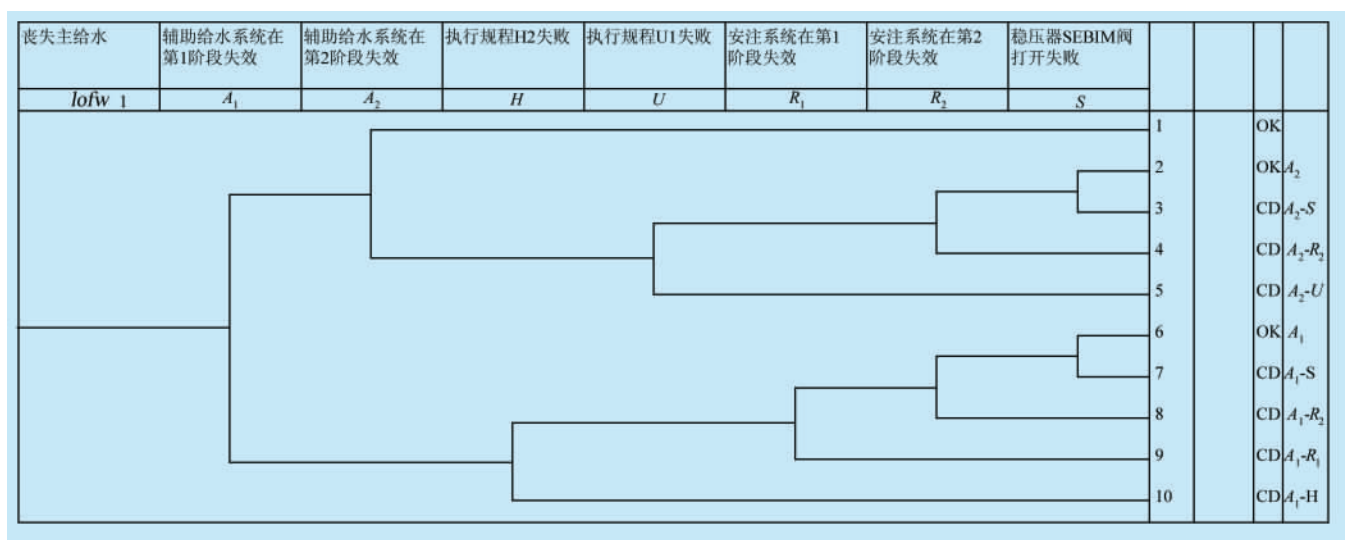


图 4 丧失主给水事件树图

Fig. 4 Event tree for accident sequence of loss of the main feed water

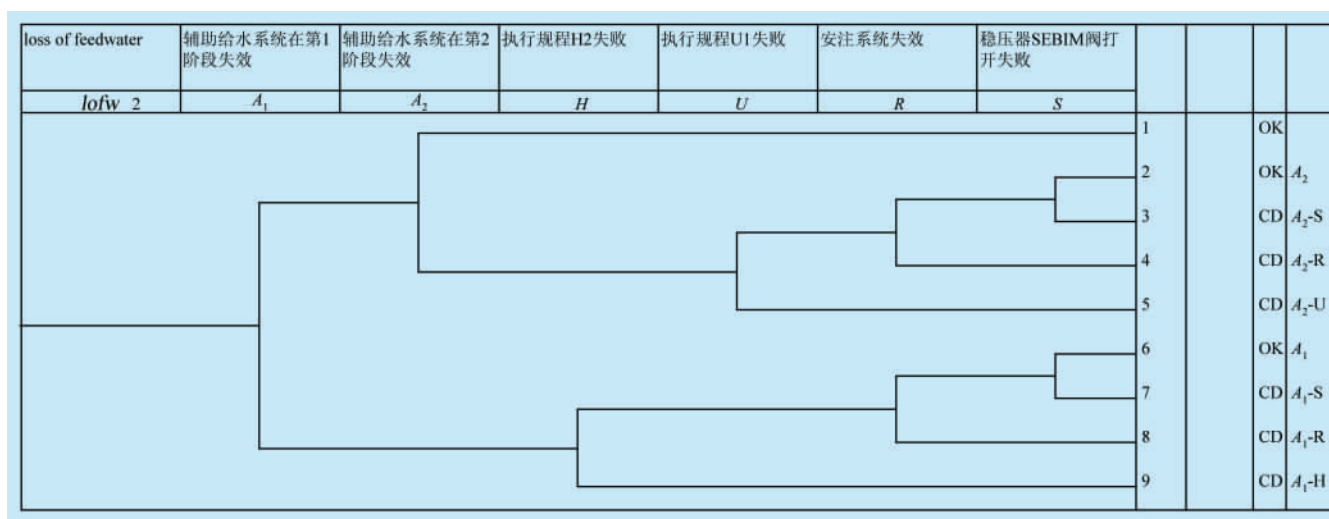


图 5 简化后的事件树图

Fig. 5 Event tree after simplification

$$P(A_2)=P(A)-P(A_1)$$

产生此问题的原因并不是 A 在不同阶段执行不同功能,而是 A 失效后的影响不同。且 A 与 R 之间存在共用系统问题,所以以上割集中 $\{A_2, R_2\}$ 不能直接计算,仍需先进行逻辑计算

$$\{A_2, R_2\} + \{A_2, R_1\} + \{A_1, R_2\} + \{A_1, R_1\} = \{A, R\}$$

而后对割集 $\{A_1, H\}$, $\{A_1, S\}$, $\{A_2, U\}$, $\{A_2, S\}$ 和 $\{A, R\}$ 进行计算求解。公式中, $\{A_2, R_1\}$ 虽然是不合理的割集,但由于其值无法准确计算,只能按照 ET/FT 中的分析方法,做保守处理。

通过分析可以看出,对此类问题,采用事件树方法分析,可以避免出现不合理的割集,这是因为事件树本身可以反映一定的逻辑顺序,但毕竟是以布尔代数为基础的静态逻辑分析方法,因此不能完全反映事件序列发展随时间的变化。

其实,这里区分 R_1 和 R_2 并无实际意义,因为分阶段方法的意义在于可以描述 A 在不同阶段失效的影响,这体现在执行 H2 规程或 U1 规程;而该方法并不适合于精确描述 A 失效时间不同, R 任务时间不同这一动态过程,对于该过程还是作保守处理的;在任务时间较短的情况下,此种保守分析方法所引起的偏差是可以接受的。因此事件树可简化为如图 5 所示。这样可以得到 6 个割集: $\{A_1, H\}$, $\{A_1, R\}$, $\{A_1, S\}$, $\{A_2, U\}$, $\{A_2, R\}$, $\{A_2, S\}$, 同样先进行逻辑计算后,再进行割集定量计算综合。

4 结论

采用分阶段分析方法、可靠性框图方法或事件树方法,均可针对在事件序列发展的不同阶段、需要操纵员执行不同操作的情况进行分析,并获得精确解,本例为 5.8×10^{-6} (堆·年)。

采用分阶段分析方法,最终归结到故障树或事件树计算,可利用现有的分析软件,便于应用。但也正因为分阶段分析方法最终仍然要归结到故障树或事件树计算,因此不能完全反映事件序列随时间的动态演变过程,对于事件序列的动态特性需要根据实际情况进行修正。

提高操纵员执行 U1 规程的可靠性有利于降低本事故情景下发生堆芯损坏的可能性。

参考文献 (References)

- [1] 谢红卫, 宫二玲, 贺勇军. 时变结构多阶段任务系统的可靠度研究[J]. 国防科技大学学报, 1999, 21(5): 41-45.
Xie Hongwei, Gong Erling, He Yongjun. *Journal National University of Defense Technology*, 1999, 21(5): 41-45.
- [2] 邢涛. 多阶段任务系统可靠性建模研究 [J]. 海军航空工程学院学报, 2006, 21(1): 172-174.
Xing Tao. *Journal Naval Aeronautical Engineering Institute*, 2006, 21(1): 172-174.
- [3] 陈玉波, 于永利, 张柳, 等. 多阶段任务系统(PMS)可靠性模型研究[J]. 系统工程与电子技术, 2006, 28(1): 146-149.
Chen Yubo, Yu Yongli, Zhang Liu, et al. *Journal of Aerospace Electronics Information Engineering and Control*, 2006, 28(1): 146-149.
- [4] Ma Y, Trivedi K S. An algorithm for reliability analysis of phased-mission systems[J]. *Journal of Reliability Engineering and System Safety*, 1999, 66: 157-170.
- [5] Murphy K E, Carter C M, Malerich A W. Reliability analysis of phased-mission systems: A correct approach [C]//Proc 53rd Reliability and Maintainability Symposium. NJ: IEEE Press, 2007: 7-12.
- [6] Alam M, Song M, Hester S L, et al. Reliability analysis of phased-mission systems: A practical approach [C]//Proc 52nd Annual Reliability and Maintainability Symposium. NJ: IEEE Press, 2006: 551-558.
- [7] Xue D, Wang X. A practical approach for phased mission analysis[J]. *Journal of Reliability Engineering and System Safety*, 1989, 25: 333-347.
- [8] Jia Z, Kang R, Wang N, et al. Complicated mission success modeling of the partially repairable system [C]//Proc 8th International Conference on Reliability, Maintainability and Safety. NJ: IEEE Press, 2009: 249-252.
- [9] Wei J, Dai G, Li F. Research of warship total mission reliability modeling based on unit mission[C]//Proc 8th International Conference on Reliability, Maintainability and Safety. NJ: IEEE Press, 2009: 260-263.

(责任编辑 赵佳)

·学术动态·

“2009 园艺科学与技术学术会议”征文



中国园艺学会拟于 2009 年 12 月 12-13 日在北京市召开“2009 园艺科学与技术学术会议”。真诚邀请园艺及其相关领域的专家学者、研究人员积极参与,共同探讨、研究园艺行业的最新理论技术及其实际应用,推动园艺向高科技化、产业化、信息化方向发展。

征文内容包括:园艺育种的最新技术及研究进展,设施园艺与观光农业,设施园艺的关键技术,温室环境控制技术,有机园艺,园艺疗法,现代化栽培技术和作物产后加工、储藏、处理技术研究,病虫害防治技术与安全生产,观赏园艺与园林,园艺的产业化及可持续发展。会上将评出一定数量的优秀论文,由组委会颁发获奖证书。

会议只接受英文文章,论文集将由英国学术出版集团出版,论文集送 ISTP 检索。征文截稿日期:2009 年 9 月 29 日。详见会议网址:www.chst2009.org。

联系方式:中国园艺学会 李老师;电话:010-81792490;电子信箱:chst-2009@163.com。