文章编号:1001 - 2486(2005)01 - 0098 - 04

基于概率风险的系统安全性分析*

董豆豆,周经伦,冯 静,龚时雨,周忠宝
(国防科技大学 人文与管理学院,湖南 长沙 410073)

摘 要:为得到系统层次上的安全性概率风险,获得定量的安全性决策依据,设计了基于概率风险的系统安全性分析方法,该方法将系统按某种标准划分成相应子系统,统计得到各子系统所有的危险源,建立相应的因果链,通过一定法则得到基于系统层次的概率风险,同时还讨论了设计方法中概率风险计算的难点问题。

关键词:安全性;概率风险;危险源;因果链
中图分类号:O211.9;E917 文献标识码:A

The Analysis of System Safety Based on Probabilistic Risk

DONG Dou-dou, ZHOU Jing-lun, FENG Jing, GONG Shi-yu, ZHOU Zhong-bao
(College of Humanities and Management, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: In order to get the risk on the level of system and to obtain the quantitative decision reference of safety, this paper proposes an analytic method of system safety based on probabilistic risk. This method will divide the system into different subsystems according to some criterion, count the danger sources of all subsystems and build causality diagrams corresponding to danger sources, and at last compute the probabilistic risk on the level of system according to some rules. The difficult problem of computing the probabilistic risk by this method is discussed.

Key words: safety; probabilistic risk; danger source; causality chain

重大事故不仅带来经济上的严重损失,而且也伴随着重大人员伤亡和恶劣的政治影响,因此安全性问题越来越得到重视。但随着大型设备系统复杂性的增加,安全性问题的合理解决必须依据系统工程的思想,建立完整的安全性分析方法,从而在实践中指导系统安全性的设计,或给决策者提供定量的决策依据。

但在当前的研究与实践中[1,2],大部分工作都集中在消除安全性的隐患,将注意力放在系统的各个部件上,而没有从系统层面上来定量分析系统的安全性。作为最终的决策者,尤其是重大设备的使用决策者,更关心和需要的是系统运行时系统层面上的安全性风险,而不是子系统或某个部件,即高级别的决策者更关心的是系统,而不是其中的某个组件。例如在发射卫星时,决策者更想要知道发射时出现事故的概率风险是多少。

1 安全性分析的主要概念

1.1 危险、危险源及危险表的建立

危险是一种可能导致事故的潜在条件或状态,它是系统或环境的一个特征。危险可以引发事故,但必须在一定的条件下,并经历一个演变过程,即系统状态变化的过程。因此,事故分析的实质是对危险演变过程、传播时间、可观察到的危险征兆以及对危险事件后果严重性级别判断的过程。

与系统相关的危险源可根据类似的和前一代系统的分析及经验数据来确定。根据初步确定的危险源列出危险源清单,作为危险分析的第一步。

* 收稿日期:2004 - 08 - 29
基金项目:国家部委基金资助项目
作者简介:董豆豆(1976—),男,博士生。

后果是危险演变的结果,即危险事件对人员、财产、系统或生态环境产生的伤害、损失、损坏或影响。后果的严重程度用严重性来度量。对后果严重性的规定有不同的标准。GJB900 中规定了严重性等级(见表 1)。

表 1 后果严重性等级

Tab. 1 Grades of result severity

等级	等级说明	事故后果说明
Ⅰ	灾难性的	人员死亡或系统报废
Ⅱ	严重的	人员严重受伤、严重职业病或系统严重损坏
Ⅲ	轻度的	人员轻度受伤,轻度职业病或系统轻度损坏
Ⅳ	轻微的	人员受伤和系统损坏轻于Ⅲ级

另外一个重要的概念是危险事件。危险事件是一种不希望的系统状态变化的现象。它反映系统功能或物理破坏的特征。危险事件可能性等级是对危险事件发生的频繁程序的度量。定性的危险事件发生可能性等级分为五级,见表 2。

表 2 危险事件发生可能性等级

Tab. 2 Probability grades of dangerous events

等级	等级说明	个体发生情况	总体发生情况
A	频繁	频繁发生	连续发生
B	很可能	在寿命期内会出现若干次	频繁发生
C	有时	在寿命期内可能有时发生	发生若干次
D	极不	在寿命期内不易发生,但有可能发生	不易发生,但有理由可预期发生
E	不可能	很不容易发生,以至于认为不会发生	不易发生,但有可能发生

1.2 因果链的建立

可以将事故发展过程看作是由一系列的事件所组成的一个事件链,事件链由初始事件、中间事件和后果三部分组成。其中,初始事件是一种导致一系列事件发生或系统状态变化开始的事件,包括由人为差错、硬件软件故障、环境因素所引起的危险事件;中间事件表示那些可能进一步恶化而不希望出现的危险事件或一些控制的紧急应付和缓解措施。

事件链采用事件序列的表达方式,简单明了地反映了事故过程及其因果关系,有时称之为因果链。一般来说,一个初始事件可能会导致几种后果,或若干个事件链可能包含一个相同的事件,如图 1 所示。

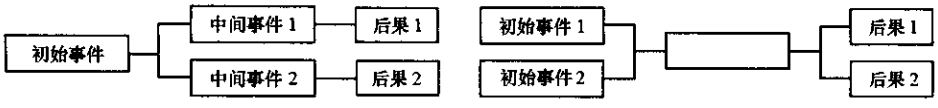

图 1 事件链的两种常用形式

Fig. 1 Two common-used forms of event chains

构造事件链的步骤:首先确定初始事件,然后通过询问方式确定每一个后面的事件。通常可以通过询问下面的问题来确定事件链:

(1) 在何种条件下这一事件会导致其它进一步的事件?

(2) 何种替代的条件下导致不同的事件?

(3) 该事件会影响到何种其它事件?会影响到不止一种事件吗?

(4) 该事件会导致什么样的进一步事件呢?

1.3 故障树的建立

可以将事件链中的中间事件作为故障树的顶事件来建立故障树。在文献[3]中,电机过热是导致事故发生的一个中间事件,对于这一事件,可以建立其故障树,如图 2 所示。

同样,每一个关键的中间事件都可以被作为顶事件建立故障树。各种具体故障的概率通常可以由专家和经验数据得到,所以顶事件的故障概率可以通过故障树求得。计算出的顶事件概率就是每一个中间事件的发生概率。由故障树底事件的发生概率计算出顶事件的概率,是一种自底向上的思想。

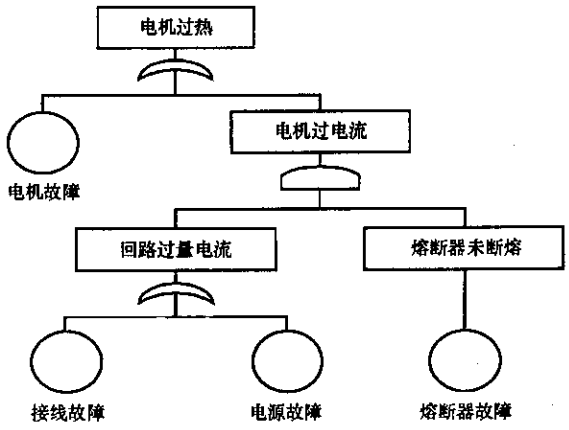

图 2 电机过热的故障树

Fig. 2 Fault tree for overheated generator

2 基于系统安全性概率风险定量分析方法设计

基于系统安全性概率风险定量分析方法可以按如下步骤进行:

首先,将要进行安全性概率风险分析的系统按一定的标准划分为相应的子系统,分别为{SubSystem1, SubSystem2,…,SubSytem$N$},见图 3。根据系统的具体情况,可以再进行深层次划分。

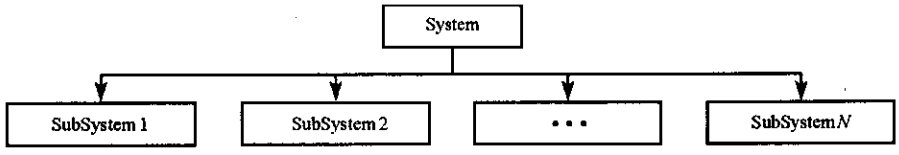

图 3 系统结构图

Fig. 3 Structure diagram for the system

再次,根据所有子系统的危险表,收集所有的危险源,从而形成危险源集 $D=\{d_1,d_2,\cdots,d_i,\cdots,d_n\}$。接下来,对每一个危险源根据其初始事件进行危险导致事件的逻辑分析,从而形成相应的事件链,即因果链。但在实际的分析中,这些因果链通常会形成一个网络,有些中间事件可能会在因果链中重复出现。在计算概率风险时,需要对这些重复出现在因果链中的中间事件进行不交化处理,这将在下一节进行论述。

对于每一个激发危险源 d_i 的引发事故,分析事故后可以得到一个结果。可以采用一个四元组来描述危险后果,即 $R_i(X_i,I_i,U_i,P_i)$。其中,R_i 表示危险,X_i 是用来描述危险后果的文字变量,I_i 表示危险后果的严重性等级,U_i 表示危险后果的效用,P_i 表示危险发生的概率。

设系统的概率风险为 P_s,由于危险有不同的严重性等级,所以可以将不同严重性等级的系统概率风险用 $P_{s\mathrm{I}}$,$P_{s\mathrm{II}}$,$P_{s\mathrm{III}}$ 表示,分别表示一级危险的概率、二级危险的概率和三级危险的概率(这里只列出了前三级的危险概率)。对于 $P_{s\mathrm{I}}$,即对应于一级危险的系统概率风险,有

$$P_{s\mathrm{I}}=P(R_{\mathrm{I}1}\cup R_{\mathrm{I}2}\cup\cdots\cup R_{\mathrm{I}i}\cup\cdots\cup R_{\mathrm{I}n})$$

其中 $R_{\mathrm{I}i}$ 表示第 i 个一级危险($i=1,\cdots,n$)。对于其它级别的概率风险可以类此计算。

最后可以通过对三个级别概率风险进行合成得到系统的概率风险。为了体现各个级别的影响因素,可根据需要引入权重因子,有

$$P_s=P_{s\mathrm{I}}\oplus P_{s\mathrm{II}}\oplus P_{s\mathrm{III}}$$

其中$\oplus$表示一种加权合成运算,可根据需要对$\oplus$的运算规则进行定义,从而可以得到系统层面上的安全概率风险 P_s,此值可以作为决策的定量依据。

3 系统概率风险计算难点分析

危险源集 $D=\{d_1,d_2,\cdots,d_i,\cdots,d_n\}$,其中,$d_i$ 对应于一个因果链,如图 4 所示。因果链中的事件概率可通过参考文献[4,5]中的方法得到。

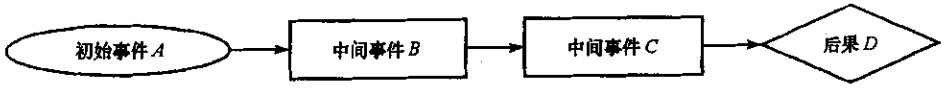

图4 d_i 所对应的事件因果链

Fig. 4 Event chains for d_i

通常在工程中,不同的因果链会经历同一个中间事件,从而导致在计算后果的终态概率风险时产生重复的计算。为了消除重复计算的影响,需要进行不交化的处理。这里举例说明中间事件的重复存在和不交化处理的原理。设初始事件和中间事件为 A_1,A_2,A_3,这些事件所导致的结果为 D,其因果链可以用图5表示。

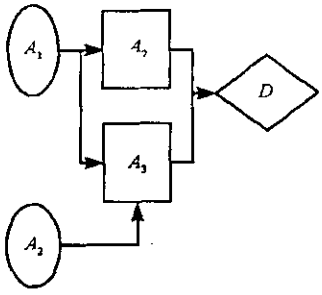

图5 初始事件和中间事件 A_1,A_2,A_3 对应的因果链

Fig. 5 Event chains for A_1,A_2,A_3

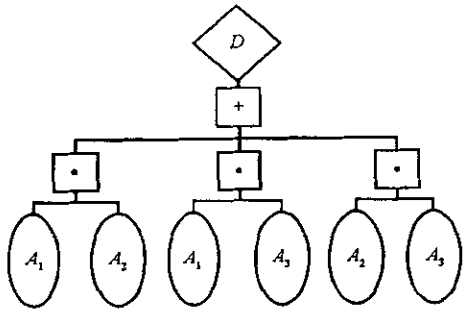

图6 因果链的另一种表示形式

Fig. 6 Another display for event chains

为方便理解,可以将图5所示的因果链表示为图6。由图6可知,因果链的结构函数 $\Psi(D)$ 可以用下式表示:

$$\Psi(D) = A_1A_2 + A_1A_3 + A_2A_3$$

如采用通常的方法根据上式求终态 D 的发生概率,假设式中有 n 项,利用普通概率和公式去求解时会产生 2^n 个分项。随着 n 的增大,分项的数目会增大到难以容忍的地步。针对这个问题,可以利用不交化的方法[6]对上式进行求解。从而可以得到上式的结果为:

$$\Psi(D) = A_1A_2 + A_1A'_2A_3 + A'_1A_2A_3$$

其中,A'表示 A 的补集。

由于 A_1A_2,$A_1A'_2A_3$,$A'_1A_2A_3$ 是互斥的,所以终态 D 的概率可以直接算出,即

$$P(D) = P(A_1A_2) + P(A_1A'_2A_3) + P(A'_1A_2A_3)$$

4 结论

在系统层面上从安全性角度分析系统的概率风险对于保证系统的安全设计和使用有着重要的意义。基于此,设计了基于概率风险的系统安全性分析方法,并讨论了计算概率风险中的难点问题,即用不交化的方法去消除重复中间事件对概率风险结果的影响。利用此方法得到的系统层面上的概率风险可作为工程安全人员决策时重要的定量依据。

参考文献:

[1] Christian P. Safety Risk Assessment and Management—the ESA Approach[J]. Reliability Engineering and System Safety,1995,49:303-309.

[2] Pate-Cornell E, Dillon R. Probabilistic Risk Analysis for the NASA Space Shuttle: A Brief History and Current Work [J]. Reliability Engineering and System Safety,2001,74:345-352.

[3] 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,2003:18-25.

[4] Jaynes E T. Prior Probability[J]. IEEE Tran. on Systems Science and Cybernetic. SSC-4, 1986:227-241.

[5] Stein C. Approximation of Improper Measures by Prior Probability Measure [M]. In Bernoulli-Bayes-Laplace Festschr, Springer-Verlag, New York, 1965:217-240.

[6] 梅启智,廖炯生,孙惠中. 系统可靠性工程基础[M]. 北京:科学出版社,1987:201-203.