陈志业　萱　铸　主编

安全系统工程在火力发电厂应用丛书

事件树分析方法

陈志业　邓庆松　王殿昌　编著

北京科学技术出版社

序　言

安全系统工程是近十多年来发展起来的一门软科学技术，它采用系统工程的方法和计算机技术，分析和评价生产过程中的不安全因素，揭示其规律，确定安全决策和预防措施，达到控制事故之目的。安全系统工程这门新兴科学，正日益为人们所接受，为安全管理工作现代化开辟了新的途径。

安全系统工程在火力发电厂应用丛书，是由华中电管局、河南省电力局、华北电力学院、湖北省电力试验研究所、河南焦作电厂等单位组成的“水电部安全系统工程课题组”编写的。该书总结了近几年来国内外研究的最新成就，介绍了课题组结合火力发电厂实际应用所取得的新成果：安全检查表、典型故障树、计算机算法等，具有较强的实用性。焦作发电厂的实践经验表明，采用安全系统工程的方法，指导安全管理，使企业安全生产面貌有所改善，经济效益得到明显提高，打破了事故不可知论的传统观念，为电业生产贯彻“安全第一、预防为主”的方针提供一种新的手段。

安全系统工程在火力发电厂应用丛书现分五册出版，由陈志业和董铸同志主编。

《安全检查表的编制与应用》由卫阳山、冀国全、邵春芝编著。

《故障树的编制与应用》由邓庆松、郭新华、马献图编著。

《故障树分析与计算机算法》由陈志业、王平、董铸编著。

《故障数据库与安全评价》由郭新华、王忙虎、荀吉辉编著。

《事件树分析方法》由陈志业、邓庆松、王殿昌编著。

本丛书可作为电力系统和其它行业、大专院校、科研单位广大工程技术人员、工人、学生、科研人员和领导干部的参考读物。

本丛书在编写过程中得到有关专家、学者和关心该书出版的王强司长、杨以涵教授、张翼鹏高工、曾令文高工、杨振鹏副教授、梁秉鲁高工、陈家玠高工、张光明工程师、杨效生工程师、孙书立工程师等的大力支持。同时在安全检查表及故障树的编制过程中，得到焦作电厂的张明德副厂长、曹允冲副厂长、区嘉荣总工程师、毋济安科长、熊克学主任、蒋桂韵主任、杨心瀛主任、刘根堂主任等领导及广大职工的大力协作，在此深表感谢。

由于作者水平有限，错误和不足之处在所难免，敬请广大读者批评指正。

编　者

1988年7月

目　　录

第一章 概 论

安全系统工程主要有系统安全分析、安全评价和安全措施等三个方面的内容。通过对系统进行细致的分析，充分认识系统存在的危险性，以便进行安全评价进而制定并采取优化的安全措施，对系统进行调整，对薄弱环节加以修正，提高系统的安全性。

系统安全分析在安全系统工程中占有十分重要的作用，目前已发表的分析方法就有数十种之多，它们从不同的角度对系统的安全性进行分析，人们可以根据实际情况选取某种方法或综合使用一些分析方法以满足安全分析的需要。在应用实践中，一般认为安全检查表、故障类型和后果影响分析、事件树分析和故障树分析法等较为实用，目前已在一些行业得到应用。

由于安全检查表、事件树分析和故障树分析方法理论完整，应用经验多，因而在电力系统，特别是在火力发电厂中采用这些方法是较为适宜和有效的。本丛书第一、二两分册已分别介绍了安全检查表和故障树分析方法的原理和应用，本分册将对事件树分析方法进行介绍。当然，读者在此基础上还应多了解一些其它分析方法的内容和特点，以便能得心应手地综合使用各种方法，取长补短，有效地进行安全分析，指导安全生产。

第一节 概率安全分析与事件树分析

随着工业生产向着大规模、高技术的特点发展，生产过

程能量剧增。高速、高压、高温、高度自动化，连续作业以及设备庞大，决定了生产过程潜在的危险性增大，损失严重性增大，迫使人们重新研究安全和损失问题，推动了事故和损失的预防技术的发展。安全系统工程就是以系统工程的方法研究和解决生产过程中安全问题的。

安全系统工程这门新学科之所以能迅速地得到发展是因为她使用了各种学科的知识，对生产过程中的不安全因素进行分析、评价，既可进行定性分析，又可以进行定量分析，打破了事故不可知论的老概念，使预测和控制事故成为可能。在进行安全分析中，需要分析事件及其发展的过程和后果。研究事件的方法之一，是设计一套在系统寿命周期的适当时候进行的试验，以保证需要时可供利用的有关系统的知识。由于不可能获得百分之百可靠的关于事件及其发生或然率的知识，人们只得接受一种在系统的运行中有某些残余风险的设计，为了评价系统的不可靠程度以及由此给系统及其操作者或使用者留下的残余风险量，安全的分析研究必须依靠统计和概率，对有关系统中故障和事件的概率处理是一个包括可靠性评价和改善的迭代过程。用概率论方法对复杂的可能发生事故的系统进行分析，并估计事故的后果的一种分析方法称为概率安全分析，简称PSA，或称概率安全评价。

任何概率安全分析都要作三部分内容：1）确定目的与规模，以制定PSA分析计划和收资范围，决定PSA做到什么程度；2）初因事件（基本事件）分析，先找出初因事件，然后逐一分析归类；3）功能模化和系统模化。所谓功能模化就是建立事件树，一个初因事件发生往往需要若干系统（或部件）投入工作，才能限制或消除事故后果的严重性，根据初因事件发生后对每个系统（或部件）投入情况进

行分析，看其是否工作正常而能完成某种功能，这样得到的分析图就是事件树。所以事件树实际上是功能树。所谓系统模化就是建立故障树。确定顶上事件后根据系统图找出引起顶上事件发生的全部原因事件，用逻辑门联系起来，形成故障树图。

事件树和故障树建立之后，应用所设计计算程序进行计算，以便求出每一事故序列的发生概率和重要度系数，对系统进行安全分析和评价。

从概率安全分析的过程中可以看出，事件树和故障树分析方法是概率安全分析的基本方法，而故障树和事件树分析方法也是安全系统工程中的重要的分析方法。这是因为安全系统工程作为一种综合了多学科知识的新兴学科，发展非常迅速，十分活跃，人们从不同的角度，根据各自实际情况，应用不同的知识领域创造了多种分析方法。概率安全分析就是以概率论为基础进行安全分析的，因此它也是安全系统工程的一个分支，正因如此，故障树和事件树分析方法成为概率安全分析的基本方法也是很自然的了。

第二节　决策树与事件树

事件树分析是从决策树引伸而来的一种分析方法，决策树是决策论中的一种决策方法。所谓决策，就是为解决当前或未来可能发生的问题，选择最佳方案的一种过程。人们生活和工作中普遍存在需要决策的情况，小自个人生活，企业管理，大至国家的经济、政治等重大方针，随时需要决策。决策贯彻管理的全过程，也贯彻安全管理的全过程，一项安全管理措施的制定或设备改造计划的确立通常会面对几种不

同情况（决策论中称为自然状态），又可能采取几种不同的方案（决策论中称为行动方案），最后要选定某一方案，即进行决策。

决策问题，根据性质不同，通常分为三类：确定型，不确定型，风险型。

确定型决策问题具备如下4个条件：

1）存在决策人希望达到的一个明确目标；

2）只存在一个确定的自然状态；

3）存在着可供决策人选择的两个或两个以上的行动方案；

4）不同的行动方案在确定状态下的益损值（利益或损失）可以计算出来。

不确定型情况下的决策是自然状态发生的概率不能知道的情况下作出决策，往往不宜作出主观可能性的估计。其决策准则有：乐观准则（最大最大准则），悲观准则（最大最小准则），乐观系数准则和等可能准则等。不确定性的决策缺乏客观标准作为依据，而是依决策者对各种自然状态的看法而定。要改进不确定情况下的决策，必须设法制定各种情况发生的概率，决策的结果可能会更合理一些。

风险型决策问题也叫统计型决策问题，或称随机型决策问题。它具备如下五个条件：

1）存在着决策人希望达到的目标；

2）存在着两个以上的行动方案可供决策人选择，最后只选定一个方案；

3）存在着两个或两个以上的不以决策人的主观意志为转移的自然状态；

4）不同的行动方案在不同自然状态下的相应益损值

可以计算出来；

5）在几种不同的自然状态中未来将究竟会出现那种自然状态，决策人不能肯定，但是各种自然状态出现的可能性（即概率），决策人可以预先估计或计算出来。

对于风险型决策问题，有两种决策准则，一是最大可能准则，它是选择一个概率最大的自然状态进行决策，将风险型问题变成确定型决策问题，二是期望值准则，它是把每个行动方案的期望值求出来，加以比较，根据决策目标的益损要求选取不同的期望值。这里的期望值是指离散型随机变量的数学期望，$E(x)=\sum_{i=1}^{n} p_i x_i$（其中$p_i$为$x=x_i$时的概率）。

益损期望值决策准则可以用决策表进行分析，也可以用决策树进行分析，决策树就是将行动方案和各自然状态用树图的方式罗列出来，构成一个树枝状的图形。其分析的关键步骤有：

1）画决策树，把某个决策问题未来发展情况的可能性和可能结果所作的预测或预计，用树状图形反映出来；

2）预计可能事件发生的概率。概率数值的确定，可凭有关人员的估算或根据过去的历史资料推算，或用特定的预测方法计算；

3）计算益损期望值。利用益损值和它们相应的概率计算出每个方案的益损期望值。

从决策过程中看到，利用了事件的概率，通过期望值这个概念来进行决策的。由于利用了统计规律，因此这样的决策进行多次其成功的决策还是占大多数的，显然比直观感觉或主观想象进行决策要合理得多。决策论就是在做某项工作或从事某项工程之前，通过分析、评价各种可能的结果，权衡利弊，根据科学的判断和预测作出最佳决策的一种系统

的方法论。

在安全管理决策分析中引入决策论，将决策树分析方法引伸为安全系统工程中的事件树分析方法。本节以上简略介绍的决策论和决策树分析方法的理论和分析步骤原则上都可用于事件树分析中，对掌握和运用事件树分析方法是有裨益的。

第三节　事件树分析的基本概念

事件树分析(*Event Tree Analysis, ETA*)是安全系统工程的重要分析方法之一，曾在美国商用核电站风险评价中做出过重要贡献。70年代初期，拉斯姆逊教授领导的小组对压水堆核电站*Surry*和沸水堆核电站*Beach Bettom*-2进行概率风险研究，1975年发表了"反应堆安全研究"的报告，代号为*WASH*—1400。报告中采用事件树和故障树的方法，对各种可能发生的事故，包括设计基准事故和非设计基准事故，估计了事故发生概率，并估计了事故的后果。*WASH*—1400当时并未引起政府和科技界的足够重视，直到1979年路易斯对它作出了肯定评价，特别是1979年3月26日美国三浬岛核电站2号机组发生严重事故之后，才获得应有的重视。因为三浬岛事故的发展过程是*WASH*—1400报告所预示的，事故中操作员的过失也正是报告中考虑的。从此人们才认识到安全分析方法是一种有效方法，报告中所采用的事件树和故障树的方法成了安全系统工程中的重要分析方法，并从核电站发展到化工和其它工业领域并得到广泛应用。现在已经在许多国家形成标准化的分析方法，如在日本就被正式列为劳动省颁发的"化工厂安全评价六阶段"的一个程序。

事件树分析最初用于可靠性分析，它是用元部件可靠性表示系统可靠性的系统分析方法之一。在进行系统安全分析时是根据事故发生的先后顺序，分成若干阶段，用树状绘图表示其可能结果的分析方法，它可用于预测事故发展趋势，研究事故预防对策。为了确定对象的安全性，首先应分析可能引起事故的各种原因及其可能的发展途径，然后分析事故的发生频率和预估其后果。事件树分析方法就可以达到这一目的。

系统中的每个元部件，都存在能否完成规定功能的两种可能。元部件正常，说明其能完成所规定的功能；元部件失效，则说明其不能完成所规定的功能。这时的元部件只具有两种状态（即决策分析中的自然状态），在可靠性分析中，人们把元部件正常的状态赋值为1，把失效状态赋值为0。按照系统的构成情况，逐次分析各元部件正常和失效情况下的结果，每个元部件正常和失效都分为二个分支，依次延续分析下去直到最后一个元部件，最后就形成了一个水平放置的形似树枝的图形，即事件树图。

现以火电厂中锅炉燃油输送管路系统为例，一般的燃油输送管路系统是由一个油泵和两个阀门（如一个截止门和一个电动门）组成，如图1-1所示。燃油经油泵A、阀门B和C送

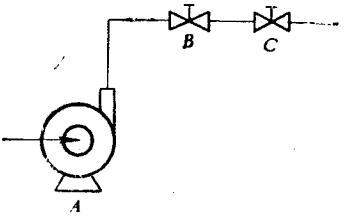

图 1-1　燃油输送系统示意图

进炉膛内燃烧。若只考虑系统中的这三个部件，可以看出A、B、C都有正常和失效的两种状态。根据系统实际结构和燃油的实际流向进行分析，当泵A接到启动信号时，可能正常启动，也可能失效不能启动，打不出油。同样截止阀B正常时能顺利开启，也可能卡死打不开；电动阀C正常时可灵活开启，也可能失灵而不能打开。将每个部件正常状态作为上分支，失效状态作为下分支，三个元素两个状态的组合应该为$2^3=8$种系统状态。由于事件树的结构是按系统的具体情况作出的，泵A处于失败状态时，系统已无法完成其功能处于失效状态，因此阀门B和C对系统结果没有影响；同样，即使泵A处在正常状态而阀门B处于失效状态时，阀门C对系统的结果也无影响，不必再分析阀门C的状态。这样分析下来就画出了这个燃油输送系统的事件树。如图1-2所示。

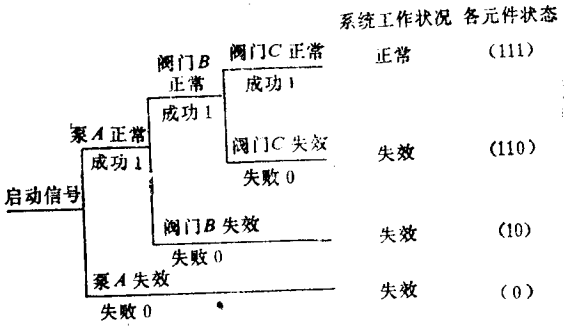

图 1-2 燃油输送系统事件树

从事件树中可以看出，只有泵A和阀门B、C均处于正常状态时系统才能正常运行，而其它三种情况，系统均为失效状态。

如果各部件的可靠度已知（当然若知道各部件失效概率

也行），就可求出系统可靠度。设泵A、阀门B和C的可靠度分别为R_A、R_B和R_C，则系统可靠度为三个部件均为正常状态时的概率值，即三事件的积事件概率

$$R_S=R_AR_BR_C$$

而系统的失效概率为$Q_S=1-R_S$

根据安全系统工程的四要素，将人、物、环境、管理作为分析对象，考虑各种因素的成功或失败的两种情况，也就是将仅以硬件系统为对象的可靠性分析方法扩大应用于系统的事故分析。我们知道，任何事故都是一个多环节事件发展变化过程的结果，从这一点看，事件树分析的实质，就是利用逻辑思维的规律和逻辑思维的形式，分析事故发生的动态过程。因此事件树分析也可以说是事故动态过程分析。

第二章 事件树的编制

事件树分析（*ETA*），是根据事故发生的先后顺序，分成若干阶段，用树技状绘图表示其可能结果然后进行分析的方法。它可用于预测事故发展趋势，研究事故的预防措施。

第一节 初因事件及其选择

每一个事故的产生都是一个动态过程，都要经过孕育、成长、发生三个阶段，而事故在发展过程中出现的事件可能有两种情况——发生和不发生（成功和失败），一个事件按哪种情况发展变化是偶然的，在连续出现的事件中，前一环节的事件影响着后一环节事件的发展变化。事件树分析就是从事故的起因开始分析，途径原因事件，到结果为止来进行的。

事件树的建立与分析就是在对可能引起事故发生的各种原因进行分析的基础上进行的，我们把引起事故的初始原因事件称为初因事件，在主要是分析引起事故的事件时，常将初因事件称为事故初因。当初因事件发生时，要求调动有关功能系统来消除事故，应用逻辑归纳方法将这种合理安排或调动有关功能系统的先后顺序过程反映出来而建立起来的树图，就是事件树。事件树是依赖于系统对初因事件的响应，每一响应都可看成一个事件，都有成功或失败的可能，因此事件树也可以说是系统对事故初因以两态为特征的客观响应树。

初因事件的分析与选择由所分析系统的范围而定，取决于分析对象和目的。按子系统的功能，初因事件可分为按事故原因分析事件树初因事件和按工艺过程分析的事件树初因事件等。

例如，火电厂中维持锅炉汽包水位是锅炉运行最重要的一项任务。汽包水位高，会破坏汽水分离装置正常的工作，降低蒸汽品质甚至会造成满水事故；汽包水位低则会破坏水循环，导致烧干锅和爆管事故。因此对于高参数、大容量的机组，除了设有锅炉汽包水位自动调节系统外，都还设置有水位保护装置。对于汽包高水位保护，设有一值、二值及三值保护。当水位达高一值时，接点接通后，发出“水位高一值”的水位信号，提醒运行人员注意加强监视，并采取必要的措施。当水位继续上升到“高二值”时，发水位信号，同时开事故放水门，紧急降低汽包水位。当水位高至三值时，应关给水总门，不破坏真空停机，并停甲、乙送风机实行紧急停炉。

在不考虑其它联锁回路，只对锅炉满水事故进行分析时，显然造成锅炉满水甚至因此停炉的最初原因是水位上升。因此这里可以将“水位上升”作为事件树的初因事件，由此开始分析事故发展的过程，得到锅炉满水事件树如图2-1所示。

在第一章第三节提到的燃油输送系统事件树（见图1-1），则是属于按工艺过程进行分析各部件正常和失效状态下的各种结果，按其操作和系统动作过程，将“启动信号”作初因事件，由此产生的系列过程中出现的系统状态进行分析而得到该事件树。

初因事件的选择与分析是建立事件树的基础，因此要求

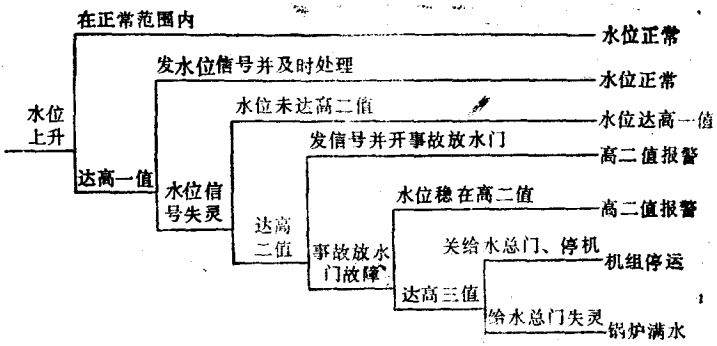

图 2-1 锅炉满水事件树

结合对系统的分析和生产工艺过程以及防止事故发生与扩大的各保护屏障进行全面分析，既要考虑对内部原因的分析，还要考虑对外部原因的分析（如外部系统失电、突发性的其它事故的影响等）。因此在建立事件树的过程中，事故初因分析和系统分析是一个不断深化的迭代过程。

对于火电机组，可以考虑的初因事件很多，作为参考举例如下：

1）快关主汽门操作失灵；

2）发电机失磁；

3）调速油压降低；

4）联锁装置未校或故障；

5）汽压超越定值；

6）发电机内冷水（氢）中断；

7）串轴保护失灵；

8）锅炉缺水；