目　录

第一章 概 述

§1-1 引 言

在分析系统可靠性时，60年代初沿用数学家提出的真值表法、概率图法、可靠性框图法等。随着系统复杂性的增加，工程师们感到应用这些方法很困难，更重要的是这些方法无法反映环境因素和人为差错的影响。于是人们努力研究简便易行的新方法。

1961年美国贝尔电话研究所的H·A·Watson在分析民兵导弹发射控制系统安全性时首先提出并应用了故障树分析法，取得了卓越的成绩。此后很多人从事应用和研究，使之逐渐完善形成了完整的理论。其应用已普及到宇航、航空、交通、机械工业、电子工业、化学工业等部门，在社会安全、经济管理领域也开始应用了。现在国际上已公认故障树分析法是可靠性安全性分析的一种简单、有效、很有发展前途的方法。

所谓故障树分析法，是首先写出分析的系统故障事件作为第一阶（即第一行），再将导致该事件发生的直接原因（包括硬件故障、环境因素、人为差错等）并列地作为第二阶，用适当的事件符号表示之，并用适当的逻辑门把它们与系统故障事件连结起来。其次，将导致第二阶各故障事件发生的原因分别并列在第二阶故障事件的下面作为第三阶，用适当的事件符号表示之，并用适当的逻辑门与第二阶相应的事件连结起来。如此逐阶展开，直到把最基本的原因都分析出来为止，这样的一张逻辑图叫做故障树（简称为FT）。根据故障树分析系统发生故障的各种途径和可靠性特征量，这就是所谓的故障树分析法（简称FTA）。

在故障树分析法中，把要分析的系统故障事件称作顶事件，把不能再分解的基本事件称作底事件，把其它事件称作中间事件。

（一）故障树分析法的特点

1．直观性强。由于故障树分析法是一种图形演绎法，因之能把系统的故障与导致该故障的诸因素（直接的、间接的、硬件的、环境的和人为的）形象地表现为故障谱。从上往下看，可以看出：系统故障与哪些单元有关系，有怎样的关系，有多大关系；从下往上看，可以看出单元故障对系统故障的影响：有什么影响，影响的途径是怎样的，影响程度有多大。

2．灵活性大。故障树分析法不仅可以反映系统内部单元与系统的故障关系，而且能反映出系统外部的因素（环境因素和人为决策错误）对系统故障的影响。

3．通用性好。由于有上述优点，因此，在设计阶段，可使设计者弹清系统的故障模式、成功模式，发现单元故障的危害性、重要度，及时发现系统的薄弱环节，因之能及时修改设计，避免严重的返工，避免研制阶段的不安全，争取首次设计成功。从而缩短了研制周期和节省资源。对军工产品和复杂系统来说缩短研制周期尤其重要。因此对设计者来说故障树分析法是一个好方法。

对贮存和使用者来说，即使是未参加设计和建树过程，故障树可以当作形象管理、维修的指南，从而可缩短培训周期。

故障树分析法除了适用于工程需要之外，还适用于分析国民经济大系统的运行，对社会

问题、军事行动决策等方面也很有用。

但是故障树分析法也有一些缺点，主要是建树很繁，工作量很大，因此易导致错漏。现在虽有了一些计算机程序，但尚无通用程序；对大型复杂系统占用计算机内存单元和时机很多，需进一步研究。

（二）故障树分析法的应用范围

通常在工程上可用于以下几方面：

1. 系统的可靠性分析，可靠性参数的定量计算。
2. 系统的安全分析和事故分析，寻找薄弱环节、制订预防措施。
3. 系统的风险评价。
4. 系统部件的重要度分析。
5. 故障诊断和检修表的制定。
6. 系统最佳探测器的配置。
7. 故障树模拟。

（三）故障树分析法的步骤

通常因评价的对象、分析的目的和精细程度等不同而不同。但一般可按以下步骤进行：

1. 选择顶事件
2. 建造故障树
3. 求故障树的结构函数
4. 定性分析
5. 定量分析

§1·2 故障事件的分类

如果系统（或部件等）不能在规定的条件下规定的时间内完成其规定的功能，则称它处于故障状态，这种事件称作故障事件。否则，称正常状态，正常事件。

故障事件可按不同标准分类。

（一）依不能完成功能的特点可分为五种形式

1. 过早地投入运行
2. 不能在规定的时间内投入运行
3. 不能在规定的时间内停止运行
4. 在运行期间停止运行
5. 完成非正常功能，或执行任务不准确。如继电器应该切断时反而接通，因电磁感应跳火花而引起火灾等。

（二）依故障原因可分为三种

1. 一次故障事件，即硬件本身造成的故障事件。

2. 二次故障事件，即环境因素、人为差错（包括软件差错）造成的故障事件。如部件因受过应力（泛指机械振动、冲击、电磁场作用，应力持续时间等超过了允许条件）而损坏；有的部件受过应力作用不能正常地完成其功能，当过应力消除之后又能自行恢复其功

能。如屏显因严重的干扰而显示不清楚，当干扰消除后，又能正常显示。

3. 受控故障事件，即部件的故障原因是系统内部其它部件输出错误的信息。

综上所述，可用图 1-1 表示部件故障事件的特征。

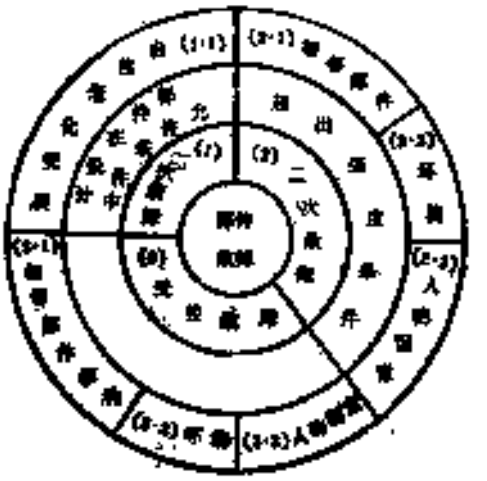


图 1-1 部件故障特征图

§1-3 故障树中使用的符号

故障树中使用的符号可分为事件符号和逻辑门符号两大类。

（一）事件符号

1. 矩形符号

矩形符号（图1-2(a)）表示顶事件和中间事件。它下面与逻辑门连结。

2. 圆形符号

圆形符号（图1-2(b)、(c)、(d)）表示底事件。其中用实线圆(b)表示硬件本身故障，用（c）表示人与人之间的差错引起的底事件，用（d）表示因操作者未发现异常现象而引起的底事件。圆形符号内的事件不能再分解。它只能作为逻辑门的输入，而不能作为其输出。

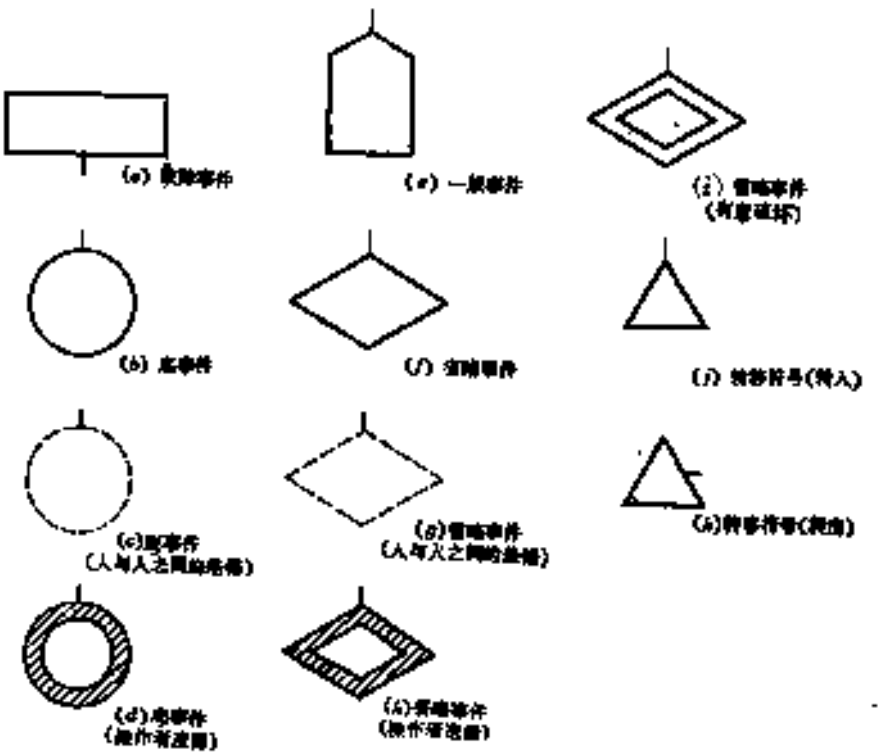


图 1-2 故障树的事件符号

3. 房形符号

房形符号（图1·2(e)）表示条件事件。一般当作一种开关。当房形符号中所给定的条件满足时，房形符号所在的逻辑门的其它输入则保留，否则去掉。房形符号内的事件可以是正常事件，也可以是故障事件。用之满足特殊条件下建树的需要。

4. 菱形符号

菱形符号表示省略事件。有的故障事件不是底事件，但因其发生的概率已知，或者因其发生的概率较小不需再分析了，或者因其无法再分析了，因之当作底事件处理。有时用实线菱形（图1·2(f)）表示硬件故障事件，用虚线菱形（图1·2(g)）表示人与人之间的错误引起的故障事件。用带斜线的双重菱形（图1·2(h)）表示操作者未发现异常现象而引起的故障事件，用双重菱形（图1·2(i)）表示由于受骗而引起的故障事件。

5. 三角形符号

三角形符号表示转移符号。在同一故障树中，有的出现完全相同的事件关系或本来就是同一事件在故障树的不同位置上重复出现，为了减轻建树工作量和使故障树简化，用转移符号进行转移。三角形上方的直线（图1·2(j)）表示从这里输入，三角形侧面的直线（图1·2(k)）表示从这里输出。在一对三角形中标出同一个编码。

（二）逻辑门符号

逻辑门符号同逻辑电路所用的符号相似。目前尚未统一，这里只介绍常用的几种。

1. 逻辑与门

逻辑与门简称与门（图1·3(a)），它表示全部输入事件都发生才能使输出事件发生的逻辑关系。

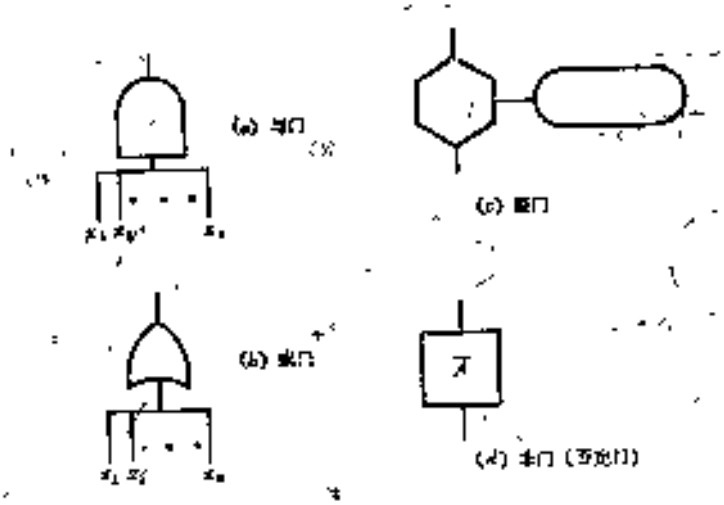


图 1·3 故障树的逻辑门符号

2. 逻辑或门

逻辑或门简称或门（图1·3(b)），它表示输入事件中只要有一个或多于一个发生就能使输出事件发生的逻辑关系。

3. 逻辑禁门

逻辑禁门简称禁门（图1·3(c)），它表示只有满足一定条件时输入事件发生才能使输

出事件发生的逻辑关系。一般用于表示某些非正常工作条件下发生的故障，专门用于表示二次故障事件。

4. 否定门

否定门简称非门（图1-3(d)）表示输出事件是输入事件的对立事件。

（三）修正门

由与门和或门加上修正符号可构成不同形式的修正门（图1-4）。

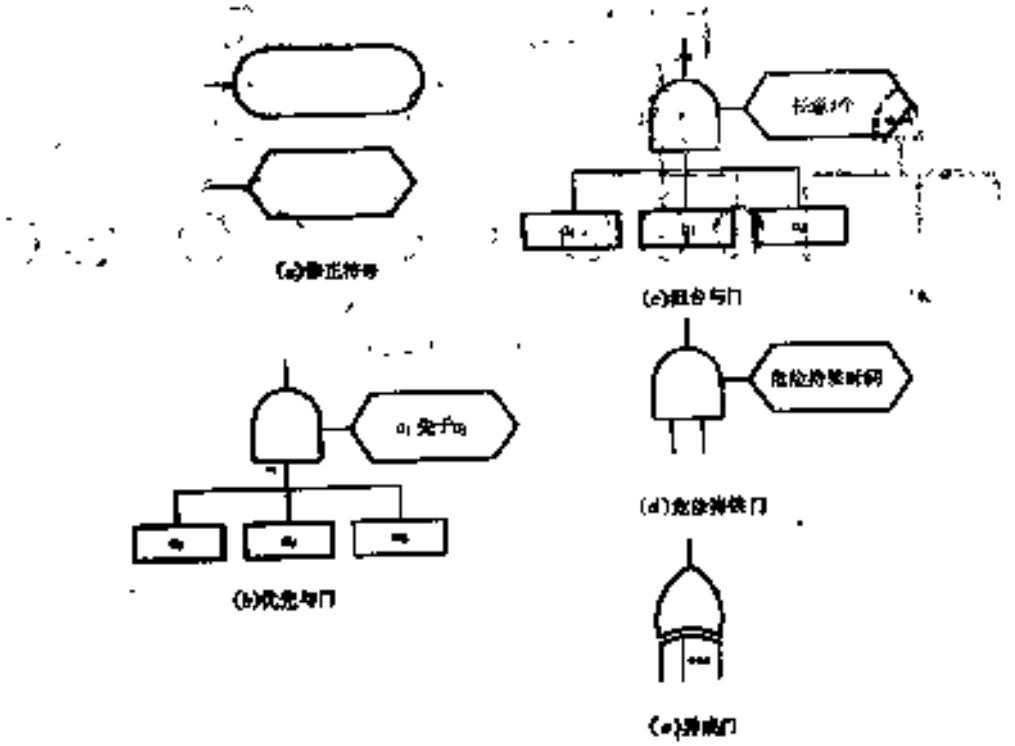


图 1-4 故障树的修正符号和修正门

1. 优先与门

在与门输入事件中，当某一事件较其它事件先发生时才能使输出事件发生，这种逻辑关系用优先与门（如图1-4(b)）表示。

2. 组合与门

当与门的输入事件多于三个时，如果任何两个先发生就能导致输出事件发生，这种逻辑关系用组合与门（图1-4(c)）表示。

3. 危险持续时间门

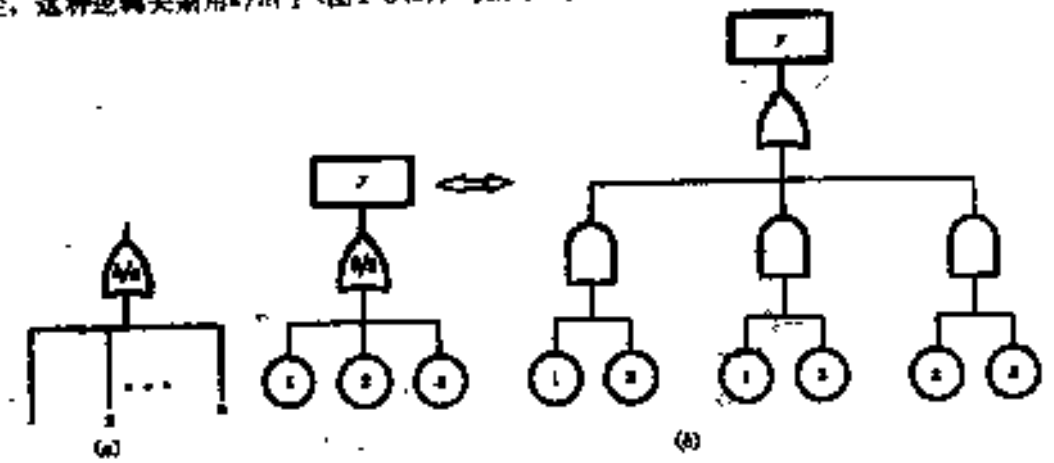
在与门输入事件中，当输入事件都发生并持续一定时间的条件下才能导致输出事件发生；可是，如果输入事件都发生了，但未持续一定的时间就不能导致输出事件发生，这种逻辑关系用危险持续时间门（图1-4(d)）表示。

4. 异或门

只有输入事件之一发生时才能导致输出事件发生，而如果有两个或两个以上的输入事件发生时，输出事件就不发生，这种逻辑关系用异或门（图1-4(e)）表示。

5. k/n门

当n个独立的输入事件中只要有k个或多于k个输入事件发生时就能导致输出事件发生，这种逻辑关系用k/n门（图1-5(a)）表示。k/n门可用或门和与门等效表示之。



(a)　　(b)

图 1-5　表决门及其等效表示举例

第二章　选择顶事件建造故障树

§2-1　选择顶事件

所谓顶事件是指所分析的系统最不希望的故障事件，它是分析的目标。

依分析的任务不同，确定顶事件的方法也不同。当任务是分析给定的故障事件时，则该事件就是顶事件；当任务是预测系统的可靠性时，就需要选择顶事件。顶事件选好了，可以使系统内部许多故障事件（中间事件和底事件）联系起来，有利于对系统的可靠性进行分析，以便提出改进建议。

（一）选择顶事件的原则

1. 要有确切的定义，而不能模棱两可。

2. 要能分解，以便分析顶事件与底事件之间的关系。

3. 要能度量，以便进行测量和定量分析。

4. 最好有代表性，以收事半功倍之效。

（二）选择顶事件的步骤

1. 明确定义系统的正常状态，故障状态和故障事件。为此要对系统的功能有足够的认识，要详尽地搜集和分析系统设计和运行的技术规范等描述系统的有关技术资料，以及故障档案。

2. 对系统的故障作初步分析。找出系统内部固有的故障事件，找出这些事件导致系统故障的所有可能的途径，即故障模式。

3. 筛选故障事件确定顶事件。在初步分析的基础上，把系统故障按类型和严重程度分类排队，从而确定最不希望发生的事件作为顶事件。在分类排队时往往需画出较大范围的粗细流程，列出系统与子系统、部件的功能关系、事故链等，以便比较。

须知，对于复杂系统，不但要分析最不希望发生的事件，还需分析其它的故障事件，因此顶事件不是唯一的。

有时对于大型复杂系统，为了分析计算方便，也可以把子系统的故障（中间事件）当作顶事件建造若干个子树进行分析计算，最后综合其结果，这样可使问题简化，工作量大大地减少。

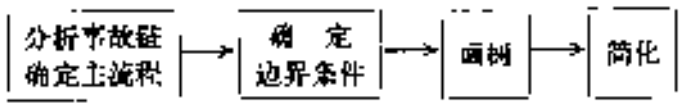
§2-2　建造故障树

故障树是故障树分析（定性和定量分析）的对象，其完善程度直接影响分析结果的准确性，其化简的程度直接影响分析的工作量，也影响故障树的直观性。因此建造故障树是故障树分析法的关键。

对于大型复杂系统，由于故障机理交错多变，逻辑关系复杂，因此要求建树者必须熟悉，并能广泛地掌握关于系统的设计、运行、安全分析等方面的知识和经验。所以一般应由设计、工艺、试验、使用和管理等方面的专家组成一个精干的班子来完成建树任务。

目前建树的方法有两大类。一是人工建树——演绎法，一是计算机辅助建树。由于人工建树可以使建树者透彻地掌握系统中故障事件的逻辑关系，因此我们这里只介绍它。

所谓用演绎法建树，如同第一节所述，它是从顶事件开始往下经过中间事件直到底事件为止逐级分解的建树方法。在顶事件确定后，建树一般分为以下几步：



（一）注意事项

为了使故障树能正确地、简明地把系统的故障事件表示出来，使人们容易直观地看出系统的故障源，因此在建造故障树时必须注意以下几点：

1、有明确的主流程，确保逻辑严谨。

所谓主流程是指能贯穿于系统各部件的功能故障，以其为纲，从顶事件到底事件逐级分解建树。这样就可使故障树的思路明确，使人一目了然。

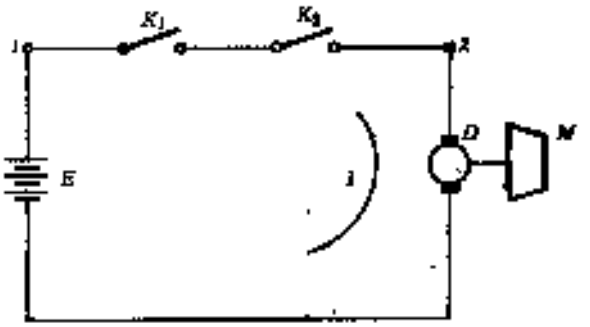


图 2-1 直流电机驱动系统

例 2-1 图 2-1 是一直流驱动系统。其中，E——24 V 直流电源，K_1——手动开关，K_2——电磁开关，D——电机，额定电压$U=24V$，故障概率$Q_D=0.001$，M——油泵，故障概率$Q_M=0$。系统故障是不供油。

以电机不能启动为顶事件建造故障树，确定主流程。电机不能启动可能是油泵M卡住、电机转子卡住、K_1和K_2未合上、电源故障和未给电机额定电流。很显然前面几种事件对此故障事件是独立事件，不能作为主流程，只有电流是贯穿回路的，是否可用它作为主流程呢？不可以。因为题中未告诉额定电流是多少，然而额定电流是由额定电压决定的，因之最好以额定电压为主流程。

但是必须指出，简单系统往往只有一个主流程；而大型复杂系统往往每一子系统有自己的主流程，此时就要因树而定。要以建树方便、思路清楚为原则，不要牵强附会。

2、合理地确定边界条件，以便确定故障树的范围。

所谓边界条件是指在建树前对系统、部件等提出的假设条件。通常有两类边界条件：

（1）系统的边界条件。它包括初始条件、已知的技术状态、已发生或正在发生的故障事件（含顶事件）、不允许出现的事件等，其中顶事件是最重要的边界条件之一。

（2）部件的边界条件。它包括假定部件所处的状态、部件发生故障的概率等。如：

① 确定不可能事件。一般把小概率事件当作不可能事件，建树时就不画出来了。如上面的例子中，可假定导线和接头故障忽略不计。

② 确定必然事件。它是系统工作时在一定条件下必然发生的事件，或必然不发生的事件。如在图 2-1 中，假定油泵、连轴器、导线及接点的故障概率为零，即它们必然不发生故障。

⑧ 确定某些事件发生的概率。如电机总故障概率$Q_D=0.001$。

上述这些假定就是一组边界条件。有了边界条件，就明确了建树的范围。根据这些边界条件，就可选“电机不能启动”为顶事件；否则就要选“油泵不供油”为顶事件了，因此建树的范围也就不同了。

但是，在确定边界条件时必须特别注意：

1° 忽略小概率事件不等于忽略小部件的故障和小故障事件。这是两个不同的概念。美国著名的WASH—1400报告，对于核电站系统的安全性分析得出十分重要的结论：小事故、小管道断裂往往比大管道断裂引起系统的故障概率更大。

2° 有的事件概率虽小，但一旦发生后果严重，这种事件就不能作为不可能事件处理。例如某导弹测试车电缆插座与导弹控制舱电缆插头连接时，插错错位的概率$Q_1\leqslant10^{-5}$，条令规定可以带电连接。但是，带电连接，一旦发生错位，就有可能使控制舱的燃气发生器点火导致控制舱报废，损失万元以上。据不完全统计，此事故在20年中曾发生过两起。因此这种事件不能忽略。

3、精确地定义故障事件。必须做到只有一种解释，切忌多意性和模棱两可、含糊不清。否则可能导致树中出现逻辑混乱、矛盾和错误。仍以图 2-1 为例，以电压为主流程所建之树如图 2-2 所示。顶事件定义为“电机不能启动”，其直接原因是电机本身故障，因其故障概率$Q_D=0.001$为已知，故为底事件；受控故障事件是“D两端无直流电压24V”。造成此故障的直接原因有两个：K_1故障断开或 2 点无直流电压24V。造成 2 点无直流电压24V的直接原因是电源输出电压低于24 V 或K_2故障断开。

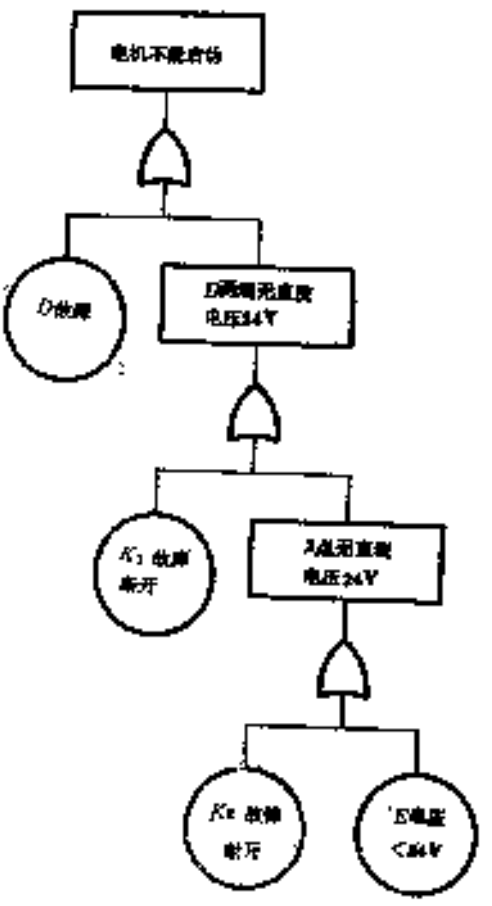


图 2-2 图2-1的故障树

若将“D两端无直流电压24V”改为“无额定电压”时看来精练了，但却带来了模棱两可的含意：是无直流电压还是无交流电压？电压是多少？

4、“先抓两头，后抓芝麻”。建树的头几步应只考虑上要的、高度可能的，或关键性的事件（可以用致命度来识别）；然后随着分析的进展，再考虑次要的事件、发生概率较小的事件。

5．严谨的逻辑性。系统中各故障事件间逻辑关系、条件必须分析清楚，不能紊乱和自相矛盾。现在举例说明之，

例2·2 照明系统的示意图如图2·3所示，其中：A——灯泡，E_1、E_2——电池，K_1——继电器J_1的常开触点，K_2——继电器的常闭触点，K_3——手动开关。

系统功能：使A始终亮。

系统描述：在正常运行时，K_3处于闭合状态，经回路Ⅱ向A供电。当K_2故障断开时，操作K_3闭合，回路Ⅲ中有电流，使J_1线圈通电，K_1闭合，由回路Ⅰ向A供电。因此不论K_2是否闭合，A总是亮的。

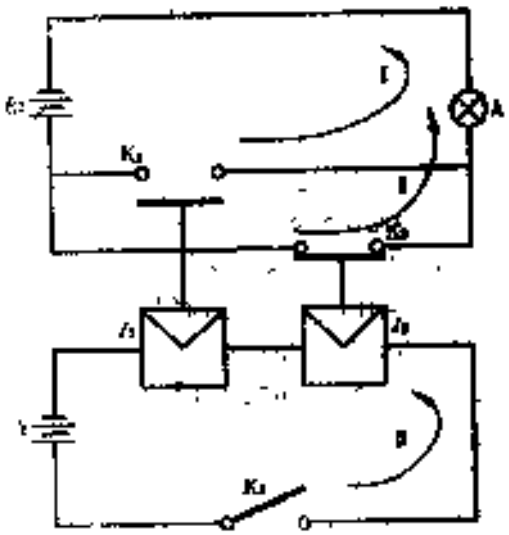


图 2·3 照明系统示意图

边界条件：不计导线故障和二次故障。

初始条件：K_2断开，K_1、K_3闭合。

顶事件：最不希望A不亮，就以它为顶事件。上流程：电流。

用演绎法可建造故障树FT_1如图2·4所示

由系统描述知，无论K_2是否闭合，只要系统运行正常，A始终亮。而Ⅲ中有电流与无电流是一对互斥事件，不可能同时发生，因此故障树FT_1与门下的逻辑关系是不成立的。按这样的故障树求解必然得出矛盾的结论。

为此必须参照图2·5的故障树FT_2，将Ⅲ中有电流和无电流分开处理。

（二）化简故障树

为了定性、定量分析方便，必须对建造的故障树进行简化。简化的标准是去掉逻辑多余事件，用简单的逻辑关系表示之。常用的方法有“修剪”法、模块化。

1. “修剪”法

所谓“修剪”法就是去掉逻辑多余事件的方法。对简单的小故障树可以用目测直接将逻辑多余的事件去掉，也可以用布尔代数运算吸收。因为

$$x \cup x = x, \qquad x \cap x = x$$

$$x_1 \cup (x_1 \cap x_2) = x_1, \qquad x \cap \bar{x} = \Phi$$

上述关系对应的故障树如图2·6所示。

很明显，图2·7的FT_1中除G_4和G_6下所表示的是2/3(F)子树外，其它的子树都是逻辑多余的，因此可将FT_1化简为FT_2。

2. 模块化

所谓模块化是指把故障树中的底事件化成若干个底事件的集合，各集合都不包含其它集合的底事件。即其包含的底事件在其它集合中没有重复出现。故障树模块化后，树的规模就变小了，在定性分析和定量分析时也就容易多了。例如图2·7的FT_1可简化为FT_3。

通常可用两种方法使故障树模块化。一是按定义直接在故障树上目测判断，二是根据故障初步分析，把相邻的中间事件作为模块。

故障树的模块化是简化故障树分析简便易行最有效的手段。应该指出，建树和简化不能完

全分为两个阶段，往往是边建边简化，建完后再统观全局进一步简化。

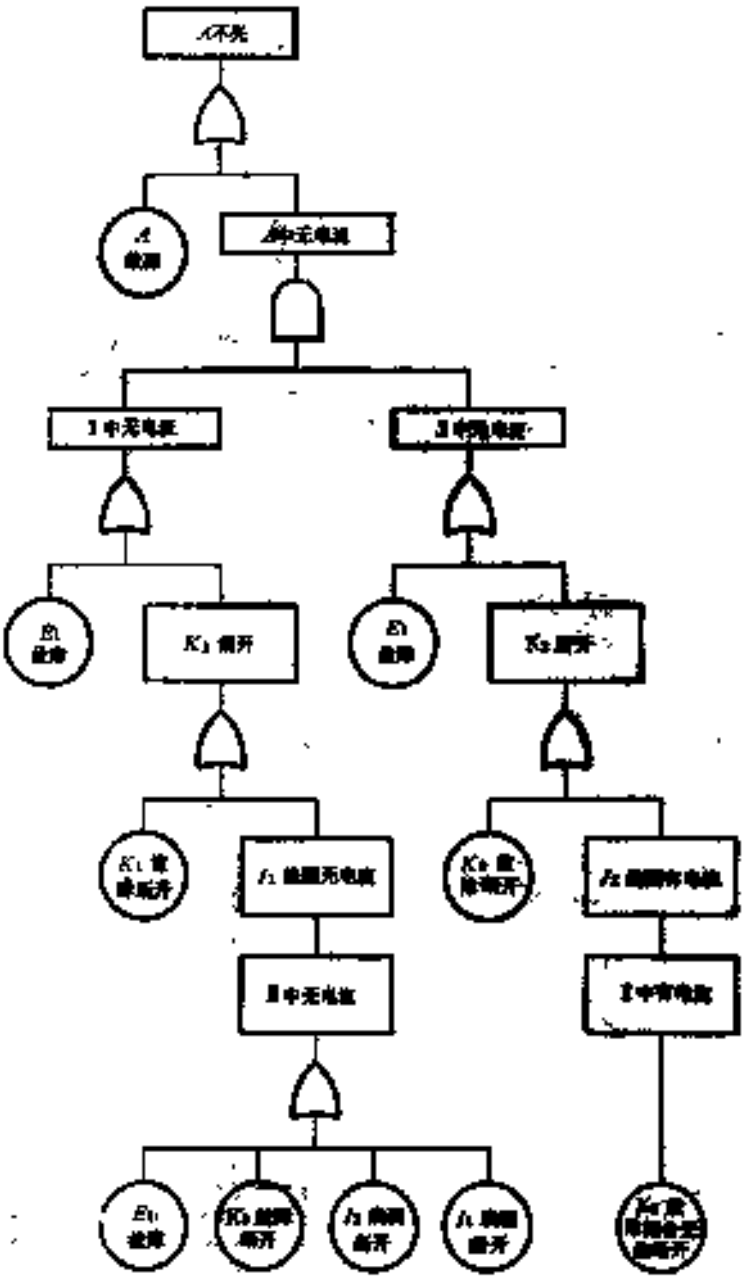


图 2-4 例2-3的故障树FT_1

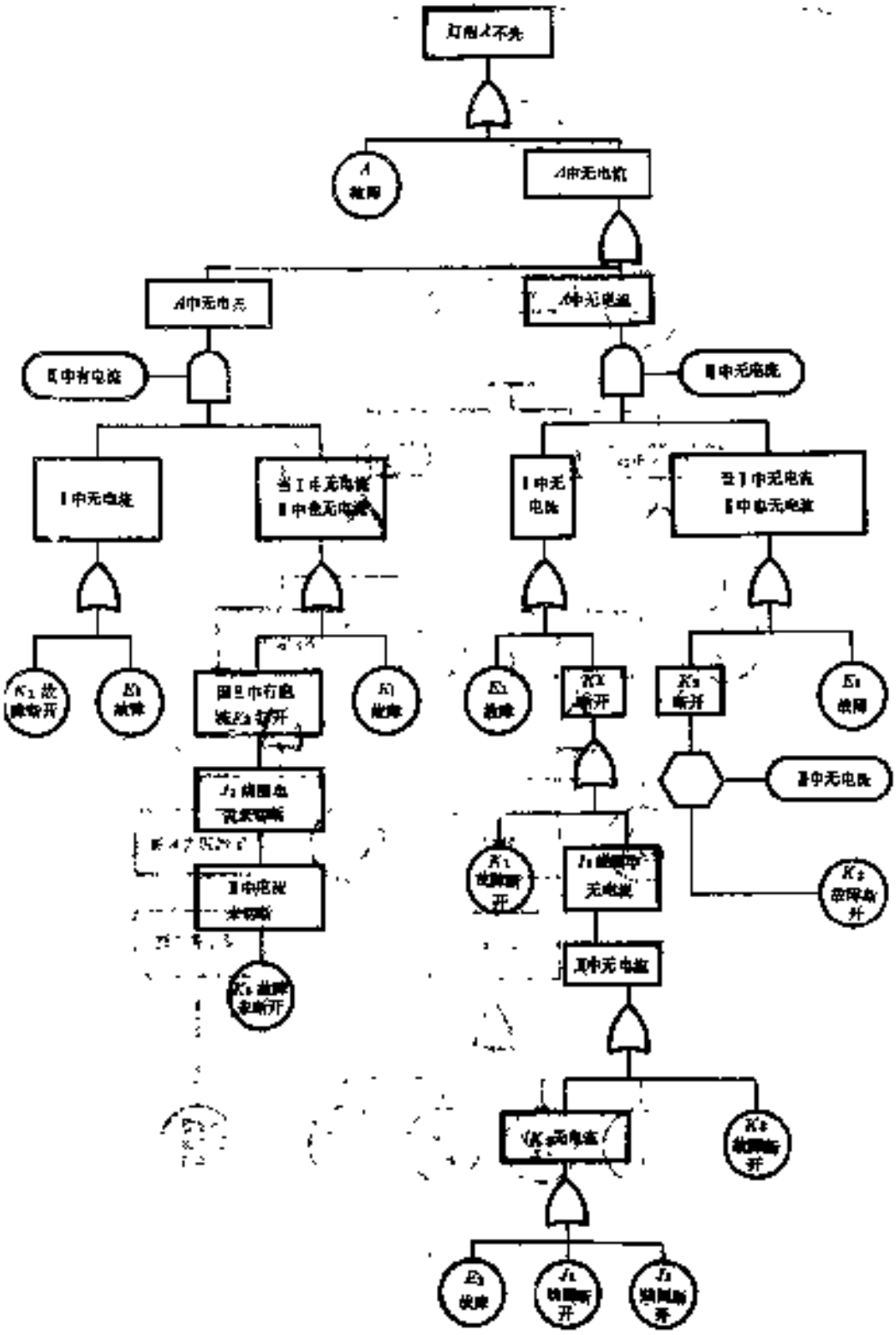


图 2-5 出2-3的故障树FT_2

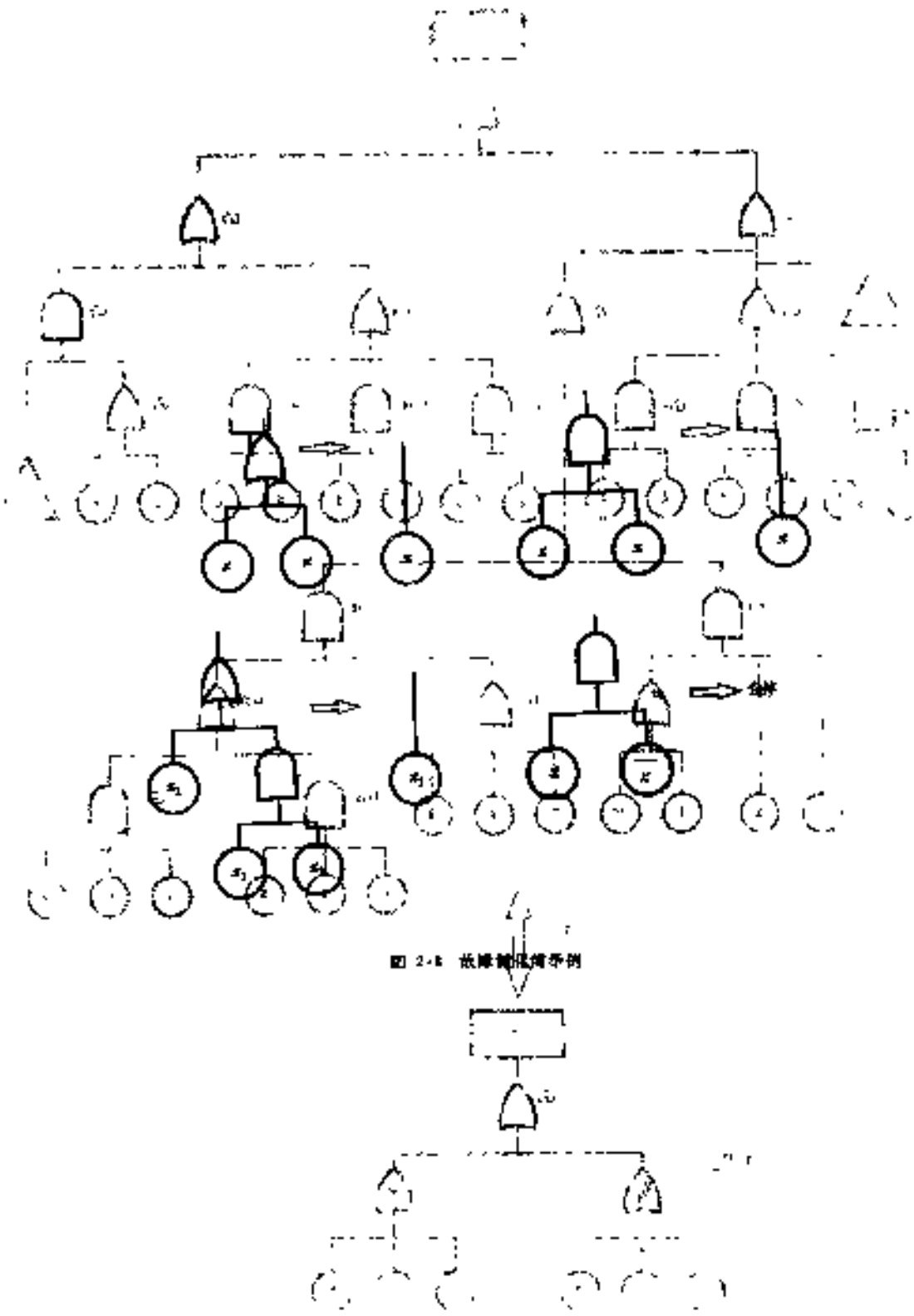


图 2-6 [illegible]

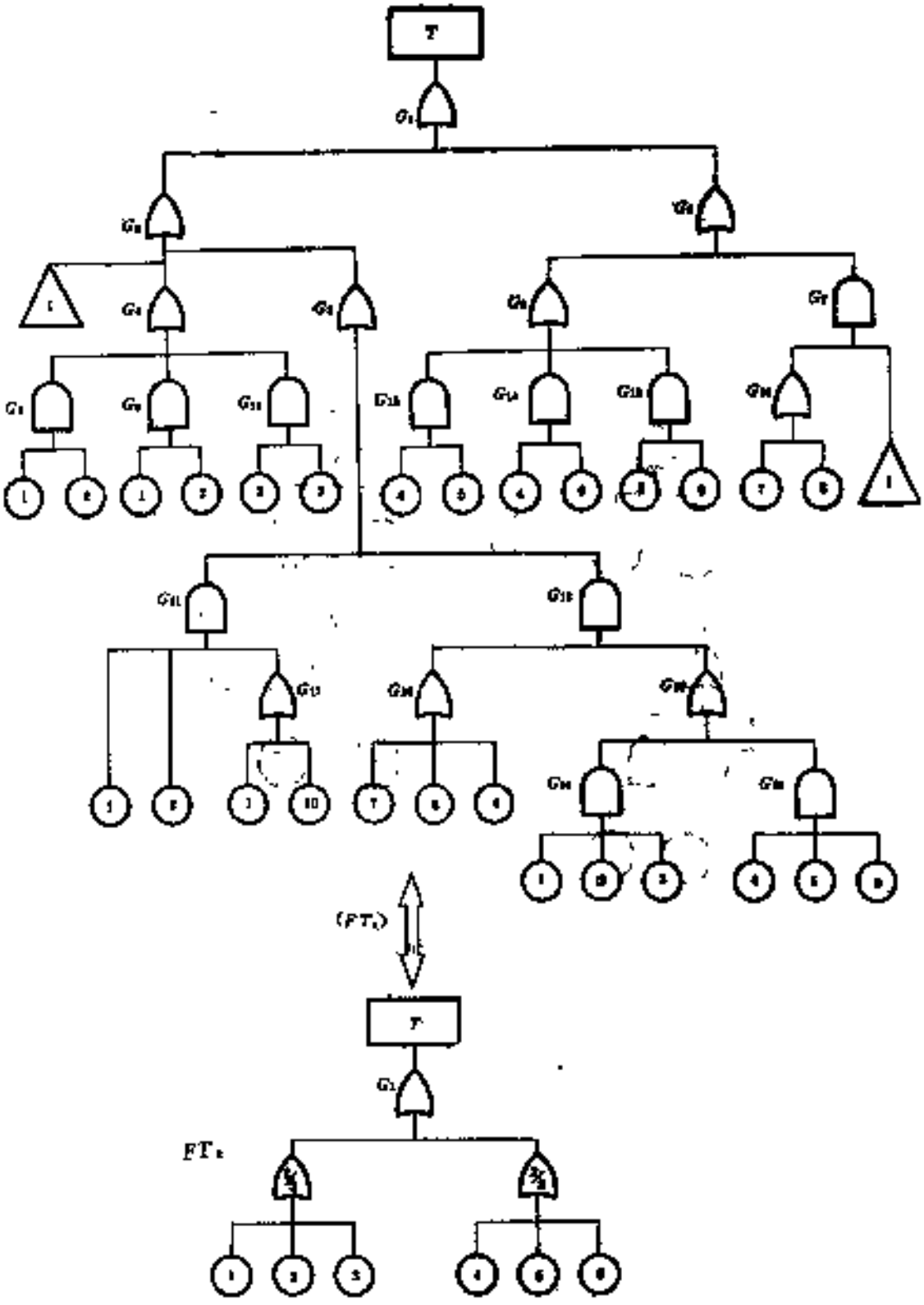

T
G_1
G_2
G_3
G_4
G_5
G_6
G_7
G_8
G_9
G_{10}
G_{11}
G_{12}
G_{13}
G_{14}
G_{15}
G_{16}
G_{17}
G_{18}
(FT_2)
T'
G_1'
FT_2

图 2-7 故障树化简举例

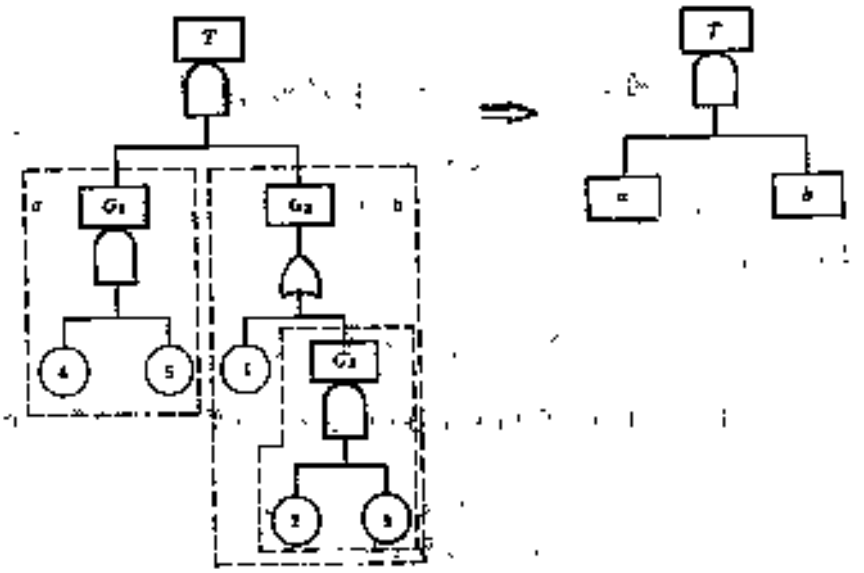


图 2-6 故障树模块化举例

第三章 故障树的结构函数

故障树的结构函数在定性分析和定量分析中很重要。本章将阐述结构函数的概念和性质，以及建立的方法。

§3·1 基本概念

考虑由 n 个不同的独立底事件所构成的故障树。引入二值变量 x_i 表示第 i 个底事件 e_i 的状态，并定义

$$x_i=\begin{cases}1 & e_i\text{发生} \\ 0 & e_i\text{不发生}\end{cases} \qquad i=1,2,\cdots,n$$

同样地引入二值变量 Φ 表示顶事件 T 的状态，并定义

$$\Phi=\begin{cases}1 & T\text{发生} \\ 0 & T\text{不发生}\end{cases}$$

因为顶事件的状态完全由底事件的状态所决定，所以顶事件的状态变量取值也完全由底事件状态变量取值所决定。若定义 Φ 是 $X=(x_1,x_2,\cdots,x_n)$ 的函数，并记作

$$\Phi=\Phi(X) \tag{3·1}$$

则称函数 Φ 为故障树的结构函数。

例3·1 图3·1所示的与门结构故障树的结构函数为

$$\Phi(X)=\prod_{i=1}^{n}x_i=\min(x_1,x_2,\cdots,x_n) \tag{3·2}$$

例3·2 图3·2所示的或门结构故障树的结构函数为

$$\Phi(X)=\coprod_{i=1}^{n}x_i=\max(x_1,x_2,\cdots,x_n) \tag{3·3}$$

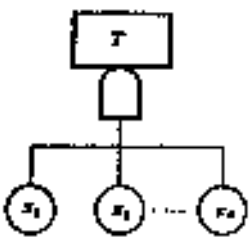


图 3·1 与门结构故障树

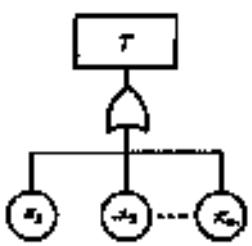


图 3·2 或门结构故障树

其中记号 $\coprod$ 表示

$$\coprod_{i=1}^{n}x_i=1-\prod_{i=1}^{n}(1-x_i) \tag{3·4}$$