卫星喷气系统设计方案的失效树分析

赵　　众　　王 杰 生

（中国科学院空间技术中心总体部）

科学卫星的发展对卫星姿态控制系统提出了高控制精度和长飞行寿命下的高可靠性要求。在三轴稳定姿态控制的卫星上，采用有源姿态控制的喷气系统，较易于满足上述两项要求。对卫星的三个相互垂直的坐标轴 x、y、z（图1）进行定向姿态控制，可分为发射进入轨道后的消旋姿态捕获和飞行中姿态控制两种情况，这两种情况都可以应用安装在卫星质心平面（图1中舱平面附近）星体边缘的一对喷嘴和安装在距离质心平面H距离的两对相互垂直喷嘴来实现。为了提高喷气系统比冲和减少星带燃料重量，目前多采用热喷气系统而不宜用冷喷气系统。本文讨论的几种方案均为热喷气系统。

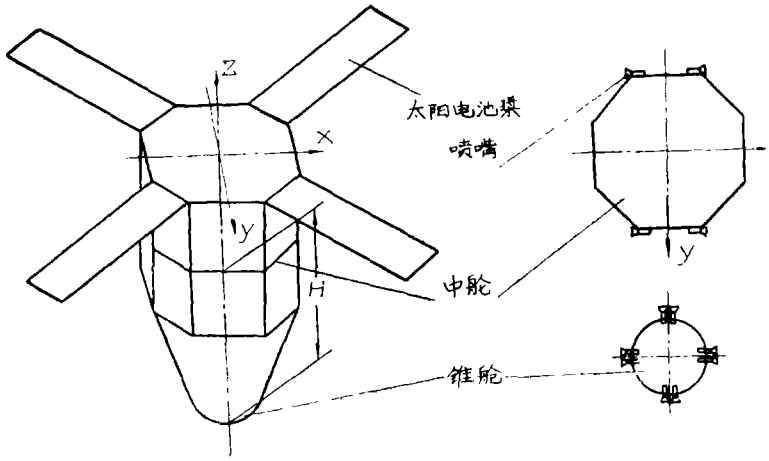


图1　喷嘴安装示意图

飞行时喷气系统通常是用来作为反作用飞轮的卸载用。采用动量交换式的反作用飞轮是卫星姿态控制的执行件，当反作用飞轮为了平衡卫星各种干扰力矩产生的动量而自身转速增加到某一控制值时，开动某喷嘴给飞轮卸载，使它的转速降到零左右。此种姿态控制方式不仅可以有效地提高姿态控制精度，而且还可以明显地节省有源控制式的喷气系统的燃料。本文列举的几种对此方案均属这种姿态控制方式。

对于长飞行寿命下的卫星，其姿态控制系统中的喷气系统是最关键的。为了提高喷气系统的可靠性，目前广泛采用优先给予喷气系统冗余设计方案。对各种冗余设计方案，可靠性预测就成为方案评价的重要依据。本文用失效树分析FTA (Fanlt Tree Analysis) 对喷气系统几种冗余设计方案进行了可靠性定量预测计算，并求出了各种方案的最小割集（即各方案的各种失效模式），找出了这几种设计方案中的最优方案，还有方案评价的结论和分析，最后提出应用FTA存在的问题和在空间机械中可以应用的几个领域的设想。本文的计算工

作引用了清华大学核能所编制的失效树计算程序 FTA—1 和 FTA—3（参见〔1〕），在 UNIVAC 1100计算机上进行计算的。

几种喷气系统方案

一）带转换开关的全路备份方案——方案之一（图2）

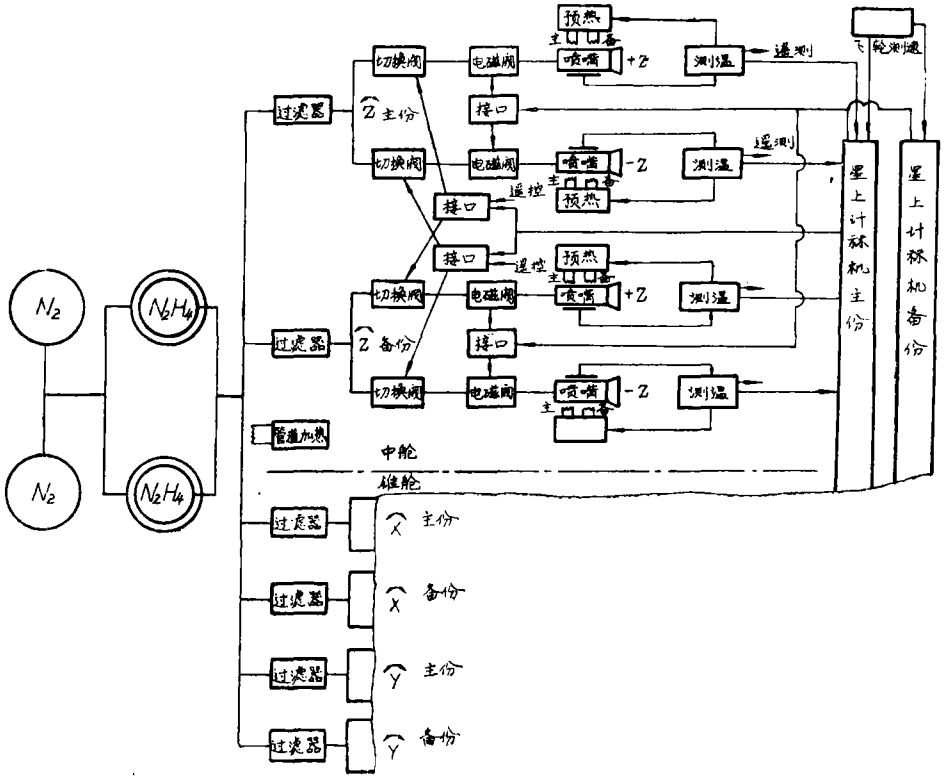


图 2　姿控喷气系统带转换开关的全路备份方案——方案之一

氮瓶内的高压氮气通过管道进入肼瓶，压缩肼瓶内的皮囊，将肼(N_2H_4) 挤入通向中舱和锥舱的管道。氮瓶和肼瓶两个并联，可以使卫星对 x 轴、y 轴重量分布较为均匀。肼分别通过主份过滤器（图2 的上面的过滤器）和备份过滤器(图 2 从上向下数第 2 个过滤器)进入主、备份切换阀。主、备份切换阀各2个分别控制绕 z 轴正、反两个方向的四个喷嘴。喷嘴的喷气脉冲宽度及脉冲数由各路上的电磁阀控制。各路电磁阀是由各轴飞轮测速传感器测得。当飞轮转速增加到某一控制值（例如达到3×10^4转／分）时的信息通过星上计算机发出指令按程序工作的。本方案的特点是：当各路喷嘴的测温系统发出喷嘴的温度信息经过星上计算机判定该路是否失效（堵塞不喷气或漏喷）时，如果失效，计算机则发出指令使该路切断（关闭），同时接通该轴备份中相同方向喷嘴的一路。这时主份中反方向（如果尚未失效）就和备份中与失效方向相同方向的喷嘴组成一组，以控制该轴上飞轮的卸载。x、y、z 三轴，每轴主、备份各有两路为一组，共计四路。两组间正向、反向还可以再相互组合。这种切换组合方式称为带转换开关的全路备份方案。

本方案中星上计算机、喷嘴预热器均有备份。为了使星上计算机等发生故障后可由地面直接应急控制，所有切换阀的接口设计成可以接受地面遥控的接口。

本方案计算机和切换阀接口的工作任务最大，同时每路均要有一切换阀，零部件数量最多。从方案图上看好象是最可靠的方案，但从后面的计算结果看并非如此。

二）带转换开关备份方案——方案之二（图3）

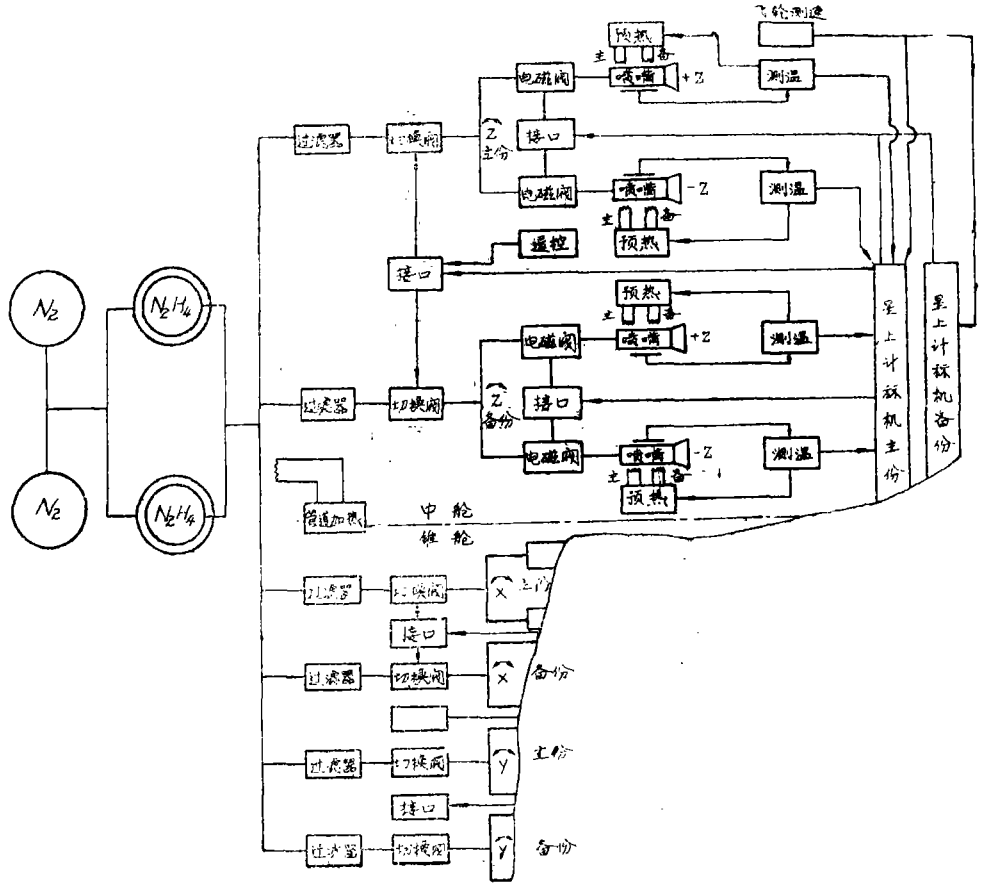


图 3　姿控喷气系统带转换开关备份方案（方案之二）

本方案其他部分与方案之一相同，只有当计算机接到某主份组失效信息后，无论该主份组的两路是否全失效，均一起被切换掉。本方案的特点是：切换时总会把一路没有失效的随着失效的一路一起被切换掉。此方案似乎有潜力可挖。它比方案之一省去六个切换阀，减少了星上计算机的负担。

三）平行备份方案——方案之三（图4）

本方案是有备份方案中零部件数量最少、星上计算机负担最轻的方案。这种方案的工作特点是：主份组和备份组在未发生故障前都一起工作，它属于并行工作冗余，本文称为平行备份方案。而方案之一和方案之二均是主份组失效后由备份组接替工作的后备冗余。平行备份方案与后备冗余方案的优劣取决于失效传感系统、失效判定系统和转换系统的可靠性。如果上述系统可靠度不高，则平行工作冗余较优。本文的具体情况如何，应以计算结果而定。

本方案在预热功耗方面有所增加。

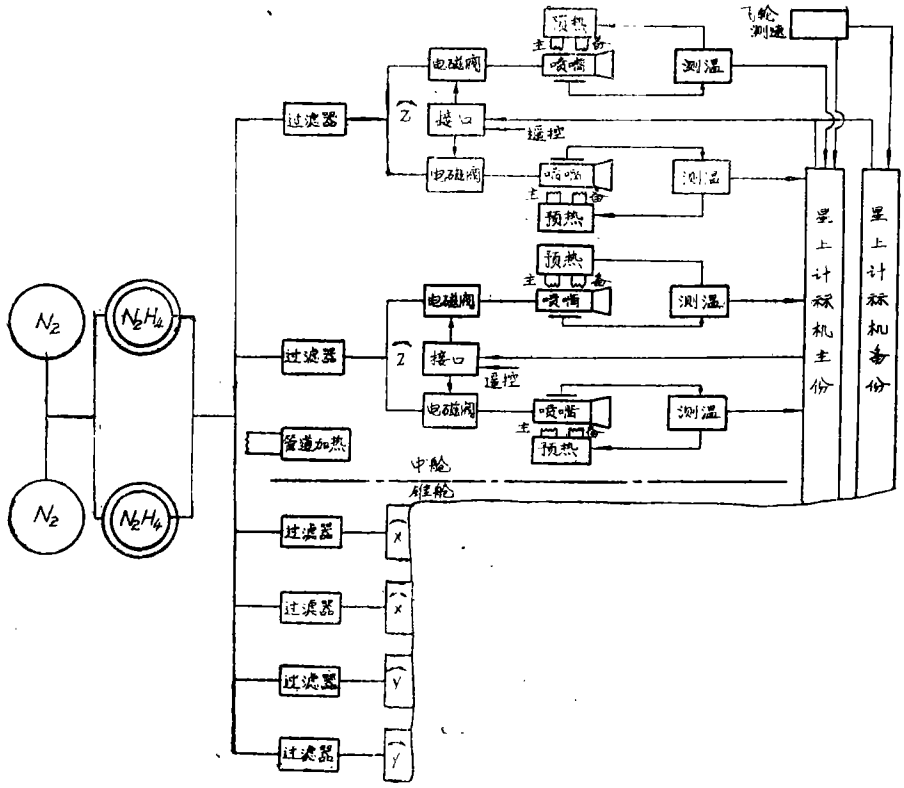


图 4　姿控喷气系统平行备份方案（方案之三）

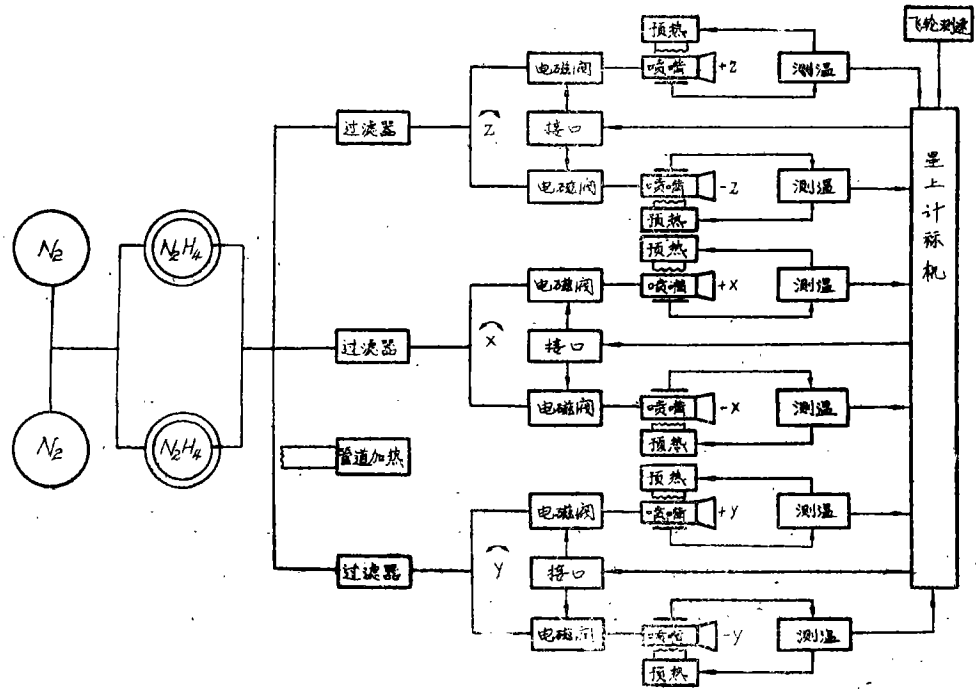


图 5　姿态控制喷气系统无备份方案（方案之四）

四）无备份方案——方案之四（图 5）

无备份方案是整个喷气系统为完成其预定功能所需最少的零部件组成的系统方案，其结构最简单，无切换阀及其接口，电磁阀、预热器、星上计算机等均无备份。本方案显然是可靠性最低的，是作为前三个冗余方案的对比方案而提出的。

FTA法在方案评价中的应用

本文所讨论的卫星喷气系统是一个包括机械、电子设备及人的因素的复杂系统，其中大多数零部件的失效分布规律尚未找到合适的解析表达式，也不能通过常用的典型概率分布：如指数分布、Poisson 分布、Weibull分布等给出可靠度$R(t)$的解析式。在这种情况下，应用FTA法可以求得系统在预定寿命时刻 t 的可靠度$R(t)$的数值，也可求出系统各阶失效模式（各阶最小割集）。这些对于系统方案的评价提供了重要的定量依据。

系统或部件的可靠度可以定义为与时间有关的某个概率函数，即对任意时刻 $t>0$，在一定工作条件下，在（0， t）这段时间中，系统或部件完成预定功能的概率，记作$R(t)$。若以随机变量X表示系统或部件正常工作的寿命，则

$$R(t)=P(X>t)=1-P(X\leqslant t)\ =1-F(t)$$

其中$F(t)=P(X\leqslant t)$ 是系统或部件寿命分布函数，也称不可靠度。

下面介绍应用 FTA 法中的几个主要问题。

一、失效树的顶事件 T

失效树的顶事件定义是："系统最不希望发生的事件"。对某系统而言，如果顶事件发生，则认为该系统失效。

卫星喷气系统的功能是对卫星消旋、姿态捕获，并在一年飞行寿命期间内对 x、y、z 三轴上的反作用飞轮卸载。因此我们确定T为：对 x、y、z 三轴正反六个方向在一年寿命期间有任意一个方向的喷嘴不喷或漏喷。不喷可能是由于推力器的毛细管堵塞、电磁阀堵塞等造成；漏喷可能是计算机误动作、电磁阀关不严等造成。前者不能达到对飞轮卸载的目的，后者反而使飞轮错误地增速，二者均造成卫星失控，也就意味着喷气系统失效。

二、失效树的建立

失效树是指某系统的顶事件与造成顶事件发生的各种有关事件以及连接它们的各种逻辑门构成。顶事件为第一级，其下一级（第二级）并列写出导致上一级事件发生的直接原因的失效事件，包括功能失效、设备运行不良、环境因素及人为错误等，两级之间用适合于它们之间逻辑关系的逻辑门相联接。如此类推，逐级向下，直到不能再分解或不宜再分解为止。不能再分解的称为基本事件，在失效树上用圆圈表示，字母B作为它的标注。不宜再分解的代表省略事件，它对此失效树没有必要进一步分析，可以作为单独处理的失效事件，在失效树上用菱形表示，字母D作为它的标注。在图 9 中对照表 1 可以看出，氦瓶失效(B_{010}, B_{011})，肼瓶失效(B_{012}, B_{013})、肼用尽(B_{016})、过滤器堵(B_{035})等均属基本事件，而电源失效(D_{017})、飞轮测速失效(D_{018})等属于省略事件。因为电源失效为卫星的另一个分系统失效，飞轮测速失效可作为姿态控制分系统中的一个部件失效，而不包括在喷气系统中，故它们在喷气系统的失效树中不作进一步分析。

失效树的逻辑门的表示符号与逻辑电路中所用符号相同。

与门(AND门)是满足下述逻辑关系的逻辑门：设$B_i(i=1,2,\cdots\cdots,n)$为门的输入事件，

A为门的输出事件。当$B_i(i=1,2,\cdots\cdots,n)$同时发生时，则$A$发生。这种逻辑关系可用事件的交表示，即

$$A=B_1\cap B_2\cap\cdots\cdots\cap B_n=\bigcap_{i=1}^{n}B_i$$

图8中的逻辑门G_{003}、G_{004}等都是逻辑与门。

或门(OR门)是满足下述逻辑关系的逻辑门，门的输入输出事件同上，当$Bi(i=1,2,\cdots\cdots,n)$中有一个发生时，则A发生。这种逻辑关系可用事件的并表示，即

$$A=B_1\cup B_2\cup\cdots\cdots\cup B_n=\bigcup_{i=1}^{n}B_i$$

图8中的逻辑门G_{001}、G_{002}等都是逻辑或门。

逻辑门除上述两个常用的以外，还有禁门、优先与门、表决与门等等，本文都未涉及，故不详述。

本文讨论的四种方案的失效树就是遵循上述逻辑关系建立的，这四棵失效树见图6——图9。建树过程中有几点技术上的问题，我们是按下列原则处理的：

1）基本事件的失效模式区分，而不是以部件区分。例如，把电磁阀堵和电磁阀漏作为两个基本事件处理。虽然它们都可以认为是电磁阀失效，但是如果作为一个失效事件处理，则在系统的失效逻辑关系上容易造成混乱。

2）把某设备(或部件)分割成若干独立部分可以解决部分冗余设计问题，例如星上计算机主份可以分割成分别对电磁阀、切换阀控制过程中的连续输出错误指令信号和无输出指令信号共四个基本事件，而星上计算机备份只对电磁阀有控制作用（对主份的部分冗余)，故它的失效可以相应分成两个基本事件（参见图3和图7)。

3）因为我们研究的是喷气系统，故取喷气系统以外的作为失效事件的分系统或部件的失效概率为零（见表1)。例如：电源失效(D_{017})、遥控切换阀失效（D_{008})、星体温控失效(D_{019})、飞轮测速失效(D_{018})等在计算中取它们的发生概率为零，即这些事件不发生。这样处理，对建立包括喷气系统在内的更大系统的失效树将更方便。

三、FTA法中的数学概念及应用

在建立失效树的基础上，就可以应用数学方法定量地评价系统方案的优劣了。

设以$P(A)$表示事件A发生的概率，则必有$0\leqslant P(A)\leqslant 1$。若$A$与$B$事件不可能同时发生，记作$A\cap B=\phi$，称$A$、$B$互不相容。若$A$发生与否不影响$B$的状态，反之，$B$发生与否也不影响$A$的状态，则称$A$、$B$相互独立。若$A$、$B$相互独立，则$A$的余$\overline{A}$和$B$的余$\overline{B}$、$\overline{A}$和$B$、$A$和$\overline{B}$也都两两相互独立。

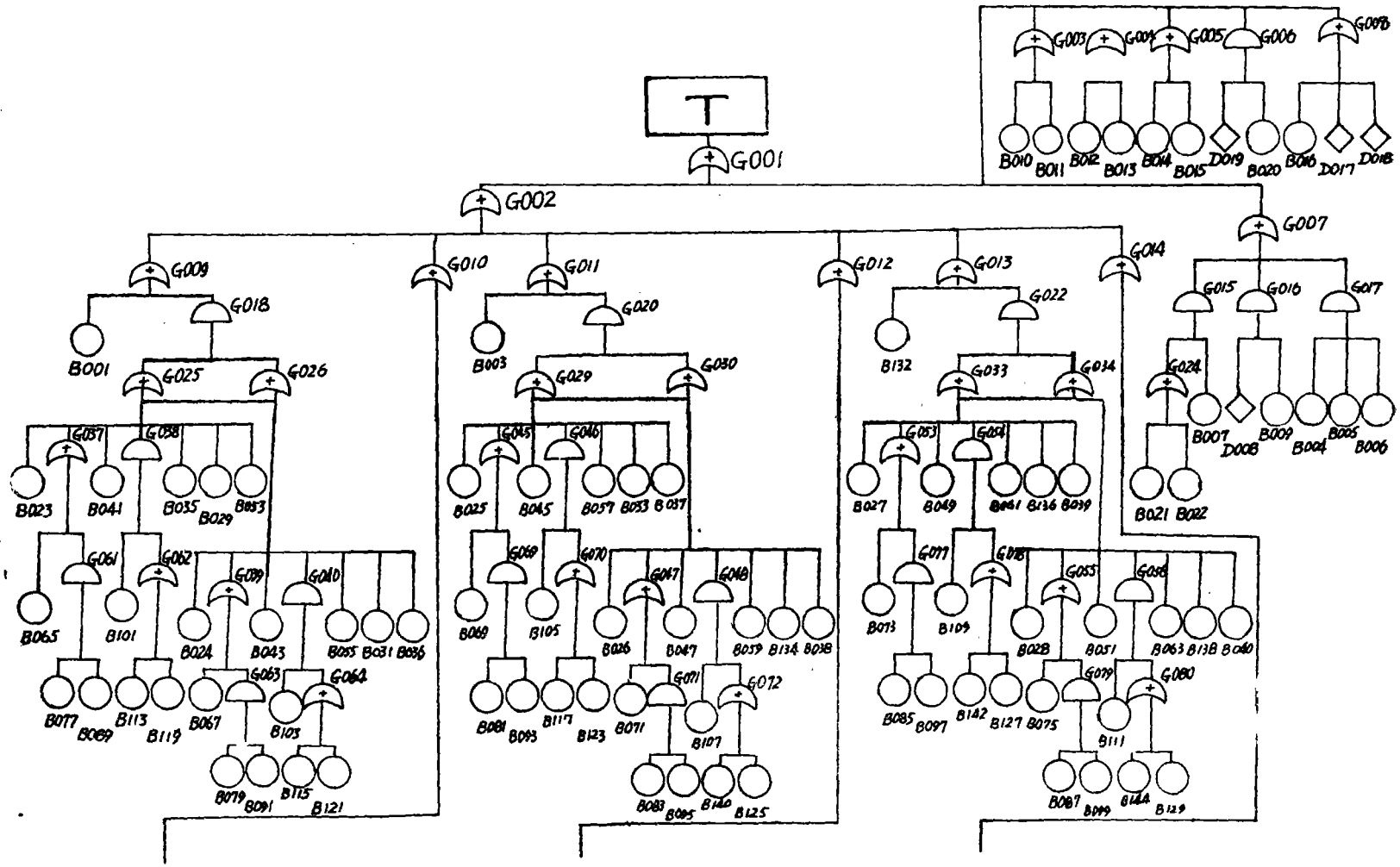
为简化，下面以AB表示$A\cap B$，以$A+B$表示$A\cup B$，有以下运算规律：

$$1^\circ\quad P\left(\bigcup_{i=1}^{n}A_i\right)=\sum_{i=1}^{n}P(A_i)-\sum_{1\leqslant i<j\leqslant n}P(A_iA_j)+$$

$$+\sum_{1\leqslant i<j<k\leqslant n}P(A_iA_jA_k)-\cdots\cdots+(-1)^{n+1}P\left(\bigcap_{i=1}^{n}A_i\right)\qquad(1)$$

若只有两个事件A、B时，上式为

$$P(A+B)=P(A)+P(B)-P(AB)$$


T
G001
G002
G003
G004
G005
G006
G008
B010
B011
B012
B013
B014
B015
D019
B020
B016
D017
D018
G007
G009
G018
B001
G025
G026
G010
G011
G020
B003
G029
G030
G012
G013
G022
B132
G033
G034
G014
G015
G016
G017
G024
B007
D008
B009
B004
B005
B006
B021
B022
G057
G058
B023
B041
B035
B029
B053
G061
G062
G059
G060
B065
B101
B024
B043
B055
B031
B036
G063
G064
B077
B069
B113
B119
B067
B103
B079
B091
B115
B121
G045
G046
B025
B045
B057
B033
B037
G069
G070
G047
G048
B069
B105
B026
B047
B059
B134
B038
G071
G072
B081
B093
B117
B123
B071
B107
B083
B095
B140
B125
G053
G054
B027
B049
B041
B136
B039
G077
G078
G055
G056
B073
B109
B028
B051
B063
B138
B040
G079
G080
B085
B097
B142
B127
B075
B111
B087
B099
B144
B129

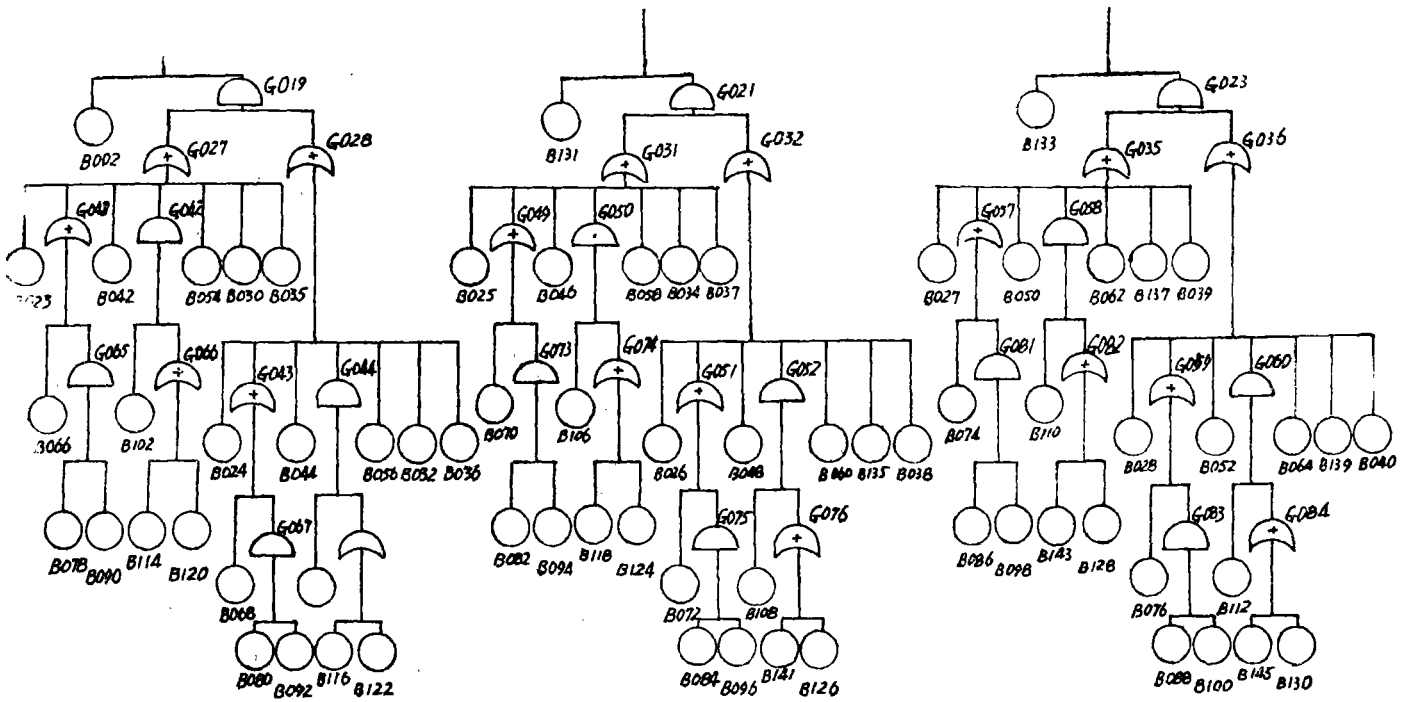
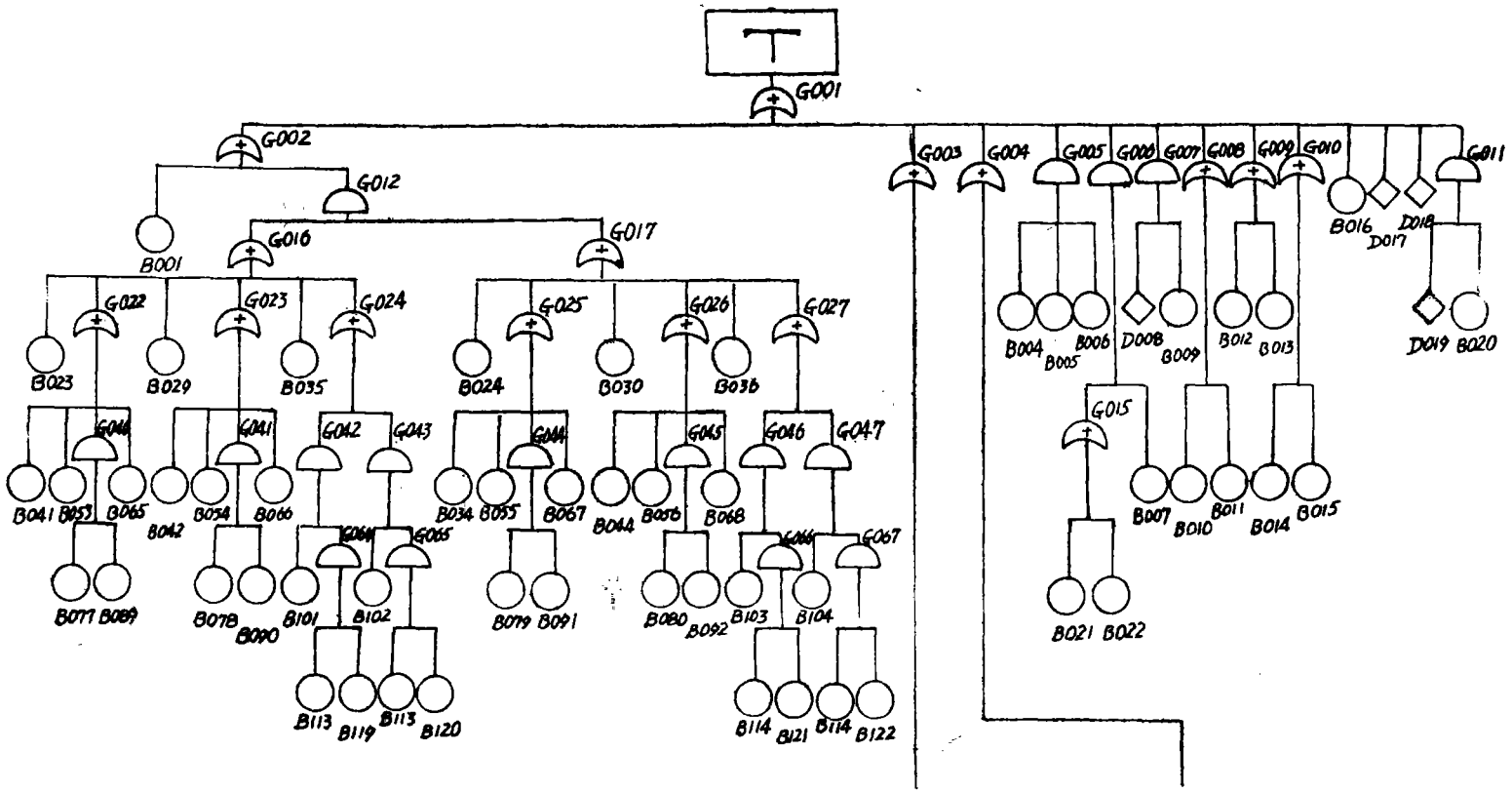


图 6　带转换开关的全路备份方案


G001
G002
G012
G003
G004
G005
G006
G007
G008
G009
G010
G011
B001
G016
G017
B016
D017
D018
B004
B005
B006
D008
B009
B012
B013
D019
B020
G022
G023
G024
G025
G026
G027
B023
B029
B035
B024
B030
B036
G015
G040
G041
G042
G043
G044
G045
G046
G047
B041
B053
B065
B042
B054
B066
B034
B055
B067
B044
B056
B068
B007
B010
B011
B014
B015
G064
G065
G066
G067
B077
B089
B078
B090
B101
B102
B079
B091
B080
B092
B103
B104
B021
B022
B113
B119
B113
B120
B114
B121
B114
B122

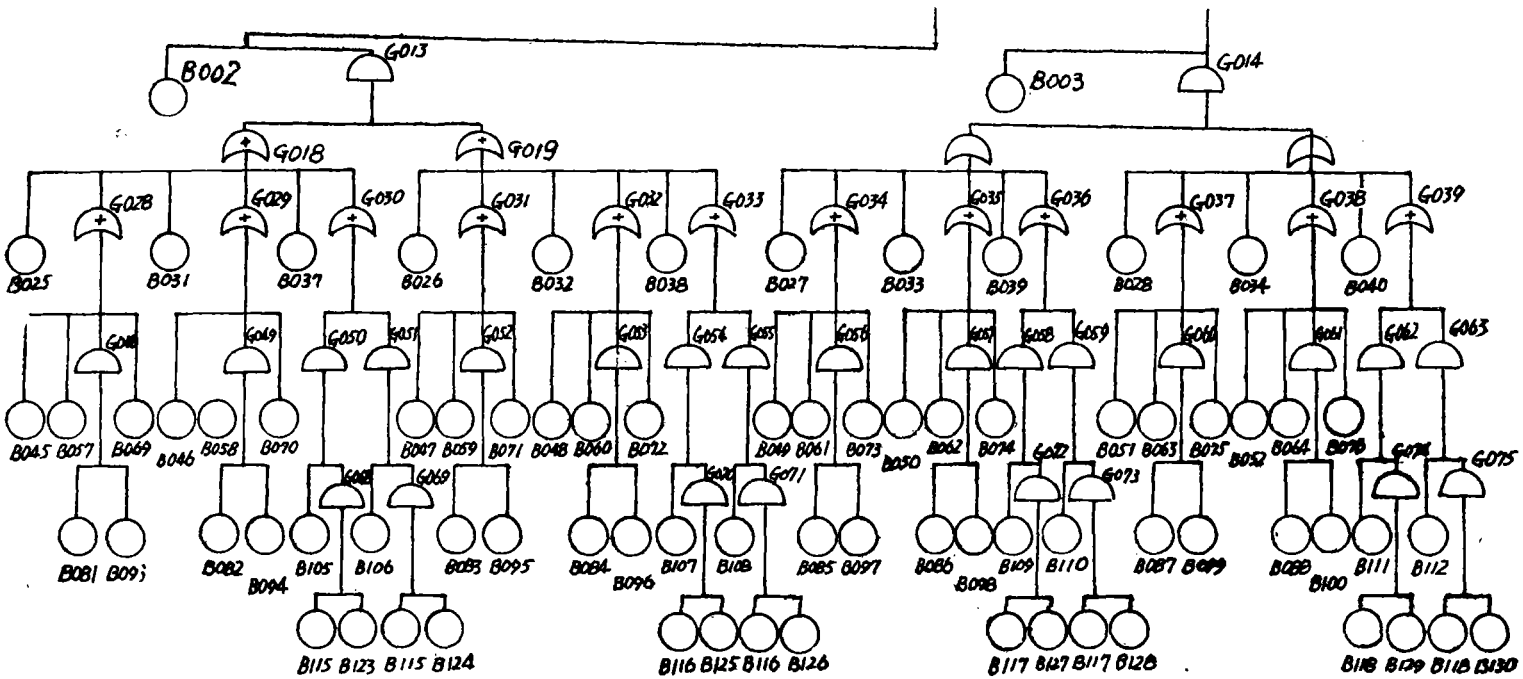
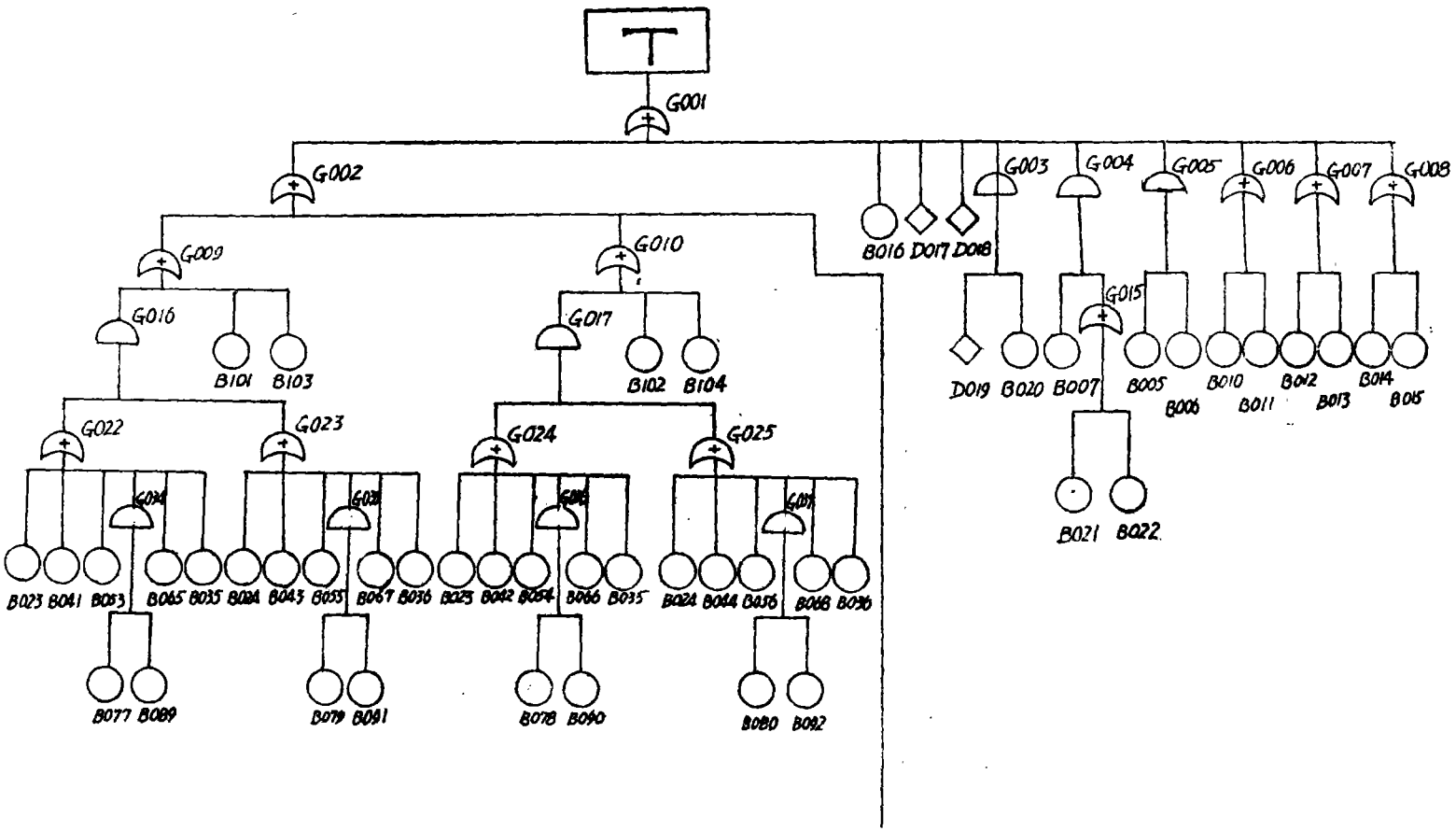


图 7　带转换开关备份方案


T
G001
G002
G003
G004
G005
G006
G007
G008
B016 D017 D018
G009
G010
G016
G017
B101 B103
B102 B104
G022
G023
G024
G025
D019 B020 B007
G015
B005 B006
B010 B011
B012 B013
B014 B015
B021 B022
B023 B041 B053 B065 B035 B024 B043 B055 B067 B036 B025 B042 B054 B066 B035 B024 B044 B056 B068 B036
B077 B089
B079 B091
B078 B090
B080 B092

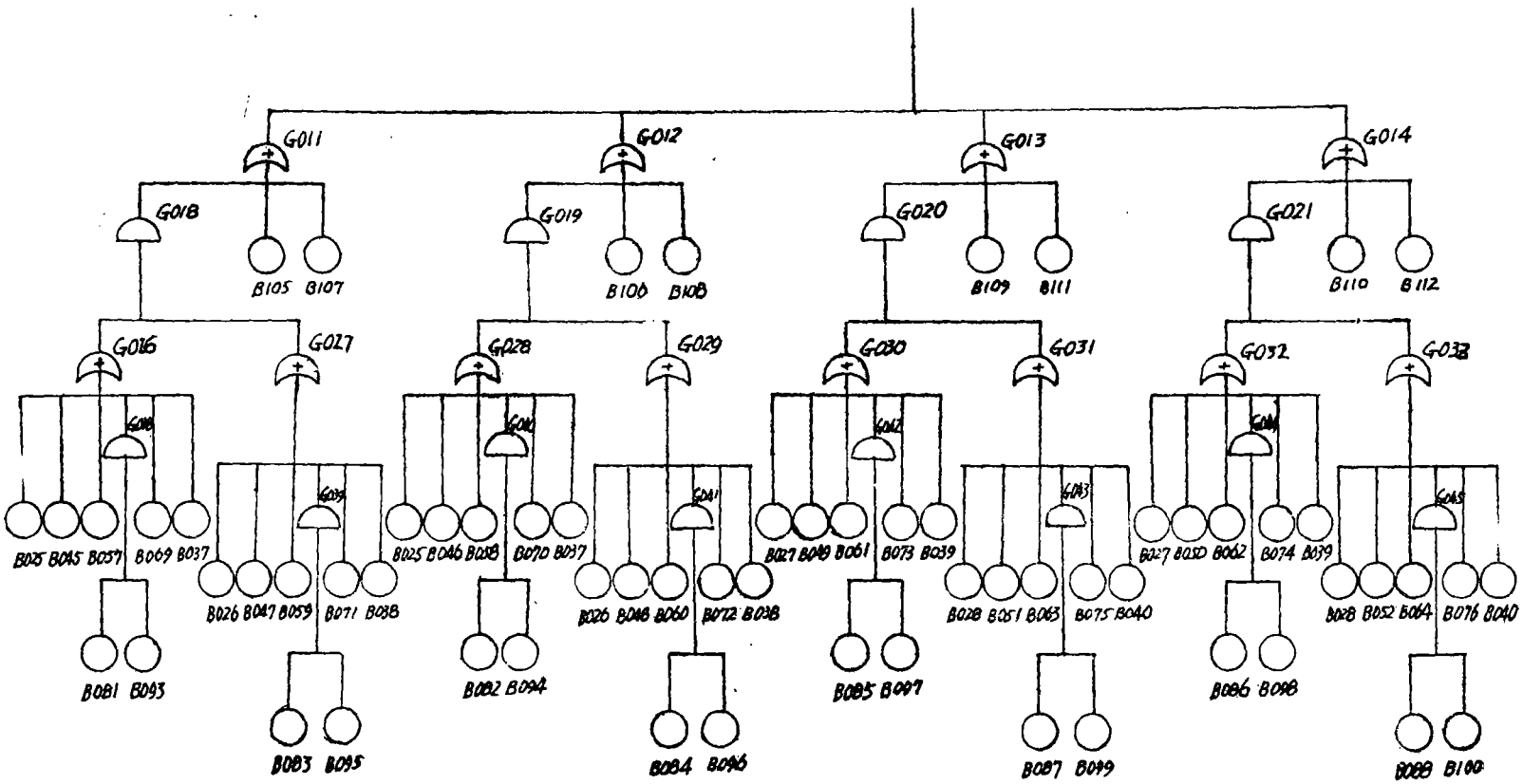

G011
G012
G013
G014
G018
G019
G020
G021
B105 B107
B106 B108
B109 B111
B110 B112
G016
G017
G028
G029
G030
G031
G032
G033
B025 B045 B057 B069 B037
B026 B047 B059 B071 B038
B025 B046 B058 B070 B037
B026 B048 B060 B072 B038
B027 B049 B061 B073 B039
B028 B051 B063 B075 B040
B027 B050 B062 B074 B039
B028 B052 B064 B076 B040
B081 B093
B083 B095
B082 B094
B084 B096
B085 B097
B087 B099
B086 B098
B088 B100

图 8　平行备份方案

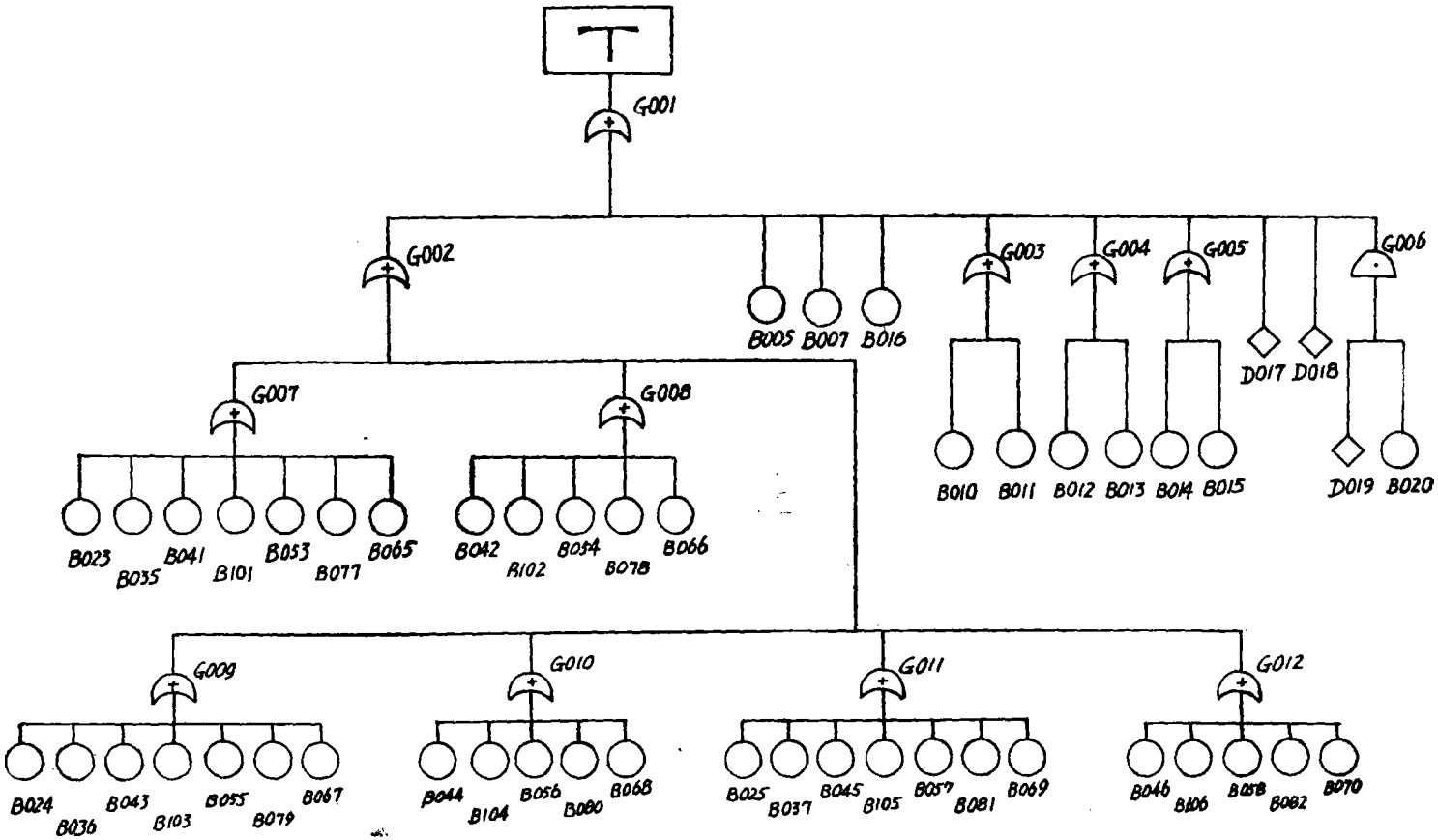

G001
G002
B005 B007 B016
G003
G004
G005
D017 D018
G006
G007
G008
B010 B011 B012 B013 B014 B015
D019 B020
B023 B035 B041 B101 B053 B077 B065
B042 B102 B054 B078 B066
G009
G010
G011
G012
B024 B036 B043 B103 B055 B079 B067
B044 B104 B056 B080 B068
B025 B037 B045 B105 B057 B081 B069
B046 B106 B058 B082 B070

图 9　无备份方案

若 $AB=\phi$，则

$$P(A+B)=P(A)+P(B) \tag{2}$$

式(2)亦可推广到多个事件的情况。

2° 若A、B相互独立，则

$$P(AB)=P(A)P(B) \tag{3}$$

可以推广到多个事件情况，即若$A_i(i=1,2,\cdots\cdots,n)$ 相互独立，有

$$P\left(\bigcap_{i=1}^{n} A_i\right)=\prod_{i=1}^{n} P(A_i) \tag{4}$$

在系统可靠性计算中，常假设组成系统的各部件相互独立，即系统中任意 n 个部件都满足(4)式。

当系统中所有部件可靠性比较高时（一般当部件的不可靠度$Fi(t)\leqslant 0.01$，$i=\overline{1,n}$），可以在失效树可靠性计算中使用(2)式进行近似计算。

失效树的最小割集也是系统方案评价中的一个重要概念。割集就是失效树中一些失效事件的集合$\{x_{i1},\cdots\cdots,x_{il}\}$，且当 $x_{i1},\cdots\cdots,x_{il}$ 都发生时，顶事件必发生。

若 $C_i=\{x_{i1},\cdots\cdots,x_{il}\}$ 是一个割集，从C_i中除去任何一个事件C_i就不再是割集了，则称C_i为最小割集。工程实际中，每个最小割集都对应着系统的一种失效模式。

引进记号：

$$x_i=\begin{cases}1 & \text{失效事件 } x_i\text{发生}\\ 0 & \text{失效事件 } x_i\text{不发生}\end{cases}\qquad i=\overline{1,n}$$

$$\phi(X)=\begin{cases}1 & \text{顶事件}T\text{ 发生}\\ 0 & \text{顶事件}T\text{ 不发生}\end{cases}$$

其中 $X=(x_1,\cdots\cdots,x_n)$

称$\phi(X)$为失效树的结构函数，若 $C_1,\cdots\cdots,C_k$ 为失效树所有最小割集，则

$$\phi(X)=\bigsqcup_{s=1}^{k}\ \prod_{i\in C_s} x_i$$

其中记号

$$\bigsqcup_{i=1}^{n} x_i=1-\prod_{i=1}^{n}(1-x_i)=\max_{i=\overline{1,n}} x_i$$

$$\prod_{i=1}^{n} x_i=\min_{i=\overline{1,n}} x_i$$

于是，若有一个最小割集中的所有失效事件都发生，则有

$$\phi(X)=1-\prod_{s=1}^{k}\left(1-\prod_{i\in C_s} x_i\right)=1$$

即顶事件T发生，由此可得

$$P(T)=P\{\phi(X)=1\}=P(\bigcup_{i=1}^{t}C_i) \tag{5}$$

这就是利用最小割集计算顶事件 T 的发生概率的公式。

应用 Fussell—Vesely 算法可以计算失效树的所有最小割集。它的步骤简述如下：从顶事件往下逐级进行。若顶事件下面是与门，则把它的所有输入（包括门和事件）排在一行；若是或门，则把它们排在同一列。然后对其中的门作下一级分解，直到分解成全部为基本事件为止，得到失效树的全部割集。最后将割集中的基本事件对应不同素数，借助素数之间的不可约性，检验它们是否最小割集（参见〔2〕）。

现以无备份方案——方案之四为例说明上述算法的应用（见图 9）。其中 G_{007}，G_{008}，G_{011}三个门输入事件种类个数都相同，但不含有相同事件，也不包含失效树其他位置出现的事件，不妨把它们的输入事件连同逻辑门看作三个概率相同的模块，用 G'_{007}、G'_{008}、G'_{011}标记。同样 G'_{008}、G'_{010}、G'_{012} 也是三个概率相同的模块。这样做的目的是把模块也当作基本事件处理，从而使系统的计算简化。同时，模块概率的计算不受该模块以外事件的影响，也较易求得。这样，方案之四失效树的所有最小割集为：$\{G'_{007}\}$，$\{G'_{008}\}$，$\{G'_{009}\}$，$\{G'_{010}\}$，$\{G'_{011}\}$，$\{G'_{012}\}$，$\{B_{005}\}$，$\{B_{007}\}$，$\{B_{010}\}$，$\{B_{011}\}$，$\{B_{012}\}$，$\{B_{013}\}$，$\{B_{014}\}$，$\{B_{015}\}$，$\{B_{016}\}$，$\{D_{017}\}$，$\{D_{018}\}$，$\{D_{019}$，$B_{020}\}$。于是，从(5)式有

$$\begin{aligned}P(T)&=1-R(t)=\\&=P(G'_{007}+G'_{008}+G'_{009}+G'_{010}+G'_{011}+G'_{012}+B_{005}+B_{007}+\\&\quad+B_{010}+B_{011}+B_{012}+B_{013}+B_{014}+B_{015}+B_{016}+D_{017}+D_{018}\\&\quad+D_{019}\ B_{020}\}\end{aligned} \tag{6}$$

要利用公式（1）进行精确计算，仍需再将（6）式括号中事件化为不交和（即互不相容事件），具体方法可参考〔2〕。

由于本文研究的系统的部件可靠度较高（不可靠度均为10^{-3}级），可以采用（2）式进行近似计算。根据表 1 的数据，可以算出

$$P(T)=2.9213\times10^{-2}$$

其中 $P(G'_{007})=P(G'_{009})=P(G'_{011})=P(B_{023})+P(B_{035})+P(B_{041})$
$+P(B_{101})+P(B_{053})+P(B_{077})+P(B_{085})=4.9753\times10^{-3}$

$P(G'_{008})=P(G'_{010})=P(G'_{012})=P(B_{042})+P(B_{102})+P(B_{054})$
$+P(B_{078})+P(B_{086})=2.1803\times10^{-3}$

显然，这样计算的结果比用精确公式（1）的计算结果要大一些（见表 2）。

喷气系统的其他三个冗余方案的失效树比方案之四的失效树复杂得多，手算十分困难。本文采用清华大学核能所的失效树程序FTA—1及FTA—3〔1〕，前者求失效树的所有最小割集，后者求失效树的顶事件概率$P(T)$。有关失效树基本事件的数据见表 1，计算结果见表 2。

应该特别指出的是：FTA—3程序求$P(T)$是在各基本事件相互独立的假设下用公式（1）计算的。公式（1）中的$A_i(i=1,2,\cdots\cdots,n)$ 应看作是失效树的所有最小割集。为了简化计算，我们略去三个部件及三个以上部件的最小割集，从而大大减小计算量，也不至影响计算结果的精度（误差分析见后）。

表 1

事　　件	说　　明	基本事件一年时发生概率 F	失 效 率 λ
$B_{001}\sim B_{003}$ $B_{131}\sim B_{133}$	* 某切换阀接口失效	1.75×10^{-4}	2×10^{-8}
B_{004}	主计算机对切换阀连续输出错信号	4.5×10^{-4}	5.1×10^{-8}
B_{005}	主计算机对电磁阀连续输出错信号	4.5×10^{-4}	5.1×10^{-8}
B_{006}	付计算机对电磁阀连续输出错信号	3×10^{-4}	3.4×10^{-8}
B_{007}	主计算机对电磁阀无输出信号	4.5×10^{-4}	5.1×10^{-8}
D_{008}	遥测遥控对切换阀控制失效	0	0
B_{009}	主计算机对切换阀无输出信号	4.5×10^{-4}	5.1×10^{-8}
$B_{010}\sim B_{011}$	* 氦瓶失效	1.3×10^{-3}	1.5×10^{-7}
$B_{012}\sim B_{013}$	* 肼瓶失效	1.3×10^{-3}	1.5×10^{-7}
$B_{014}\sim B_{015}$	* 皮囊失效	3.85×10^{-4}	4.4×10^{-8}
B_{016}	肼用尽	8.756×10^{-4}	1×10^{-7}
D_{017}	电源失效	0	0
D_{018}	飞轮测速失效	0	0
D_{019}	星体温度失控	0	0
B_{020}	* 肼管路加热失效	8.756×10^{-4}	1×10^{-7}
B_{021}	付计算机对电磁阀无输出信号	3×10^{-4}	3.4×10^{-8}
B_{022}	* 计算机转换开关失效	1×10^{-4}	1.1×10^{-8}
$B_{023}\sim B_{028}$	* 某电磁阀接口失效	1.75×10^{-4}	2.0×10^{-8}
$B_{029}\sim B_{034}$ $B_{134}\sim B_{139}$	某切换阀堵	1.314×10^{-4}	1.5×10^{-8}
$B_{035}\sim B_{040}$	* 某过滤器堵	2.62×10^{-3}	3×10^{-7}
$B_{041}\sim B_{052}$	* 某电磁阀堵	1.314×10^{-4}	1.5×10^{-8}
$B_{053}\sim B_{064}$	* 某喷嘴堵	6.04×10^{-4}	6.9×10^{-8}
$B_{065}\sim B_{076}$	某预热器测温失效	4.376×10^{-4}	5×10^{-8}
$B_{077}\sim B_{088}$	某主预热器失效	8.756×10^{-4}	1×10^{-7}
$B_{089}\sim B_{100}$	某付预热器失效	8.756×10^{-4}	1×10^{-7}
$B_{101}\sim B_{112}$	* 某电磁阀漏	1.314×10^{-4}	1.5×10^{-8}
$B_{113}\sim B_{118}$ $B_{140}\sim B_{145}$	某切换阀漏	1.314×10^{-4}	1.5×10^{-8}
$B_{119}\sim B_{130}$	某喷嘴测温失效	4.379×10^{-4}	5×10^{-8}

注一：有"*"的数据系参考〔5〕的数据。

注二：无"."的数据系估计数据。

注三：失效率：$\lambda=-\ln(1-F)/8760$，计算λ是运用$FTA-3$程序的需要。

表2　　各方案失效树计算结果

方案		1	2	3	4
失效树	门数	84	75	45	12
	基本事件数	145	130	100	49
最小割集数	一部件	15	12	21	47
	二部件	208	247	142	60
	三部件	217	109	60	0
	四部件	54	120	6	0
	五部件	0	24	0	0
	六部件	0	12	0	0
	总计	494	524	229	48
顶事件概率 P(T)	半年时	3.998×10^{-3}	3.737×10^{-3}	1.895×10^{-3}	1.457×10^{-2}
	一年时	8.000×10^{-3}	7.484×10^{-3}	3.814×10^{-3}	2.877×10^{-2}
	一年半时	1.203×10^{-2}	1.127×10^{-2}	5.768×10^{-3}	4.299×10^{-2}
可靠度 $R(t)$	半年时	0.996002	0.996263	0.998105	0.98543
	一年时	0.992000	0.992516	0.996186	0.97123
	一年半时	0.98797	0.98873	0.994232	0.95701

注：$P(T)$半年和一年半时的概率值是所有基本事件服从指数分布的假设下计算出的，仅供参考。一年时的$P(T)$值不受上述假设的影响。

结论与分析

一、各方案失效树计算结果表明，平行备份方案——方案之三有明显的优越性，表现如下：

1）它的门数为方案1的0.535，为方案2的0.6。它的基本事件数为方案1的0.689，为方案2的0.769。表明它的结构简单，部件少，因而重量轻。

2）它的最小割集数为方案1的0.463，为方案2的0.437，说明此方案失效模式较少。

3）工作寿命为一年时方案3的系统失效概率仅为方案1的系统失效概率的0.476，为方案2的0.509，为方案4的0.132（几乎少了一个数量级），故本方案可靠性最佳。特别是在部件可靠度降低的情况下，它们的差距将进一步明显增大。

4）从工程方面我们进行了方案3的初步可行性分析，认为它是一个较为理想的方案。

二、关于系统顶事件概率$P(T)$的误差分析

应用FTA—3计算系统顶事件概率$P(T)$时我们略去了三个及三个以上部件的最小割集，

现将这种忽略的误差分析如下：

由于被忽略的最小割集数最多不超过300个（见表2），且基本事件一年时发生的概率F基本不超过10^{-8}（见表1），这样给$P(T)$带来的误差不大于$300\times(10^{-8})^3=3\times10^{-7}$。

此外，本文各方案中有些基本事件之间并不相互独立，如某电磁阀或切换阀的“堵”与“漏”，星上计算机控制切换阀或电磁阀时无信号与连续错信号。以基本事件B_{041}、B_{101}（即第一个电磁阀“堵”及“漏”）为例，它们不是相互独立事件，故不满足

$$P(B_{041}\ B_{101})=P(B_{041})P(B_{101})$$

因而与FTA—3的假设相违背。但是，幸好本文各方案中相互不独立事件均是互不相容事件，故上述二事件满足

$$P(B_{041}\ B_{101})=0$$

所以在用FTA—3计算$P(T)$时，对B_{041}、B_{101}这样一对相互不独立事件，要产生数值为$P(B_{041})P(B_{101})$的误差。本文讨论的四个方案中，这类相互不独立事件均不超过30对（如方案3仅有15对），故给$P(T)$造成的误差不大于$30\times(10^{-8})^2=3\times10^{-5}$。

考虑上述两类误差，可知本文计算$P(T)$的误差在4×10^{-5}之内。

三、为了准确地应用失效树分析方法进行系统的失效概率计算，必须对系统各基本事件发生概率进行测定收集，并且对各种零部件的失效分布规律进行研究。由于这方面的工作刚刚开始，工作量又极大，故往往采用参考、估计的办法解决数据不全的问题，因而就必然影响FTA法计算系统可靠度的精确度。我们认为：在这种情况下，对设计方案进行评价和优选更有重要的实际意义。

空间机械可以应用FTA的几个领域

空间技术的发展要求空间机械的可靠性愈来愈高，它们的故障或失效会带来政治上、经济上的巨大损失以及人身危害。由于这类系统设计的某些必须的技术数据不可能完全靠试验取得，所以不能按一般机械工程所采用的“设计——试验——改进设计——第二轮试验——定型鉴定”的方式进行，而必须采用所谓“首次试验成功”的设计原则。FTA在实现这种设计原则中有着突出的贡献。

FTA可以使人们直观地了解和掌握复杂系统内部件之间的内在联系，明确基本事件导致系统失效发生的途径及程度。除本文讨论的它可以作为系统方案评价手段以外，FTA还可以应用于下列几个空间机械的领域：

1）计算出系统中各零部件的重要度，找出系统的薄弱环节，采用强化办法的提高全系统的可靠度。还可以按部件主次给予合理的可靠度分配，实现系统最优化方案设计。

2）对空间机械系统进行故障预测诊断，制定最佳运行方案，进行事故分析及采取应急措施。

3）系统的安全分析。利用FTA可以比较彻底地找出各种条件下系统可能的潜在失效模式，对系统进行安全审查[6]。

4）系统的风险评价。

5）系统最佳探测器的配置。

6）失效模拟。可以应用失效树作为系统发生失效时信息反馈的模拟模型，把失效树逻

辑设计成计算机程序模拟系统，通过电传打字机通讯来帮助操作人员针对出现的故障做出决策，以保证系统安全。

7）改进系统设计。

FTA 法要求使用者对系统有深刻的理解、具有丰富的经验和较宽广的知识面，否则极易将重要的基本失效事件遗漏或把逻辑关系搞错，所以一般需要有各方面的专家共同建立失效树。

目前使用布尔变量所表示的系统布尔函数仅限于 0 、1 两种状态。对于非两态系统或在非额定工作状况下运行的系统进行分析，尚存在一定困难。在定量计算中需要的技术数据，对于机械部件来说尤为缺乏，有待逐渐积累与完善。

参 考 文 献

[1] 清华大学核能所FTA—1，FTA—3 计算程序。

[2] 曹晋华、程侃；系统可靠性数学理论，1980.

[3] B. L. 阿姆斯塔特；可靠性数学.

[4] 科技大学；“姿控系统”讲义.

[5] N70—34455 ERTS Subsystems Studies.
N70—34456 ERTS Subsystems Studies.

[6] 牧野铁治；《油压と空气压》第 9 卷第 7 号. 1978. 11.