

故 障 树

计 算 机 分 析 及 信 息 管 理 系 统

冶金部安全环保研究院
冶金部长城钢厂四分厂
一九八七年

故障树计算机分析及信息管理系统

故障树分析 (Fault Tree Analysis, FTA) 是安全系统工程中, 最重要的分析方法之一, 它能有效地分析、预测、评价和控制系统中的危险源。利用计算机建立故障树分析系统具有分析速度快, 便于存贮故障树信息, 并可随时打印输出故障树原始信息和分析结果等优点。

一、原理和方法

故障树分析的主要内容有: 最小割集和最小径集的计算和分析; 顶事件概率值的计算; 基本事件重要度的计算和分析。基本事件的重要度包括结构重要度、概率重要度和临界重要度。在这些分析内容中, 最小割集和最小径集的计算是最重要的分析内容, 其它的分析内容都要以最小割集或最小径集为基础。

(一) 故障树最小割集的二进制求法

目前已发展起来了很多种求故障树最小割集或最小径集的计算机算法。如: Fussell算法, Semanderes算法, COMBO算法, 蒙特卡罗模拟, 以及综合COMBO算法和蒙特卡罗模拟而设计的PREP算法程序等。我们开发的故障树分析软件采用的是二进制求最小割集或最小径集的方法。

用二进制求故障树最小割集或最小径集是通过将基本事件转换成二进制数码, 采用自下而上(bottom-up)的方式, 用二进制的逻辑运算来求最小割集。二进制是在计算机的高速内存贮器内进行的布尔代数处理, 可以迅速并有效地计算出含有较多基本事件的大型故障树的最小割集或最小径集。

1. 用二进制求最小割集的步骤

- (1) 用整数 $1, 2, \dots, N$ 重新标记基本事件, 其中 N 是故障树基本事件的总数;
- (2) 从故障树最下面一层的逻辑门开始, 用基本事件表示各个门的割集, 然后将割集转换成二进制行。割集中某一基本事件的号码就等于二进制行中的一个位置;
- (3) 按逻辑门的类型进行割集组合, 并消除超集, 逐渐推进到故障树最上面的一个

逻辑门；

(4) 在最上面的逻辑门进行割集组合和消除超集的运算，便得到用二进制行表示的故障树最小割集。

2 二进制行的转换

假设在故障树中通往第 i 个逻辑门割集数为 K_i 。根据门 i 的类型按下式计算 K_i ：

$$K_i = \begin{cases} K_{i,1} \times K_{i,2} \times \dots \times K_{i,j} \times \dots & (i \text{ 为 AND 时}) \end{cases} \quad (1.1)$$

$$\begin{cases} K_{i,1} + K_{i,2} + \dots + K_{i,j} + \dots & (i \text{ 为 OR 时}) \end{cases} \quad (1.2)$$

若门 i 的第 j 个输入是基本事件，则 $K_{i,j}=1$ ；若第 j 个输入是门 m ，则 $K_{i,j}=K_m$ 。如果门 i 是故障树最上面一个逻辑门，则 K_i 给出故障树的割集数。

对门 i 建立一个 $K_i \times N$ 的矩阵，并把矩阵中的每个位置清零。假设通往 i 门的第一个割集的整数表示是 $\{2, 4, 6, 8\}$ 。通过在矩阵中第二、四、六、八位置上置 1 就把割集 $\{2, 4, 6, 8\}$ 转换成了二进制行，如表一所示。通往 i 门剩下的 $(K_i - 1)$ 个割集可用类似方法写出。

表一

1	2	3	4	5	6	7	8	9		N
0	1	0	1	0	1	0	1	0		0

3 割集的组合

割集的组合对 AND 和 OR 有不同的方式，下面通过具体的实例来说明。

例 1：如图一所示。逻辑门 a 下接门 b 和门 c 。 b 门有两组最小割集 A 和 B ； c 门也有两组最小割集 C 和 D 。

设： $A = \{2, 4, 6\}$ $B = \{1, 3\}$

$$C = \{1,4,5\} \quad D = \{3,6\}$$

a 门是 AND 首先根据式(1.1)计算门 a 的割集数。

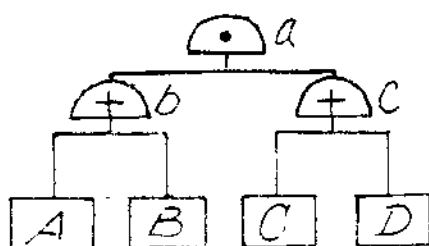
$$\text{已知: } K_b = 2 \quad K_c = 2$$

$$\text{所以: } K_a = K_{a,1} \times K_{a,2}$$

$$= K_b \times K_c$$

$$= 2 \times 2$$

$$= 4$$



把 a 门和 b 门的最小割集转换成用二进制行表示，并对 a 门建立一个 4×6 阶的矩阵。将 b 门的最小割集与 c 门的最小割集相组合，如表二所示，并得到 a 门的四组割集为：

$\{1,2,4,5,6\}$ 、 $\{2,3,4,6\}$ 、 $\{1,3,4,5\}$ 、 $\{1,3,6\}$

表二

		1	2	3	4	5	6
b 门	A	0	1	0	1	0	1
	B	1	0	1	0	0	0

c 门	C	1	0	0	1	1	0
	D	0	0	1	0	0	1

a 门	AUC	1	1	0	1	1	1
	AUD	0	1	1	1	0	1
	BOC	1	0	1	1	1	0
	BUD	1	0	1	0	0	1

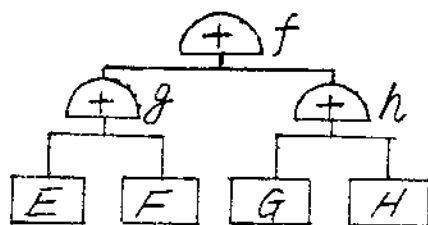
例 2: 在图二中, 门 f 是 OR , 它下面联接着门 g 和门 h 。 g 门有两组最小割集: $E = \{1, 2, 3\}$ 和 $F = \{2, 4\}$, h 门的两组最小割集为: $G = \{3, 4\}$ 和 $H = \{1, 5\}$ 。根据式(1.2)计算 f 门的割集数。

$$K_f = K_{f,1} + K_{f,2}$$

$$= K_g + K_h$$

$$= 2 + 2$$

$$= 4$$



对门 f 建立一个 4×5 阶的矩阵。 f 门是 OR , 它的割集是由门 g 和门 h 的最小割集所组成(见表三), 即 f 门的四组割集为:

$\{1, 2, 3\}$ 、 $\{2, 4\}$ 、 $\{3, 4\}$ 、 $\{1, 5\}$

表三

		1	2	3	4	5
g 门	E	1	1	1	0	0
	F	0	1	0	1	0

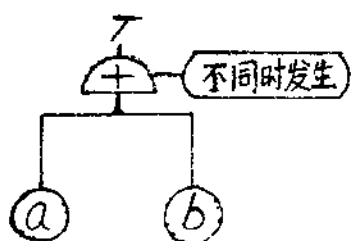
h 门	G	0	0	1	1	0
	H	1	0	0	0	1

f 门	E	1	1	1	0	0
	F	0	1	0	1	0
	G	0	0	1	1	0
	H	1	0	0	0	1

4 消除超集

在消除超集的逻辑运算中, 将运用“异或门”(排斥或门)的运算规则。异或门如图

三所示，当且仅当输入事件中的任一个发生，而其它事件都不发生时，异或门才有输出。表四是异或门的真值表。



表四

a	b	T
0	0	0
0	1	1
1	0	1
1	1	0

假设通过割集的组合得到通往故障树中逻辑门G的割集有四组为：

$$A = \{2, 5, 8\} \quad B = \{2, 5, 8\} \quad C = \{2, 4, 5, 6, 8, 10\} \quad D = \{3, 7, 9\}$$

表五

	1	2	3	4	5	6	7	8	9	10
A	0	1	0	0	1	0	0	1	0	0
B	0	1	0	0	1	0	0	1	0	0
C	0	1	0	1	1	1	0	1	0	1
D	0	0	1	0	0	0	1	0	1	0

$A \oplus B$	0	0	0	0	0	0	0	0	0	0
--------------	---	---	---	---	---	---	---	---	---	---

$A \oplus C$	0	0	0	1	0	1	0	0	0	1
$(A \oplus C) \cap A$	0	0	0	0	0	0	0	0	0	0

$A \oplus D$	0	1	1	0	1	0	1	1	1	0
$(A \oplus D) \cap A$	0	1	0	0	1	0	0	1	0	0
$(A \oplus D) \cap D$	0	0	1	0	0	0	1	0	1	0

表五列出了消除超集的逻辑运算过程。重复的集也通过这一逻辑运算被去掉。表中进行的第一个逻辑运算是“ A 异或 B ”，在表中写作 $A \oplus B$ ，根据前面所介绍的异或门逻辑运算规则，通过二进制行的运算来完成。第一个步骤 $A \oplus B$ 的运算结果得到一个各位置都是0的二进制行，这说明割集 B 是割集 A 的重复集，从而应去掉割集 B 。运算从 $A \oplus C$ 重新开始，得到另一个二进制行，将 $A \oplus C$ 的逻辑运算结果通过“与”逻辑运算与割集 A 组合，记为 $(A \oplus C) \cap A$ ，运算结果又得到一个各位置都是0的二进制行。说明割集 C 是割集 A 的超集，所以应消去超集 C ，保留割集 A 以待进一步分析。接下去进行 $A \oplus D$ 运算，并将运算结果通过“与”逻辑分别与割集 A 和割集 D 组合，记为 $(A \oplus D) \cap A$ 和 $(A \oplus D) \cap D$ 。表中可以看到，割集 A 和割集 D 与 $A \oplus D$ 的交不为0。因此， A 不是 D 的超集； D 也不是 A 的超集。从而故障树中通往逻辑门 G 的最小割集为：

$$A = \{2, 5, 8\} \quad D = \{3, 7, 9\}$$

用二进制行求故障树的最小径集，只需预先作出原故障树的对偶树，然后按上述求最小割集的分法，求出对偶树的最小割集，即为原故障树的最小径集。

(二)用最小割集求故障树顶事件概率值

求出了故障树的最小割集，则可按下式计算故障树顶事件的概率值。

$$G = \sum_{r=1}^K \prod_{i \in K_r} P_i - \sum_{1 \leq r < s \leq K} \prod_{i \in K_r \cap K_s} P_i + \dots + (-1)^{K-1} \prod_{i \in K_1} P_i$$

式中： G —— 顶事件概率值。

P_i —— 基本事件概率值。

K —— 最小割集数。

在故障树分析中，往往遇到很复杂和庞大的故障树，含较多的基本事件，故障树的最小割集数目也很多。要精确计算顶事件的发生概率是非常困难的，即使借助计算机也

需要相当长的时间。从实际出发选用近似的计算方法，既节约时间和人力，也能满足一般的分析精度要求。

事实上，精确计算的结果也未必十分精确。这是因为各基本事件的概率值都要靠人凭经验来最后确定一个可取值，而且影响基本事件概率值的因素很多，不同场合影响程度也不相同。这说明选用并不精确的基本事件概率值进行精确计算，必然得出不太精确的结果。所以用近似算法计算顶事件概率值是适宜的。

顶事件概率值的近似计算方法很多，我们采用的是以下近似公式：

$$G \approx \prod_{r=1}^K \prod_{i \in K_r} P_i$$

这种近似算法认为，虽然在故障树的各最小割集中包含相同的基本事件，但把各个最小割集看作是相互独立的。

(三) 基本事件重要度计算

1. 结构重要度

结构重要度与基本事件在故障树中的位置有关，它是从故障树的结构上分析各基本事件的重要度。

考查某一基本事件 i ，假定其它基本事件的状态固定不变，基本事件 i 的状态从 0 变到 1 时，顶事件的状态变化有三种情况：

$$(1) \quad \Phi(0, x) = 0 \rightarrow \Phi(1, x) = 1$$

$$\text{即} \quad \Phi(1, x) - \Phi(0, x) = 1$$

$$(2) \quad \Phi(0, x) = 0 \rightarrow \Phi(1, x) = 0$$

$$\text{即} \quad \Phi(1, x) - \Phi(0, x) = 0$$

$$(3) \quad \Phi(0, x) = 1 \rightarrow \Phi(1, x) = 1$$

$$\text{即} \quad \Phi(1, x) - \Phi(0, x) = 0$$

第二、三种情况说明基本事件 i 的状态变化对顶事件的状态无影响。第一种情况，

基本事件 i 的状态从 0 变到 1，顶事件的状态也从 0 变到 1，即 $\Phi(1, x) - \Phi(0, x) = 1$ 。说明基本事件 i 的状态变化对顶事件状态有影响；这种情况越多，基本事件 i 就越重要。

n 个基本事件中，把基本事件 i 作为考查对象，改变其它基本事件的状态组合，组合总数为 2^{n-1} 。因此，基本事件 i 的结构重要度 $I(i)$ 为：

$$I(i) = \frac{1}{2^{n-1}} \sum \{ \Phi(1, x) - \Phi(0, x) \}$$

2. 概率重要度

概率重要度是分析各基本事件发生概率的增减，对顶事件发生概率的影响程度。顶事件概率 G 是关于基本事件概率值的多重线性函数，因此，基本事件 i 的概率重要度 $lg(i)$ 为：

$$lg(i) = \partial G / \partial P_i$$

当基本事件概率值都取 $1/2$ 时，基本事件 i 的概率重要度与结构重要度相等。即：

$$I(i) = lg(i) \Big|_{P_j = 1/2 \quad (j = 1, 2, 3, \dots, n)}$$

3. 临界重要度

概率重要度没有反映改善概率值小的基本事件比改善概率值大的基本事件更困难的事实。用基本事件发生概率的变化率与顶事件发生概率的改变率的比值来衡量基本事件重要度，称为临界重要度。

$$Clg(i) = \partial \ln G / \partial \ln P_i$$

临界重要度 $Clg(i)$ 与概率重要度 $lg(i)$ 的关系为：

$$Clg(i) = P_i / G \times lg(i)$$

二. 系统功能与操作

(一)系统简介

1.功能

《故障树分析系统》由下列三部份组成：

(1) 故障树分析存贮

该部份的功能是输入故障树的原始信息；进行故障树的分析计算；存贮原始信息和分析结果。

(2) 故障树查询

该部份可按用户要求查询系统存贮的全部故障树。查询内容包括：故障树矩阵、事件符号与中文对照表、最小割集及发生概率、顶事件发生概率、基本事件的结构重要度、概率重要度和临界重要度。该部份还可删除系统存贮的故障树。

(3) 打印输出分析结果

该部份按用户要求打印系统存贮的故障树信息和分析结果，输出以下六类信息：

- a.故障树矩阵
- b.事件符号与中文对照表
- c.最小割集及概率值
- d.顶事件发生概率
- e.基本事件重要度
- f.重要度排列顺序

2.系统配置

该系统软件是在IBM--PC/XT上开发的，它可适用于IBM--PC/XT、IBM--PC/AT、长城机、以及IBM--PC/XT兼容机。

计算机配制为：

硬件：一套IBM--PC/XT或兼容机

软件：CCDOS2.0以上的汉字操作系统、扩展BASIC 语言

(二)系统操作

本系统的操作全部采用人机对话形式。系统启动后, 屏幕将会出现提示菜单, 供用户选择使用。使用者只需掌握简单的计算机基本操作技能, 便可方便地使用本系统。

系统启动: 将《故障树分析系统》软盘插入A (或B)驱动器后, 关好驱动器门。键入以下命令。

A > FTA <CR>

系统启动后首先出现如图 1所示的屏幕。

```
*****
*               冶金工业部安全环保研究院               *
*               故 障 树 分 析 系 统                       *
*               =====                                     *
* 系统功能:1)本系统采用故障树数理逻辑分析方法。        *
*           2)系统能进行故障树的分析和计算。            *
*           3)系统能存贮故障树的原始信息和分析结果。    *
*           4)系统存贮的信息可供随时查询并打印输出。    *
*               (按任一键进入系统)                        *
*****
```

图 1

该文字屏幕介绍功能。按任一键后, 出现系统功能选择屏幕(如图 2)。

```
*****
*               系 统 功 能 选 择                           *
*               =====                                     *
* 1)故障树分析存贮      2)故障树查询                       *
* 3)打印输出分析结果    0)退出系统                         *
*               请选择系统功能(0—3) ?                      *
*****
```

图 2

1.故障树分析存贮

当选择 1时,将出现如图 3所示的屏幕。该屏幕说明故障树分析存贮时的注意事项。

```
*****
*                               *
*               注 意 事 项               *
*               =====               *
*  1)在使用本系统之前,应先阅读<<故障树分析系统使 *
*    用说明书>>,以便能正确地使用本系统。 *
*  2)在使用该功能时,应按使用说明,将故障树原始信 *
*    息标准化。 *
*  3)如果用户未按使用说明标准化,信息输入将会引起 *
*    系统出错。 *
*                               *
*               (准备好了吗<Y/N> ?) *
*                               *
*****
```

图 3

如果用户未按使用说明将故障树原始信息标准化,则键入 N,系统返回到如图 2所示的屏幕。

故障树原始信息的标准化程序:

- (1) 给要分析的故障树命名。
- (2) 用正整数1,2,3,...,N 重新标记基本事件,其中 N是故障树基本事件总数。
- (3) 用一个英文字母(如:T,A,B,...)或一个英文字母后跟一个0--9的数字(如:T1,A2,B3,...)来表示故障树的顶上事件和中间事件。
- (4) 将故障树转换成矩阵形式。
- (5) 计算故障树中逻辑门的总数;找出故障树中逻辑门的最大输入量。
- (6) 写出各事件符号的中文名称和基本事件的概率值。

输入故障树信息之前，必须进行以上六步工作。
进行故障树信息输入时，将出现如图 4所示的屏幕。

```

*****
*           故 障 树 分 析 存 贮           *
*           =====                       *
*      1) 请键入故障树名称？               *
*      2) 请键入故障树的逻辑门总数？       *
*      3) 请键入故障树中逻辑门的最大输入量？ *
*      4) 请键入故障树的基本事件总数？     *
*      选择：(1--下一页 2--修改)？         *
*****

```

图 4

用户可按屏幕提示输入故障树原始信息。
选择 2时，系统按用户要求修改任一项已输入的信息。
选择 1时，将出现如图 5所示的屏幕。

故 障 树 矩 阵

序号：	事件：	逻辑门：	输入量：	输入事件：
(1)	T	OR	2	A1,A2
(2)	A1	OR	2	B1,B2
(3)	A2	OR	2	L1,L2
(4)	B1	AND	2	C1,C2
(5)	B2	OR	2	C3,C4
(6)	C1	AND	2	1,2
(7)	C2	OR	3	3,4,5

- (8) C3 OR 2 6,7
 (9) C4 ?

选择: (1--下一页 2--前一页 3--修改)?

图 5

用户必须按标准的故障树矩阵进行信息输入。每个屏幕能输入18个逻辑门的信息，输完一屏后，系统自动换屏，直至输完所有逻辑门的信息。故障树矩阵全部输入完后：

选择 3，可对任一逻辑门的信息进行修改。

选择 2，显示前一屏18个逻辑门的信息。

选择 1，显示下一屏18个逻辑门的信息。

当已显示完故障树全部逻辑门的信息后，继续选择 1，将出现如图 6所示的屏幕。

事件符号和中文对照

序号：	事件符号：	中文名称：	概率值：
(1)	I	钩子坠落	
(2)	A1	钢绳断裂	
(3)	A2	吊钩脱落	
(4)	B1	重物拉断	
(5)	B2	机械扭断	
(6)	C1	超负荷起吊	
(7)	C2	钢绳损坏	
(8)	C3	钢绳卷乱	
(9)	C4	吊钩窜顶	
(10)	D1	吊钩上升窜顶	
(11)	D2	吊钩落地反转上升窜顶	
(12)	F1	吊钩一直上升	

(13)	F2	限位失灵	
(14)	1	操作失灵	0.1
(15)	2	?	?

图 6

用户按屏幕提示输入事件的中文名称和基本事件的概率值。每个屏幕能输入18个事件的中文名称和基本事件的概率值，输完一屏后，系统自动换屏，直至输完所有事件的中文名称和基本事件的概率值。全部输入完后：

选择 3，可修改任一事件的中文名称和基本事件的概率值。

选择 2，显示前一屏18个事件符号、中文名称和概率值。

选择 1，显示下一屏18个事件符号、中文名称和概率值。

当已显示完全部事件后，继续选择 1，系统进入运算阶段。屏幕出现如下文字提示：

系统正在运行！

请稍候！！

运算结束后，屏幕出现如下文字提示，并伴有蜂鸣声。然后，系统返回到如图 2 所示的屏幕。

运算结束！

返回主系统！！

2. 故障树查询

当选择 2 时，将出现如图 7 所示的屏幕。

故 障 树 查 询

(共存有< 1>个故障树)

序号： ***** 故 障 树 名 称 *****

(1) 行车、副钩坠落故障树

选择：(1--下一页 2--前一页 3--查询 4--删除 0--退出)？

图 7

选择 0, 退出查询, 系统返回到如图 2 所示的屏幕。

选择 1, 显示下一屏 18 个故障树。

选择 2, 显示前一屏 18 个故障树。

选择 4, 删除系统存贮的故障树。屏幕出现如下文字提示:

删除最后一个记录, 即删除序号为(n)的故障树!!

键入 Y 后, 删除; 键入 N 后, 退出删除。

选择 3, 系统按用户要求查询任一故障树的原始信息和分析结果。当选择故障树后, 将出现如图 8 所示的屏幕。按屏幕提示用户可查询故障树矩阵、事件符号与中文对照表、最小割集及发生概率和基本事件重要度。

```

*****
*           行车主、副钩坠落故障树           *
*           基本事件总数为: 13                 *
*           求出最小割集 ( 12 ) 组              *
*           顶上事件发生概率为: 2.413392E-04    *
*   1> 查询故障树矩阵   2> 查询符号与中文对照表  *
*   3> 查询最小割集     4> 查询基本事件重要度   *
*           选择: (1,2,3,4,0<退出>) ?          *
*****

```

图 8

3. 打印输出分析结果

当选择 3 时, 将出现如图 9 所示的屏幕。

故 障 树 打 印

(共存有< 1>个故障树)

序号: ***** 故 障 树 名 称 *****

(1) 行车、副钩坠落故障树

选择: (1--下一页 2--前一页 3--打印 0--退出)?

图 9

选择 0, 退出打印, 系统返回到如图 2 所示的屏幕。

选择 1, 显示下一屏 18 个故障树。

选择 2, 显示前一屏 18 个故障树。

选择 3, 系统按用户要求, 打印任一故障树。当选择故障树后, 将出现如图 10 所示的屏幕, 并打印<<故障树计算机分析报告>>。

```
*****
*          行车主、副钩坠落故障树          *
*          基本事件总数为: 13                *
*          求出最小割集 ( 12 ) 组            *
*          顶上事件发生概率为: 2.413392E-04  *
*          打 印 输 出 以 下 文 件:          *
*          1> 故障树矩阵          2> 事件符号与中文对照表 *
*          3> 最小割集重要度      4> 顶上事件发生概率      *
*          5> 基本事件重要度      6> 重要度排列顺序        *
*****
```

图 10