中华人民共和国国家标准

UDC 519.28
：007.3

GB 7829—87

故障树分析程序

Procedure for fault tree analysis

1 总则

1.1 目的

故障树分析是系统可靠性和安全性分析的工具之一。故障树分析包括定性分析和定量分析。定性分折的主要目的是：寻找导致与系统有关的不希望事件发生的原因和原因的组合，即寻找导致顶事件发生的所有故障模式。定量分析的主要目的是：当给定所有底事件发生的概率时，求出顶事件发生的概率及其他定量指标。在系统设计阶段，故障树分析可帮助判明潜在的故障，以便改进设计（包括维修性设计）；在系统使用维修阶段，可帮助故障诊断、改进使用维修方案。

1.2 范围

本标准规定了系统可靠性和安全性的故障树分析的一般程序，主要适用于底事件和顶事件均为两状态的正规故障树。

2 引证标准

GB 3187—82《可靠性基本名词术语及定义》。

GB 4888—85《故障树的名词术语和符号》。

3 术语

本标准采用 GB 3187—82 和 GB 4888—85 中规定的术语定义。并补充以下术语：

3.1 模块

对于已经规范化和简化（见 5.3 和 5.4.1）的正规故障树，模块是至少有两个底事件，但不是所有底事件的集合，这些底事件向上可到达同一个逻辑门，并且必须通过此门才能到达顶事件，故障树的所有其他底事件向上均不能到达该逻辑门。

3.2 最大模块

经规范化和简化的正规故障树的最大模块是该故障树的一个模块，且没有其他模块包含它。

3.3 割集

割集是导致正规故障树顶事件发生的若干底事件的集合。

3.4 最小割集

最小割集是导致正规故障树顶事件发生的数目不可再少的底事件的集合。它表示引起故障树顶事件发生的一种故障模式。

3.5 结构函数

故障树的结构函数定义为：

$$\phi(X_1, X_2, \cdots, X_n) = \begin{cases} 1, & \text{若顶事件发生} \\ 0, & \text{若顶事件不发生} \end{cases}$$

国家标准局 1987-06-03 批准　　1988-01-01 实施

其中 n 为故障树底事件的数目，X_1，X_2，…，X_n 为描述底事件状态的布尔变量，即

$$X_i=\begin{cases}1，若第\ i\ 个底事件发生\\0，若第\ i\ 个底事件不发生\end{cases}\qquad i=1，2，\cdots，n$$

3.6 底事件结构重要度

第 i 个底事件的结构重要度为：

$$I_\phi(i)=\frac{1}{2^{n-1}}\sum_{(X_1,\cdots,X_{i-1},X_{i+1},\cdots,X_n)}[\phi(X_1，\cdots，X_{i-1}，1，X_{i+1}，\cdots，X_n)-\phi(X_1，\cdots，X_{i-1}，0，X_{i+1}，\cdots，X_n)]$$

$$i=1，2，\cdots，n$$

其中 ϕ（。）是故障树的给构函数，$\sum_{(X_1,\cdots,X_{i-1},X_{i+1},\cdots X_n)}$ 是对 X_1，X_2，…，X_{i-1}，X_{i+1}，…，X_n 分别取 0 或 1 的所有可能求和。

底事件结构重要度从故障树结构的角度反映了各底事件在故障树中的重要程度。

3.7 底事件概率重要度

第 i 个底事件的概率重要度为：

$$I_P(i)=\frac{\partial}{\partial q_i}Q(q_1，q_2，\cdots，q_n)，\qquad i=1，2，\cdots，n$$

其中 $Q(q_1，q_2，\cdots，q_n)$ 为顶事件发生的概率。在底事件相互独立的条件下，它是各底事件发生概率 q_1，q_2，…，q_n 的一个函数。

第 i 个底事件的概率重要度表示，当第 i 个底事件发生概率的微小变化而导致顶事件发生概率的变化率。

3.8 底事件的相对概率重要度

第 i 个底事件的相对概率重要度为

$$I_C(i)=\frac{q_i}{Q(q_1，q_2，\cdots，q_n)}\cdot\frac{\partial}{\partial q_i}Q(q_1，q_2，\cdots，q_n)\qquad i=1，2，\cdots，n$$

第 i 个底事件的相对概率重要度表示，当第 i 个底事件发生概率微小的相对变化而导致顶事件发生概率的相对变化率。

4 故障树分析的预备步骤

4.1 确定分析的范围

a. 定义系统。包括：系统的设计意图、实际结构、功能、边界（包括接口）、运行模式、环境条件和故障判据。

b. 确定分析的目的和内容。

c. 明确对系统所作的基本假设。包括：对系统运行和维修条件的假设，以及在所有可能的使用条件下与性能有关的假设。

4.2 熟悉系统

对系统应有详细的和透彻的了解。为此，需要系统设计人员、使用维修人员和可靠性或安全性分析人员的合作。对系统进行故障模式和效应分析将会促进对系统故障规律的深入了解，从而有助于正确确定顶事件和建立故障树。

5 工作项目

5.1 确定顶事件

根据分析的目的、系统的故障判据和对系统的了解，确定与系统有关的不希望发生的事件，即顶事件。通常这个事件明显地影响系统的技术性能、经济性、可靠性、安全性或其他所要求的特征。顶事件必须有明确的定义，它是故障树分析的中心。

当我们关心的与系统有关的不希望事件不止一个时，可以将所有这些不希望事件作为同一个假设顶事件的输入事件，从而把问题归结为仅有一个顶事件的情形来进行统一处理。

5.2 建立故障树

建立故障树是一个反复深入、逐步完善的过程，通常应该在系统早期设计阶段开始。随着系统设计的进展和对故障模式的不断增加的理解，故障树随之增大。建立故障树要避免遗漏重要的故障模式。

5.2.1 分析中考虑的事件

建立故障树时考虑的事件应包括硬件故障，也要包括可能发生的软件故障和人为失误，以及所有与系统运行有关的条件、环境和其它因素。

所有故障事件必须有明确的定义，并需指出每个故障事件发生的条件。

5.2.2 共因事件的处理

出现在故障树不同分支中的同一个原因事件称为共因事件。它影响两个或两个以上不同的结果事件。如果某个故障事件是共因事件，则在故障树不同分支中出现的该事件必须用同一个事件标号。当该共因事件不是底事件时，则应该用相同转移符号简化。

5.2.3 建立故障树的方法

建立故障树的方法有演绎法、判定表法和合成法等。演绎法主要用于人工建树，判定表法和合成法主要用于计算机辅助建树。

5.2.4 演绎法建树

演绎法建树应从顶事件开始由上而下，循序渐进逐级进行，步骤如下：

a. 分析顶事件，寻找引起顶事件发生的直接的必要和充分的原因。将顶事件作为输出事件，将所有直接原因作为输入事件，并根据这些事件实际的逻辑关系用适当的逻辑门相联系。

b. 分析每一个与顶事件直接相联系的输入事件。如果该事件还能进一步分解，则将其作为下一级的输出事件，如同a中对顶事件那样进行处理。

c. 重复上述步骤，逐级向下分解，直到所有的输入事件不能再分解或不必要再分解为止。这些输入事件即为故障树的底事件。

对每一级结果事件的分解必须严格遵守寻找“直接的必要和充分的原因”，以避免某些故障模式的遗漏。

5.3 故障树规范化

为了对故障树作统一的描述和分析，必须将建造出来的故障树规范化，成为仅含有底事件、结果事件以及“与”、“或”、“非”三种逻辑门的故障树。

故障树规范化的主要内容包括：

a. 将未探明事件或当作基本事件或删去；

b. 将顺序与门变换为与门；

c. 将表决门变换为或门和与门的组合；

d. 将异或门变换为或门、与门和非门的组合；

e. 将禁门变换为与门。

5.4 故障树的简化和模块分解

故障树的简化和模块分解是减小故障树规模从而节省分析工作量的有效措施。

5.4.1 故障树简化

a. 去掉明显的逻辑多余事件和明显的逻辑多余门。

b. 用相同转移符号表示相同子树，用相似转移符号表示相似子树。

5.4.2 故障树模块分解

a. 按模块和最大模块的定义（见 3.1 和 3.2），找出故障树中的尽可能大的模块。如果有计算机软件可用的话，求出故障树的所有最大模块。

b. 每个模块构成一个模块子树，可单独地进行定性分析和定量分析。

c. 对每个模块子树用一个等效的虚设底事件来代替，使原故障树的规模减小。

d. 在故障树定性分析和定量分析后，可根据实际需要，将顶事件与各模块之间的关系转换为顶事件与底事件之间的关系。

5.5 定性分析

用下行法或上行法求故障树的所有最小割集。

5.5.1 下行法

下行法的基本原则是：对每一个输出事件，若下面是或门，则将该或门下的每一个输入事件各自排成一行；若下面是与门，则将该与门下的所有输入事件排在同一行。

下行法的步骤是：从顶事件开始，由上向下逐级进行，对每个结果事件重复上述原则，直到所有结果事件均被处理，所得每一行的底事件的集合均为故障树的一个割集。最后按最小割集的定义，对各行的割集通过两两比较，划去那些非最小割集的行，剩下的即为故障树的所有最小割集。

下行法求故障树所有最小割集的释例见附录 A 的 A.1。

5.5.2 上行法

上行法的基本原则是：对每个结果事件，若下面是或门，则将此结果事件表示为该或门下的各输入事件的布尔和（事件并）；若下面是与门，则将此结果事件表示为该与门下的输入事件的布尔积（事件交）。

上行法的步骤是：从底事件开始，由下向上逐级进行。对每个结果事件重复上述原则，直到所有结果事件均被处理。将所得的表达式逐次代入，按布尔运算的规则，将顶事件表示成底事件积之和的最简式，其中每一项对应于故障树的一个最小割集，从而得到故障树的所有最小割集。

上行法求故障树所有最小割集的释例见附录 A 的 A.2。

5.6 定量分析

如有足够数据，能够估计出故障树中各底事件发生的概率，则在所有底事件相互独立的条件下，可对故障树进行下述定量分析。

5.6.1 顶事件发生的概率

求顶事件发生的概率的方法有：真值表法、概率图法、容斥公式法、不交布尔代数法等。真值表法和概率图法仅适用于故障树底事件个数少的情形。容斥公式法仅适用于故障树最小割集个数少的情形。当故障树的规模比较大的情况，可用不交布尔代数法。

用不交布尔代数法求顶事件发生概率的释例见附录 B 的 B.1。

5.6.2 重要度

根据实际需要，选择某个或某几个重要度指标，并定量计算出来。在故障树分析中最基本的重要度是：底事件的结构重要度、概率重要度和相对概率重要度。

释例见附录 B 的 B.2。

6 故障树分析报告

以下只是规定了故障树分析报告的基本条款：

a. 目的和范围。

b. 系统描述：
   设计描述；
   系统运行；
   详细的系统边界定义。

c. 假设：
   系统设计的假设；
   运行维修、试验和检测的假设；
   可靠性模型化的假设。

d. 系统故障的定义和判据。

e. 故障树分析：
   分析、数据和所使用的符号表。

f. 结果和结论。

根据特定系统分析的需要，可补充其他的条款，例如：

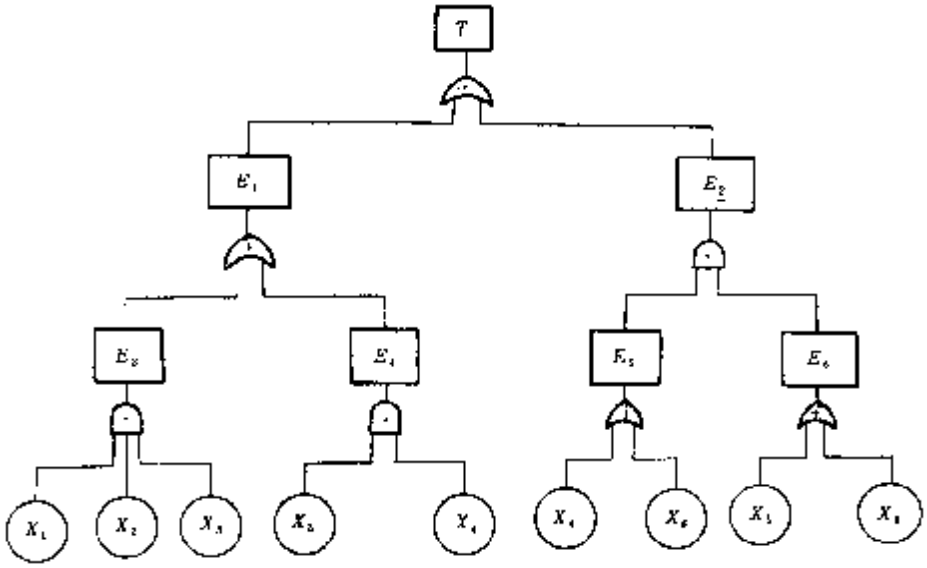
a. 系统的功能框图或电路图；

b. 所用的可靠性数据和资料的摘要；

c. 以计算机可读形式表示的故障树描述。

附 录 A
故障树定性分析的释例
（参考件）

A.1 下行法求故障树的所有最小割集



对于图所给的故障树，下行法的步骤可见下表：

步骤					
0	1	2	3	4	5
T	E_1 E_2	E_3 E_4 E_5E_6	$X_1X_2X_3$ X_3X_4 X_4E_6 X_6E_6	$X_1X_2X_3$ X_3X_4 X_4X_5 X_4X_6 X_6X_5 $X_6X_6=X_6$	$X_1X_2X_3$ X_3X_4 X_4X_5 X_6

步骤 1. 顶事件 T 下面是或门，将该门下的输入事件 E_1 和 E_2 各自排成一行。

步骤 2. 事件 E_1 下面是或门，将该门下的输入事件 E_3 和 E_4 各自排成一行；事件 E_2 下面是与门，将该门下的输入事件 E_5 和 E_6 排在同一行。

步骤 3. 事件 E_3 下面是与门，将该门下的输入事件 X_1，X_2 和 X_3 排在同一行；事件 E_4 下面是与门，将该门下的输入事件 X_3 和 X_4 排在同一行；事件 E_5 下面是或门，将该门下的输入事件 X_4 和 X_6 各自排成一行，并与事件 E_6 组合成 X_4E_6 和 X_6E_6。

步骤 4. 事件 E_6 下面是或门，将该门下的输入事件 X_5 和 X_6 各自排成一行，并与事件 X_4 组合成 X_4X_5 和 X_4X_6；与事件 X_6 组合成 X_5X_6 和 X_6X_6。

至此，故障树的所有结果事件都已被处理。步骤 4 所得的每行均为一个割集。

步骤 5. 进行两两比较，因为 $\{X_6\}$ 是割集，故 $\{X_4, X_6\}$ 和 $\{X_5, X_6\}$ 不是最小割集，必须划去。最后得该故障树的所有最小割集为：

$$\{X_6\}, \{X_3, X_4\}, \{X_4, X_5\}, \{X_1, X_2, X_3\}$$

A.2 上行法求故障树的所有最小割集

对于图 A 1 所给的故障树，从底事件开始，

$E_3=X_1X_2X_3$，$E_4=X_3X_4$，

$E_5=X_4+X_6$，$E_6=X_5+X_6$，

$E_1=E_3+E_4=X_1X_2X_3+X_3X_4$，

$$E_2=E_5E_6=(X_4+X_6)(X_5+X_6)$$
$$=X_4X_5+X_4X_6+X_5X_6+X_6X_6$$
$$=X_4X_5+X_6,$$

$$T=E_1+E_2=X_6+X_3X_4+X_4X_5+X_1X_2X_3$$

故得故障树的所有最小割集：

$\{X_6\}, \{X_3, X_4\}, \{X_4, X_5\}, \{X_1, X_2, X_3\}$

附 录 B
故障树定量分析的释例
（参考件）

对于附录 A 中图所给的故障树，已知所有底事件相互独立，且给定所有底事件发生的概率：

q_1	q_2	q_3	q_4	q_5	q_6
0.02	0.02	0.03	0.025	0.025	0.01

B.1 不交布尔代数法求顶事件发生的概率

用不交布尔代数法求顶事件发生的概率，步骤如下：

a. 由附录 A 求得的所有最小割集，立即可将顶事件表示为各底事件积之和的最简布尔表达式

$$T=X_6+X_3X_4+X_4X_5+X_1X_2X_3$$

b. 将上式化为互不相交的布尔和

$$\begin{aligned}T&=X_6+X_3X_4\overline{X}_6+X_4X_5\overline{X}_6\overline{X}_3+X_1X_2X_3\overline{X}_6\overline{X}_4\ (\overline{X}_4+X_4\overline{X}_5)\\&=X_6+X_3X_4\overline{X}_6+X_4X_5\overline{X}_6\overline{X}_3+X_1X_2X_3\overline{X}_6\overline{X}_4\end{aligned}$$

其中 $\overline{X}_i$ 表示底事件 X_i 的对立事件，即表示第 i 个底事件不发生。

c. 将 b 中已不交化的表达式两端求概率，得顶事件发生的概率

$$\begin{aligned}&Q\ (q_1,\ q_2,\ \cdots,\ q_6)\\&=P\ (X_6)+P\ (X_3X_4\overline{X}_6)+P\ (X_4X_5\overline{X}_6\overline{X}_3)+P\ (X_1X_2X_3\overline{X}_6\overline{X}_4)\\&=q_6+q_3q_4p_6+p_3q_4q_5p_6+q_1q_2q_3p_4p_6\end{aligned}$$

其中 $p_i=1-q_i$ 表示第 i 个底事件不发生的概率。作数值计算，得到顶事件发生的概率为：

$$Q=0.011354$$

B.2 重要度

B.2.1 底事件的概率重要度

由 3.7，第 i 个底事件的概率重要度为：

$$I_P\ (i)=\frac{\partial}{\partial q_i}Q\ (q_1,\ q_2,\ \cdots,\ q_6)$$

$$i=1,\ 2,\ 3,\ \cdots,\ 6$$

将 B.1 c 中的 Q（。）代入，得：

$$I_P\ (1)=q_2q_3p_4p_6$$

$$I_P\ (2)=q_1q_3p_4p_6$$

$$I_P\ (3)=q_4p_6-q_4q_5p_6+q_1q_2p_4p_6$$

$$I_P\ (4)=q_3p_6+p_3q_5p_6-q_1q_2q_3p_6$$

$$I_P\ (5)=p_3q_4p_6$$

$I_P(6)=1-q_3q_4-p_3q_4q_5-q_1q_2q_3p_4$

作数值计算，得各底事件的概率重要度为：

$I_P(1)$	$I_P(2)$	$I_P(3)$
0.000 579 1	0.000 579 1	0.024 52
$I_P(4)$	$I_P(5)$	$I_P(6)$
0.053 70	0.024 01	0.998 6

B.2.2 底事件的相对概率重要度

由 3.8，底事件的相对概率重要度为：

$$I_C(i)=\frac{q_i}{Q(q_1,q_2,\cdots,q_6)}\cdot\frac{\partial}{\partial q_i}Q(q_1,q_2,\cdots,q_6)$$

$$=\frac{q_iI_P(i)}{Q(q_1,q_2,\cdots,q_6)}$$

$$i=1,2,3,\cdots,6$$

其中 $Q(\circ)$ 和 $I_P(i)$ 已分别由 B.1 c 和 B.2.1 求得。

作数值计算，得各底事件的相对概率重要度为：

$I_C(1)$	$I_C(2)$	$I_C(3)$	$I_C(4)$	$I_C(5)$	$I_C(6)$
0.001 020	0.001 020	0.064 78	0.118 2	0.052 86	0.879 5

B.2.3 底事件的结构重要度

在 3.6 给出了底事件结构重要度的定义。底事件的结构重要度完全由故障树的结构所决定，与底事件发生概率的大小无关。理论上已经证明：当所有底事件发生的概率都取$\frac{1}{2}$时，底事件的概率重要度等于底事件的结构重要度。故在 B.2.1 的 $I_P(i)$ 表达式中，用

$$q_k=p_k=\frac{1}{2},\quad k=1,2,\cdots,6$$

代入，作数值计算，得各底事件的结构重要度为：

$I_\phi(1)$	$I_\phi(2)$	$I_\phi(3)$	$I_\phi(4)$	$I_\phi(5)$	$I_\phi(6)$
$\frac{1}{16}$	$\frac{1}{16}$	$\frac{3}{16}$	$\frac{5}{16}$	$\frac{1}{8}$	$\frac{9}{16}$

附加说明：

本标准由中华人民共和国电子工业部提出。

本标准由全国电工电子产品可靠性与维修性标准化技术委员会归口。

本标准主要起草人曹晋华、廖炯生、史定华、苏德清。