陈志业 董 铸 主编

安全系统工程在火力发电厂应用丛书

故障树的编制与应用

邓庆松 郭新华 马献图 编著

北京科学技术出版社

第一章　绪　论

大家知道，安全技术是随着生产的产生而产生，随着生产的发展而发展的。生产技术水平的提高和工业规模的扩大无疑地促进了生产率的提高和社会的进步，同时也增加了公害的影响、事故的频率和规模，因而也就提出了如何防止公害、减少事故的社会问题，安全技术便逐渐形成一门综合性学科。

作为先行的电力工业正以极高的速度迅速发展。为了提高效率，满足用电需要，火力发电厂的机组日趋高参数、大容量化。在火力发电过程中，由于是采用锅炉产生高温高压蒸汽，推动汽轮发电机组高速旋转发电，加上电力生产具有产、供、销同时进行的特点，使得发电设备发生事故的可能性增加、事故性质严重，对社会影响很大。除了造成发电设备的直接损失外，对其它行业产生的间接损失也是巨大的。因此，“安全第一”，一直是电力生产的基本方针。

过去，人们一直是在出现事故后，进行事故分析，查找原因，吸取经验教训，采取预防措施，制定法规，防止事故重复发生，设立专职机构，进行监督检查和宣传教育等。这些工作对安全工作的确起了重要作用。但可以看出这种方法难以改变安全工作落后于生产的状态，难以做到“防患于未然”，究其原因：

首先是由于生产技术不断进步与发展，生产规模日益扩大，单机容量不断扩大，生产设备越来越复杂，人们对新技术中许多潜在性危险因素还认识不清，因此对事故的预防处于被动地位。

其次是按事故发生后进行分析处理的办法，对一个复杂的大系统来讲，只能找出局部的引起事故的原因，解决安全问题陷入片面性，缺乏系统性。

第三由于安全问题是体现于生产过程之中，生产中如果不发生事故，就看不到安全工作的作用，更看不出安全工作的直接经济效益，因此安全工作在平时不易引起人们重视，更不易引起人们对它进行深入研究的兴趣，对研究掌握安全技术缺乏自觉性。

由于习惯于凭经验和直觉处理生产中的安全问题，而不是由表及里地进行综合性分析，因而不能准确地判断和发现潜在的事故危险性，这是过去安全技术工作最大的弱点。过去，往往只能作出“安全”或“不安全”的定性判断，却不能对“生产的安全性有多大？”“发生事故的可能性有多大”等问题作出定量的回答，使人们对生产过程的安全程度心中无数，对如何控制重大事故的发生陷于盲目性，无法驾驭生产过程的顺利进行，保证安全生产。

对过去的安全管理工作进行改进，使之适应生产技术的发展，正日益引起了人们的重视。期望找到一个更有效的办法，能够事先预测到事故发生的可能性，掌握事故发生的规律，作出定性和定量的评价，对危险性加以辨识，从而根据危险性的评价结果提出相应的安全措施，达到控制事故的目的。安全系统工程就是为了这一目的发展起来的一门新兴科学。

第一节　安全系统工程与故障树分析

概略地说，安全系统工程就是用系统工程的观点、原理和计算技术，对系统的危险性进行识别、分析、评价、并根据分

析所得的结果去调整工艺、设备、操作方法、管理制度、生产检修周期和费用投资等因素，使系统可能发生的事故减少到最低限度进而得到控制，并使系统达到最佳安全状态的一种科学方法。

安全系统工程在发展过程中，已形成数十种分析方法，故障树分析是其中的一种。人们为了把握住导致系统发生故障的诸因素，把各种直接的、间接的、环境的和人为的因素与系统故障的关系用一种故障谱形象地表现出来，成为一种系统的失效模型。这种模型用图的形式反映出来，形如一棵倒置的树，因而称为故障树。

故障树（Fault Tree）简称FT，是根据布尔逻辑用图表示系统的特定故障（称为顶上事件）与统计工作为独立的基本故障原因（称为基本事件）之间的相互关系，它是对故障发生的基本原因进行推理分析，然后建立的从结果到原因描述故障的有向逻辑图。这种图是一种逻辑分析过程，遵从逻辑学演绎分析原则，体现了故障与引起故障诸因素的逻辑关系。

所谓故障树分析（Fault Tree Analysis），简称FTA，是根据所研究的系统建立起来的故障树，运用一定规律对故障树进行逻辑运算，定性和定量地对各基本事件在引起顶上事件中的作用和系统的危险性进行分析、预测和评价，进而进行控制的一种方法。

由于故障树具有直观、明了、思路清晰、逻辑性强等特点，既可作定性分析，又可进行定量分析，因而得到广泛的应用。火力发电厂的生产过程和设备结构复杂，发生事故几率较多，引起事故的原因复杂，各原因又是相互影响，对于某一事故发生的原因，要想迅速作出全面正确的判断是很困难的，而要得到系统的危险性有多大的答案更不可能。故障树分析方

法为应用计算机分析创造了条件。针对一个编制好的故障树，用计算机进行分析，完成人脑不能完成的工作，可打破传统的“事故不可知论”的概念。因此，在火力发电厂采用故障树分析方法，对事故的分析、预测和控制将起到有效的积极作用。

第二节　故障树分析的产生与发展

故障树分析方法是安全系统工程最重要的分析方法之一。它的产生与发展，也是生产技术发展的必然趋势和结果。

1957年，苏联成功地发射了第一颗人造卫星以后，美国为了争夺空中优势，匆忙进行导弹技术的开发。开始时，由于对系统的可靠性与安全性考虑和研究不够，在一年半的时间内连续发生了四次重大事故，损失数百万美元，使代价高昂的导弹系统，由于安全方面的缺陷全部报废。事故调查表明，必须从根本上，消除影响安全方面的重大隐患。最后不得不推翻原方案，从头开始研究工作。沉痛的教训迫使人们认识到在研究工作中必须认真考虑系统的可靠性与安全性。于是美国空军在进行导弹系统研究工作前，首先研究了导弹系统的安全性问题。贝尔电话实验室的维森（Watson），1962年提出了故障树分析方法并首先应用于民兵式导弹发射控制系统，解决了研制系统的可靠性和安全性问题，保证了系统的研究成功。

核武器和核工业的出现，安全问题更成了人们极为关心的重要课题。迫于社会舆论，美国原子能委员会和国防部对核设施作了极其严格的限制，有关部门增加了对核设施的安全投资，加强对安全性可靠性的研究。1972年美国三里岛核电站发生事故，引起了公众的恐慌和指责。为此，美国总统停止休假，赶回白宫，美国政府组织了麻省理工学院拉斯姆逊

（Rasmusson）教授为首的十几名专家，用了两年时间，耗资三百万美元，对商用核电站作了风险评价。1974年发表了题为"原子能电站风险评价"的报告，即著名《拉氏报告》。该报告收集了原子能电站各部位历年发生的事故，分析了事故发生的概率，大量采用故障树和事件树分析，依据各种故障数据，对核电站的安全作出了令人信服的定量评价。这是故障树分析方法一次成功的应用实例，在社会上引起了极大反响，受到世界各国的广泛重视。

一方面，生产技术的发展推动了新产品新技术的开发；产品的安全性要求越来越高，又需要人们寻求提高系统安全性的新方法、新途径。故障树分析方法就这样在研究、设计、制造、生产等各个环节开始应用并推广起来。另一方面，随着系统工程学、概率论、图论、集合论的发展，又使故障树分析方法得到迅速的发展与完善，特别是电子计算机技术的发展，满足了大型故障树的复杂计算要求，为故障树分析的深入研究创造了条件。随着故障树分析方法广泛地应用于设计制造与生产实践，必将对安全技术的发展和安全管理的现代化起到推动作用。

我国对故障树分析的研究和应用是从70年代开始的。1976年清华大学核能技术研究所根据国外文献的报导，对于故障树在核反应堆安全评价方面的应用作了初步探索，接着又在电视机生产等系统上作了实际研究，取得了可喜的成果。1978年，天津东方化工厂首次试用故障树分析方法对生产中的事故进行分析和控制，取得了一定的经验。1982年，在北京市劳动保护研究所召开了第一次安全系统工程座谈会。以后，这种分析方法开始在许多省、市和企业中试行和推广，充分显示了它的科学性和先进性。近几年来，我国机械、冶金、军工、化工、铁

路、矿山等行业都先后推广了安全系统工程，积累了不少经验。实践证明，故障树分析方法完全适用于我国国民经济各部门、各行业的安全管理，在电力工业中也同样具有广泛应用范围和发展前景的。

第三节　故障树分析的步骤

故障树分析过程大致可分为以下十个步骤。当然，根据分析的要求和人力，物力条件可选取其中几步进行。

1.确定所要分析的系统

首先要确定进行分析的系统所包含的内容及其边界范围。例如一个火电厂，首先要确定分析的对象是锅炉、汽机还是发电机，锅炉本体中是燃料系统、给水系统还是蒸汽系统。只有明确了系统，才能有明确的对象，作出别人能理解的正确分析。

2.熟悉系统

熟悉系统，是正确地编制故障树，进而能作出正确分析的关键。要求确实了解系统的构成、功能、工艺（或生产）过程、操作运行情况、保护设备、各种重要参数和越限指标等，必要时还应掌握工艺流程图及结构布置图，以作为编制故障树的依据。在熟悉系统的基础上作出的分析才能反映系统的客观实际。

3.调查系统发生的事故

尽量广泛地调查所分析系统的所有事故，既包括过去和现在已发生的事故，也包括估计将来可能发生的事故；既要了解所研究的本系统发生的事故，也要了解同类系统发生的事故。如对某一型号的锅炉进行分析时，同时也应尽量收集掌握其它型号锅炉发生的事故，详尽了解各次事故的分析资料。这些，对于编制故障树，找出基本事件，是有很大帮助的。

4.确定故障树的顶上事件

顶上事件是系统不希望发生的事件。根据事故调查和统计分析的结果，按照事故发生的频率和事故损失的严重性两个方面，将容易发生且后果严重或偶尔会发生但损失很大的事故作为不希望发生的事件，即顶上事件。例如，在锅炉设备的事故中，造成锅炉停炉的事故显然是不希望发生的，因此，可以将这事故确定为顶上事件。

5.调查引起顶上事件发生的基本事件

在熟悉系统、分析事故的基础上，找出引起顶上事件发生的各种因素，按照安全系统工程的分析内容，这些因素应包括：人、机、管理、环境，即包括机械设备故障、操作失误、维修质量和维护不良、管理指挥错误，影响顶上事件发生的环境不良等。在全面分析的基础上确定它们的因果关系和逻辑关系，最下面的原因事件即为基本事件。

6.编制故障树

在以上工作的基础上，可以着手编制故障树。按照演绎分析的方法，从顶上事件开始，一级一级往下分析各自的直接原因事件，直到基本事件为止。根据相互间的逻辑关系，用规定的逻辑门连接上下层事件，就形成了一个事故逻辑关系图，即为故障树。对所画的故障树要反复推敲、检查，看其是否符合逻辑分析原则，即：上一层事件应是下层事件的必然结果，下一层事件应是上层事件的充分条件。同时还应反复核实直接原因事件是否全部找齐，具有定量意义。

7.定性分析

故障树的定性分析，是根据编制的故障树，利用布尔代数进行化简，然后求取故障树的最小割集和最小径集。最小割集是导致顶上事件发生的基本事件的最小集合；最小径集是顶上

事件不发生所需的最低限度的径集。由此作出基本事件的结构重要度分析，得出定性分析的结论。定性分析是由故障树的结构出发，找出基本事件在故障树结构中所占的地位，其目的是分析该类事故的发生规律及特点，找出控制事故的可行方案，并按轻重缓急采取对策。

8.定量分析

定量分析是用定量的观点对故障树中顶上事件发生的概率和各基本事件的重要度作出分析。首先需要确定各基本事件的故障率，计算其发生概率。以此为基础求取顶上事件的发生概率，并算出各基本事件的概率重要度和临界重要度等。

9.比较分析

将定量分析中求得的顶上事件发生概率与通过统计分析得到的事故发生概率进行比较，如果两者相差很大，则应考虑故障树图是否正确，检查基本原因事件是否找齐，上下层事件间的逻辑关系是否正确，各基本事件的故障率确定得是否合适等。若有问题，应返回第五步重新检查分析并对故障树进行修改。

10.安全性评价

经过定性和定量分析后得到的顶上事件发生概率如果超过预定的目标值，则要研究降低事故发生概率的各种可能。由事故发生频率与事故损失严重度得到的损失率超过允许的安全指标时，必须予以调整。由定性定量分析的结论中得到多种降低事故发生频率的方案，根据人力、财力条件选取最佳方案 确定设备改造和加强人为控制。

以上十个步骤可以用故障树分析程序流程图表示（图1—1），在实际分析应用中可根据需要和可能任选其中几项进行分析，但编制出正确的故障树是进行分析工作的基础，至于定性和定量分析，对于较大的故障树，可以借助电子计算机进行。

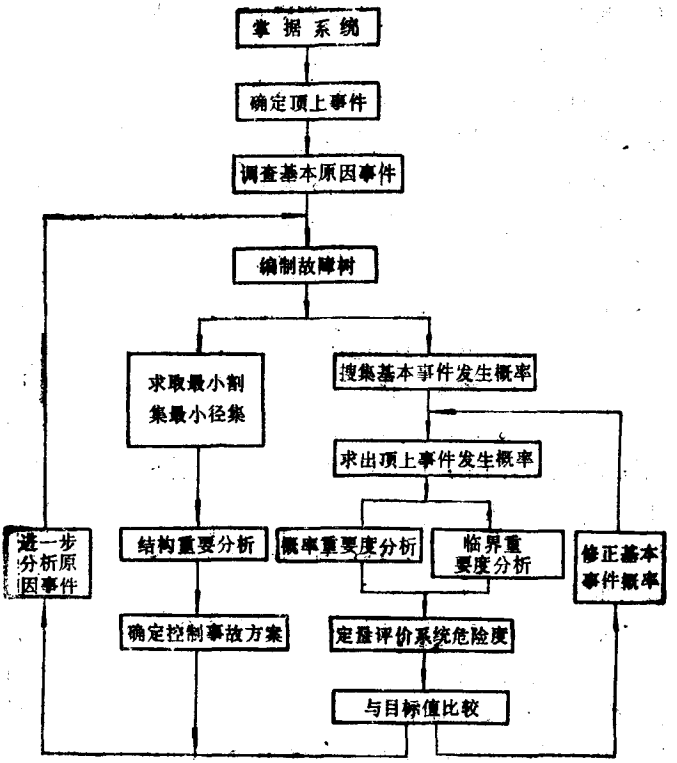


图 1—1　故障树分析程序

第四节　故障树分析的特点

故障树分析是一种最适于对系统进行全局分析的工程逻辑方法，故障树正确反映了事故与产生原因之间的内在关系，故障树分析就是根据对于所研究的系统建立起来的故障树，经过逻辑运算，用量的关系反映出特定事故（即顶上事件）与基本故障原因（即基本事件）之间的关系，因而是一种静态的微

观分析法。在实际应用中看出它具有以下特点：

（1）故障树是用逻辑门将事故发生的原因和结果连接起来的有向树图。由于在编制过程中就是通过对事故原因进行详尽分析，并将它们的内在关系用逻辑门给予反映，因此它能直观、形象地描绘事故发生情况，清晰地反映出顶上事件与基本原因事件之间的逻辑关系，具有鲜明的逻辑性。

（2）故障树是对被研究系统进行了深入分析后编制出来的，它不是对某一类或某一次特定事故原因的简单分析，而是详细占有历次事故资料即同类系统所出现的或估计会出现的事故分析资料后，将某一特定事故和其产生原因用图形象地表现为一个故障谱。因此它可以全面地、系统地概括出所有导致事故发生的各种因素，既包括设备和机械部件的故障，又包括了环境和人的因素；既考虑了设计、制造的缺陷，又考虑到运行和维护的问题，是对人、机、管理、环境四大要素的综合分析，具有很强的系统性。

（3）故障树是根据因果关系确定的各层事件用逻辑门连接起来的图形，因而具备可以直接利用该图进行计算的可能。由故障树求取最小割集，可以掌握事故发生的各种可能性，可以直观比较系统的危险性；求取最小径集，可以了解防止事故发生的各种途径，选择控制事故的最佳方案，也可以直观地比较系统的安全性，对系统作出定性分析。利用故障树可以在掌握了基本事件发生概率的基础上，进行定量分析，求得顶上事件的发生概率，从而对事故发生进行预测，对系统的安全性进行评价，确立改善系统安全性能的最佳方案等等。故障树分析方法，对“危险性”和“安全性”问题的回答，已经超脱出主观感觉领域的议论，因此作为一种分析方法具有明显的科学性。

（4）一个完整的故障树充分地反映了生产工艺、全过程

管理的各个环节，本身就是一套完整的事故分析资料，既可作为进行生产工艺，安全教育的辅助教材，又可作为分析人员充分理解系统的工具，还具有把分析结果以第三者能理解的形式作信息传递的优点。因此它是传递安全生产知识、进行安全教育和事故分析的工具，具有较大的适用性。

（5）故障树分析是安全系统工程的重要分析方法之一，同时也是安全系统工程发展的重要标志。故障树分析方法将量的概念引入安全评价，就可利用电子计算机进行复杂的计算分析，完成人工难以完成的工作。因此使得故障树分析可以与其它分析技术综合应用，互为补充，以取得更好的应用效果。这种分析方法既可以被具有一般数学知识的人们掌握，在研究应用方面具有很大的通用性，又给有志于进行深入研究的人们，具有广阔的发展前景。

由于故障树分析具有这些特点，因而在它发展起来的不长时间里，已经得到了广泛的推广和应用。

第二章　故障树的编制

从第一章介绍的故障树分析步骤中看出，编制一个好的故障树是进行故障树分析的基础。本章将着重讨论故障树的编制方法，并结合在试点单位的实践经验给读者介绍一些编树过程中应注意的问题和技巧。

第一节　故障树的符号及其意义

故障树是由各种事件符号和它们相互连接的逻辑门组成的。事件是树的节点，逻辑门是表示一节点与其它节点连接性质的符号。这里介绍几种最常用的符号。

一、事件符号

1.矩形符号 

矩形符号表示顶上事件，或中间事件，是需要进一步往下分析的事件。将事件名称扼要地记入矩形框内。这里需要指出，在用矩形符号表示顶上事件时，要求对顶上事件的描述要明确，切忌含糊不清。例如：把“锅炉灭火放炮”作为顶上事件，就不够明确，因为不知道是指锅炉灭火还是指锅炉放炮，改为“锅炉灭火后放炮”作为顶上事件就明确多了。对于这样一个顶上事件，找到引起锅炉灭火后可能引起放炮的各种原因，就可以着手编制故障树。为了通俗易懂，将“放炮”改为“炉膛爆炸”，更加术语化，因此在最后确定顶上事件时采用“锅炉灭火后炉膛爆炸”进行描述。由此可见，正确选择顶上事件是件重要的事情。

2.圆形符号 

表示基本原因事件，或称基本事件。包括设备故障、人的失误、环境因素等。它表示最基本的、不需要继续往下分析的事件。如："焊接质量差"，"管内有异物"，"给水自动调节失灵"等，都属于基本事件，可用圆形符号表示。

3.屋形符号 

表示正常事件。它是系统在正常状态下发生的正常事件。也有人称为激发事件。如锅炉炉膛里烟气对省煤器等受热面的冲刷称为"正常磨损"等，都可用屋形符号来表示。

4.菱形符号 

表示省略事件。以下三种情况均可用菱形符号表示：

（1）不必进一步分析的事件，如故障树中凡是因设计和制造质量等问题，这样的事件不必进一步分析。

（2）某些由于不可抗拒的原因，如自然灾害中的雷击事件等不能进一步分析的事件。

（3）由于情报不足，不能进一步分析的事件。

四种符号中，除矩形符号外，其余三种符号均表示无须进一步往下分析的事件，称为基本事件符号。和应用矩形符号一样，将事件简要而确切地写在符号内。读者还可根据实际需要选择另外的图形符号，以便详细区别事件种类。

二、逻辑门符号

逻辑门符号是用来表示顶上事件、中间事件和基本事件间的逻辑关系的符号。用逻辑门符号可以正确反映各事件之间的数理逻辑关系。逻辑门符号大体上有：与门、或门、条件与

门、条件或门和限制门等等。为了便于读者掌握，这里以实例说明各种门的意义和作用。

1.与门 

与门是表示输入B_1、B_2和输出A之间为逻辑乘的关系。A为输出端，B_1、B_2为输入端。在输入事件B_1、B_2同时发生的情况下，输出事件A才发生，两者缺一不可。一般表达式为：$A=B_1 \cdot B_2$。

例如：锅炉发生满水事故的直接原因有三个：①水位上升；②事故放水门失灵；③司炉错误调整水位。它们之间为逻辑乘的关系，如图2—1所示。只有B_1、B_2、B_3同时发生，才会导致事件A发生。

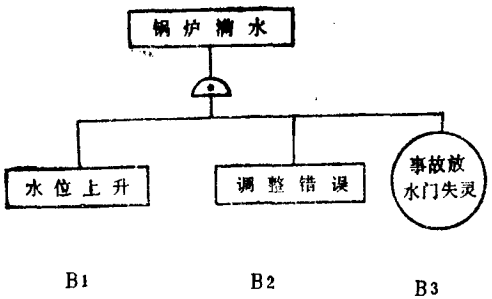


图 2-1 与门实例

在实际生产活动中用与门连接上下层事件的情况是很多的。例如：使用手持电动工具触电，原因可能是漏电、没有安全保护措施、保护接地(或接零)失效三个，只有三者同时发生才会导致触电事故。又如锅炉炉膛上层受热面结焦是炉膛出口

温度高和燃煤灰熔点低同时存在的结果。以上例子中的输入和输出事件间的关系，在编制故障树时都应用与门来反映。

2.或门 

或门是表示输入B_1、B_2和输出A之间为逻辑加的关系。A为输出端，B_1、B_2为输入端，当输入事件B_1、B_2中任何一个事件发生都会导致事件A发生。这种关系的一般表达式为：$A=B_1+B_2$。对有若干个输入事件时，$A=B_1+B_2+\cdots+B_n$。

〔例1〕“油膜破坏”和“大瓦温度高”都是造成“钢球磨煤机烧大瓦”的直接原因，而且它们任一个发生都会引起烧大瓦，因此，它们之间遵照或的逻辑关系。按照结果事件在上，直接原因在下的原则，在故障树中它们被表示成图2—2所示的或门结构。

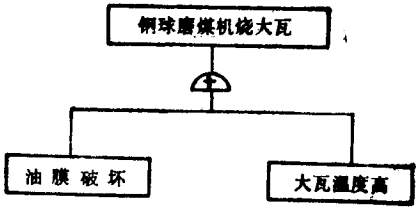


图 2—2 或门实例(1)

〔例2〕670t/h锅炉受热面的水冷壁管泄漏共有下列原因：管子局部严重腐蚀；掉大焦砸坏水冷壁管；管子局部吹损；安装检修质量差；水冷壁管膨胀不均；管子局部过热等。这六种导致水冷壁管泄漏的原因中，任一个发生都有可能导致上层事件发生，因此用或门连接如图2—3所示。

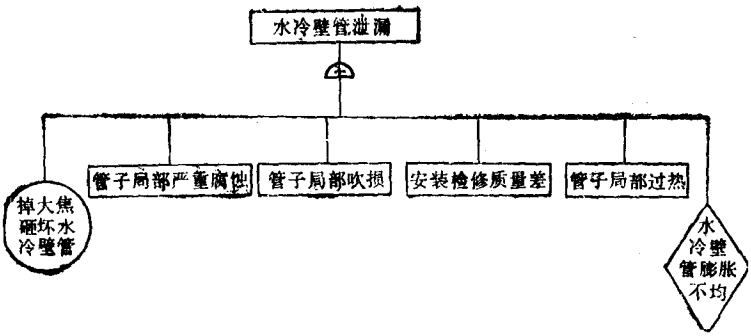
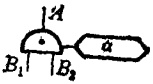


图 2-3 或门实例(2)

这六种直接导致水冷壁管泄漏的原因事件，实际上是六种不同泄漏机理的逻辑并列，将它们罗列出来便于分别进行详细分析。

3.条件与门



条件与门表示除输入事件B_1、B_2同时发生外，还要在满足条件α的情况下，输出端A事件才发生，否则就不发生。条件记入六边形框内。它是一种逻辑修饰符号。通常在进行故障树分析时将条件当作一个基本事件处理，根据条件与门的定义，输入事件和条件一起与上层事件构成与门关系，其逻辑表达式为：$A = B_1 B_2 \alpha$。

例如，在配电系统发生低压触电死亡的直接原因事件是：人体接触带电体；安全联锁保护装置失效；抢救不力等，但这些直接原因事件同时发生也并不一定死亡，造成死亡最终取决于通过人体心脏的电流I与通电时间t的乘积$It > 50mA \cdot s$，这一条件就应在条件与门的六边形符号内注明，以表示条件限制，