系统安全与事故分析技术论文集

劳动人事部劳动保护科学研究所

系统安全与事故分析技术论文集

〈译文集〉

劳动人事部劳动保护科学研究所

1984.10 北京

前　言

建立我国劳动保护科学管理的新体制，首要任务是开拓系统安全工程和系统安全管理。

为大幅度降低伤亡事故，务必急速普及、推广故障树分析（FTA）等系统分析方法；安全预测法；事故致因判定和安全评价；事故分析和安全对策以及新型防护装置（安全互锁器等）的应用等系统安全知识。

劳动人事部劳动保护研究所的工程师们选译了系统安全方面的论文廿五篇并汇编成册，以飨读者。本书内容包括系统安全的基本理论和方法；计算机在安全上的应用以及产品系统安全设计等新知识。内容虽不尽全面，专业术语虽有待推敲，但从引进国外先进的安全软科学知识方面，他们是做出了贡献的。

本译文集由王斌工程师选编、总校，国伟超、刘奇英等同志做了大量组织工作，每篇末署名的各位译者付出了辛勤劳动，这是应向他们致谢的。

由于编印译文集缺乏经验，有疏漏之处敬请读者批评指正。

劳动人事部劳动保护科学研究所

所长　隋鹏程副教授

1984.10

目　录

关于工艺系统故障树编制方法的研究

（报告一）

——基本算法及其应用——

（日）佐山隼敏

摘　要

本文提出了以化工厂、原子能发电厂等为对象编制系统故障树的一种方法，本法以有向图解和自动控制的方框图的研究方法为基础，绘制记载了各种故障模型的方框图，并根据方框图，给出了逐次展开树的基本算法，按该法来编制具有反馈回路的流量控制系统的故障树，由此阐明其树的编制过程，并且也揭示了应用上的特性。

1.绪言

故障树分析法是能够定量评价大规模系统的危险的方法之一，过去已被应用于对原子能发电、化工厂和LNG（液化天燃气）基地的危险评价。然而，要把这些系统作为对象来编制故障树却是极为困难的问题。

世界各国也已就故障树作成的算法提出若干方案，但尚没有一种方法达到确立作成算法的阶段，危险评价的实施情况，各国也大不相同。在美国有专门从事危险评价的工程技

术公司，所以各企业把一切委托给该公司即可。而在我国就必须各企业对自己公司的工厂实施危险评价。考虑到这种情况，本论文以以下观点为基础：

(1) 把石油化工厂、原子能发电厂等的车间、工艺过程作为研究对象的系统。

(2) 非编制专业的技术人员也能理解，并且实用的方法。

(3) 要使树的编制成为过去发展了的科学的延伸，譬如说，要明确工艺过程控制与编制树的关系。

本论文以有向图解的研究方法为基础，并组合工艺过程控制的方框图，由此进一步改进了过去树编制法，而推荐实用的故障树编制法。在叙述该方法概要的同时，通过对一些简单问题的应用，阐明编制法的步骤。在续篇中，还将进一步对紧急断路系统和复杂系统的应用实例作介绍。

2. 以往树编制法的概要及其问题

关于故障树编制法，虽已对一九六〇年的初期情况作过概要介绍，对最新的研究，本刊也报告了其主要算法和文献。本文将对树编制法的观点和其主要问题进行阐述。以工厂为对象，树编制的算法可大致分为以下二类：

(1) 采用digraph（有向图）的方法；

(2) 采用decision table（真值表或判定法）的方法。

Powers等人提出的有向图树编制法是用有向图表现工艺过程的状况，并在图中记入故障模型，以此编制树的方法。该法重视工艺过程中各参数的功能，但各要素在图中则表现不出。因此，实际上树编制者是在对照工艺流程图的同

时，边考虑各要素工作的参数状态，边编制树的。此外，当参数取二个值时的算法还没有发表。

虽然人们认为用有向图的方法很适用，但要把由计算机合成树作为最终目的，在实际应用上还有问题，其应用例也不多。

decision table法是用decision table（真值表）表现各个要素的输入、输出和内部模型的状态，并根据真值表作成树。在表中考虑到各因素能起作用的总的情况，因此，即便是一个因素，组合的数也很多，所以在大规模系统中，人工编制树几乎是不可能的。为此发明了编制树的计算机编码，在现阶段，也许是最出色的编制树的计算机编码。

但这种方法也存在问题。系统中各要素因有多种形式的组合联接，因而难以编制成可解决所有组合形式的计算机编码。譬如，反馈控制回路和紧急断路回路交叉组合联接而相互干扰时，就不能用这种方法编制树。

若用decision table，虽可详细规定各个要素的功能，但对于系统内各要素以复杂形式组合的问题的应用是困难的。

因此，本文提出在某种程度上解决了过去方法存在的问题的树编制法方案。

第一，编制树的方法，不是以计算机的合成为目的，而是以手工编制树为目的。在以复杂形式组合的化工厂中，不可能编制出适用于所有组合形式的计算机编码。另外在实际中，编制树这项工作既能使我们充分了解对象系统的内容，又有助于我们制定必要的对策。

第二，采纳了方框图的研究方法。现在，因工艺过程控

制的研究方法已得到普及，故方框图也为技术人员充分了解。因此，使树的编制成为工艺过程控制的延伸，由此可明确编制树与过去科学的有机联系，同时易于着手进行树的编制。

第三、本方法虽以有向图为基础，但对有向图的基础理论则不是特别需要。另外采用decision table对各要素的功能作了分析，但省略了细节。

最后，本方法已在几家工厂中应用，对树编制的结果也作了报告。本方法的实用性是无可置疑的，但对编制树的算法未作详细报告。本论文将修改过去编制过程中暴露出的算法中存在的问题，同时在以后的论文中，还将进一步报告复杂系统的树编制的算法。

3.术语、符号和方框图

在此，如图1所示，以流量控制系统为例，给编制树所需术语、符号下定义，并阐述有关的方框图。该控制系统由测流孔（探测器）、流量调节器（FC）、管道-a、流量控制阀（FCV）四个要素构成。在表示系统状态的参数时，用了以下符号：

T：温度，P：压力，F：流量，C：浓度，L：液位，I：电流 'ΔP：压差。

分别给流程图各要素的入口、出口位置标上号码，

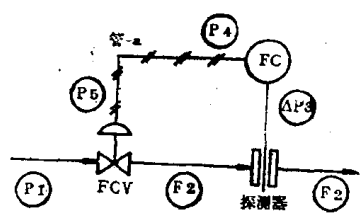

图1　流量控制系统流程图

与参数符号共同表示。P1和T2表示位置1的压力和位置2的温度，图2所示为标上参数和位置的流量控制系统的方框图。

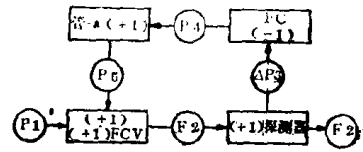

图2　方框图

假设对象系统的设计、运转条件已作了规定，仅从其标准值考察参数的变动（deviation）。如果参数中有变动发生，则用（+1，0，-1或者HIGH，ZERO，LOW）表示，这些符号分别具有以下意义：

+1，HIGH：参数值比标准值增加，变量为正号。例如温度、压力上升。

0，ZERO：参数值与标准值在某一范围内一致。例如温度、压力不变。

-1，LOW：参数值比标准值减少，变量为负号。例如温度、压力降低。

但是对变动量的大小不特别规定。

P1·(+1)或者P1·HIGH表示位置1的压力增加。以下，在叙述参数时用P1·HIGH，叙述方框图故障条件时用(+1，0，-1)。

把进入某一要素的参变量及由此出来的参变量的变化分别定义为输入和输出。此时，要素输入和输出的关系可由该要素的增益（gain）来表示。增益是自动控制上所用的术语。在此，作为要素的增益，仅仅考虑取(+1，0，-1)这样三个离散值的情况。例如，在FCV中，假定阀的开放度一定，若输入为P1·HIGH，则输出为P2·HIGH，该要素的增益为+1。增益与输入、输出的关系可用下式表

示：

（输入）×（增益）=（输出）　　（1）

如果增益值为0，则输出与输入无关，也为0。即为输入不传送到输出的情况。各要素的增益值可在要素内部输入的箭头线符号旁注（+1）或（-1）表示。要素的增益是反映其功能的尺度，在流量控制系统中，FC的增益为-1，其他要素的增益均为+1。图2记有各要素的增益。

4.含有故障模型的方框图

在编制故障树时，需要决定对象系统各要素的故障模型。根据各要素的结构、使用条件、环境等的不同，要素的故障模型也不一样。针对流量控制系统设定表1所示故障模型。

表1　　各要素的故障模型

要　素	故障模型
FCV	FAILURE(失灵)，OPEN(开启)，CLOSED(关闭)
FC	FAILURE(失灵),HIGH OUTPUT(高输出),LOW OUTPUT(低输出)
	SETPOINT TOOHIGH(设定值高),SETPOINT TOOLOW(设定值低)
SENSOR	FAILURE(无输出),HIGH OUTPUT(高输出),LOW OUTPUT(低输出)
TUbe—a	LEAK(漏泄)，PLUGGED(堵塞)

故障模型分为输入不传递到输出的故障及给出错误输出的故障二类，以下概要说明。

(1) 不传递输入的故障：如果发生这种故障，则要素的增益为0，输出与输入无关，为ZERO。表1 FAILUR 所

表示的故障模型均与此相当。在记入方框图时，如图3所示在括弧里写上故障模型名(0)，并用箭头线指向要素的增益。

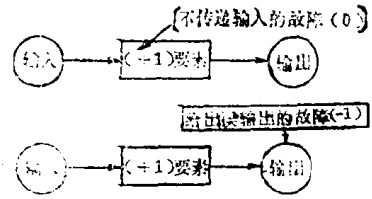

图3　故障模型的记入方法

(2) 给出错误输出的故障：如果发生这种故障，则与输入无关的故障模型指定的“+1”或“-1”中的一值成为输出。在记入方框图时，如图3所示，在长方形中记入故障模型名和输出值，并用箭头线指向输出。

在图2方框图中记入表1的故障模型，其结果如图4所示，该图称为故障模型方框图。

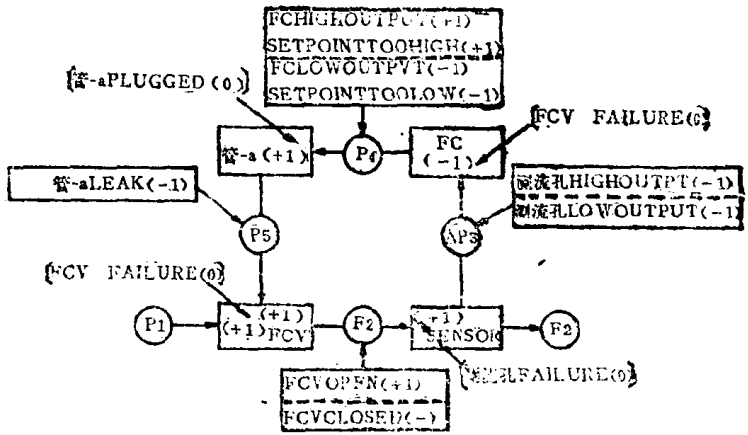

图4　故障模型方框图

当要素的输入和输出均为一个时，输出只能根据(1)式来决定。但象图4 FCV那样有二个输入时，要素的输出可

分别根据（输入）×（增益）的组合来决定。对应各输入的（1）式的值要考虑其要素内部的变量，故将其称为内部变量或者内部事件。

假设某要素输入变量为A，输出变量为B，则（输入A）×（增益）的值为（+1，0，-1）中任何一值，将其表示为（A→B·HIGH，A→B·ZERO，A→B·LOW）。在展开树时，最初要用内部变量来决定给出目的输出的变量的组合。其次因为若规定了其内部变量，就可根据（输入）×（增益）的关系决定输入的值，故可逐层展开树。

在以前的故障树编制法中，采用了直接以输入表示输出的方法。由于使用了内部变量这一概念，因而在展开树时，能够对各要素的输出、内部变量及输入各阶段全面地、逐次地加以研究，使树的展开非常容易，这是本方法的一大特色。

5.树展开算法的基础

5.1 未记入故障模型的变量、事件的展开

（1）不带输入的变量、事件：该变量、事件因不能使原因进一步展开，故称为未开发事件。图4的P1与这种情况相当。

（2）要素有一个输入和输出：图5（1）所示情况显然能够展开。但是在A→B·HIGH，还是尚未涉及到A的输入、增益的阶段。

（3）要素有二个输入，未构成反馈回路：输出为HIGH（LOW），因为一个内部变量也可以成为HIGH(LOW)，

故可用“或门”展开，如图5(2)所示。

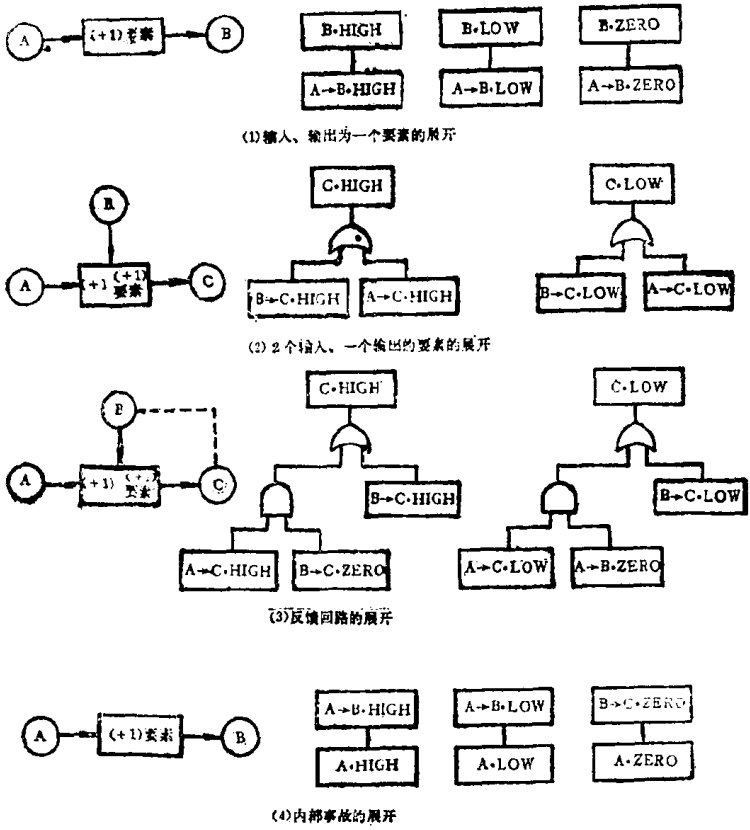

图5　变量事件的展开

(4) 要素有二个输入，构成反馈控制回路：在负反馈回路中，该回路内要素的增益的积为－1。反馈回路输出为HIGH（LOW）时，是因该回路发出误信号之故，或者是因对输入为HIGH（LOW）这样的外干扰，回路不工作之

故。这时的展开如图5（3）所示。

（5）内部变量在输入展开：以上用内部变量、事件展开了输出变量或事件。要进一步将内部变量以输入变量、事件来展开时，就成为图5（4）增益为＋1时的情况。

以上的展开均可用truth table（真值表）验证，细节从略。

5.2 记入了故障模型的变量、事件的展开

（1）不传递输入的故障：输出变量为ZERO时，是因输入为ZERO，或者发生不传递输入的故障，故如图6（1）所示，可用或门展开。

（2）给以错误输出的故障：输出为HIGH(LOW)时，是因内部变量为HIGH（LOW），或者是因发生给出错误输出的故障，故如图6（2）所示，可用或门展开。图6（2）中仅表示输出为HIGH的情况，而当输出为LOW时，结果也是一样的。

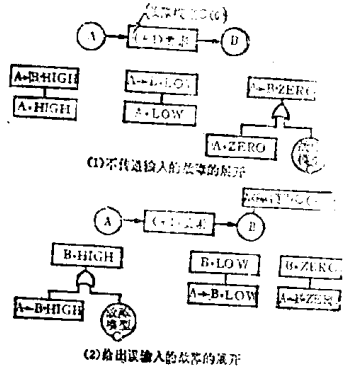

图6　有故障模型的变量事件的展开

5.3 事件制约条件

根据逻辑结构的观点，故障树不允许在某一事故事件E的下面出现E的排斥事件。把这一排斥事件除去的条件就是事件制约条件。

譬如，以图4的F2·HIGH这一事件为例，F2·HIGH就是事件制约条件。在该事件下面，因不允许F2·LOW、F2·ZERO这样的事件，故须把它们作为违背制约条件的

事件除去。

如排斥事件是或门的输入，则仅将排斥事件从或门的输入中除去即可。其理由是因为只要其他输入事件出现，就会产生或门的输出事件，如果排斥事件是与门的输入，那么即使其他输入事件全部出现，只要不产生其排斥事件，与门的输出事件就不会产生。因此可将与门和其下面的事件全部除去。若该门的输出事件又是上一级与门的输入事件，则其上一级的与门也要除去，最后一直到或门输入处为止。图7所示为事件制约条件的应用实例。

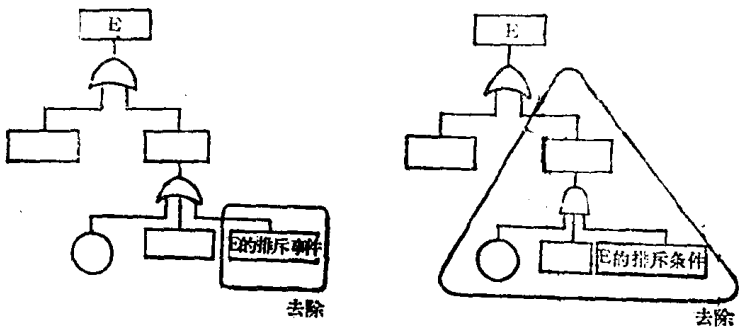

图7　事件制约条件的应用

这样的排斥事件之所以在树中出现，譬如在展开反馈控制回路的事故事件时，是因为最终包含有正常事件的缘故。这在下面树的展开分析中很清楚。

6.流量控制系统故障树的编制

根据图4的故障模型方框图，用上面所述的算法编制流