第 23 卷 第 6 期
1997 年 11 月

自 动 化 学 报
ACTA AUTOMATICA SINICA

Vol. 23, No. 6
Nov., 1997

短 文

控制系统故障树自动建造方法的研究

陶 军 李应红 辛宇峰

(空军工程学院一系 西安 710038)

摘 要 在对建树过程进行规范化描述的基础上,阐述了控制系统中反馈、前馈、分流和汇流等复杂结构在多状态故障树自动建造中的识别及处理算法. 在此基础上形成的专家系统软件,可直接利用已有部件模型库,按指定顶事件状态自动生成故障树,节约了人力和时间,对 FTA 技术的推广有一定促进作用.

关键词 规范描述,系统模型,自动建树.

1 引言

故障树分析法在可靠性工程界应用十分广泛,但其中传统手工故障树(FT)的建造却需耗费巨大的人力、物力和时间,而且建树过程无规范化描述,发生遗漏和错误几乎是不可避免的. 所以 FT 自动建造已成为可靠性工程界重点的追求目标. 但由于自动建树的复杂性,直到 80 年代末 90 年代初才产生了一些可初步使用的 FT 自动建造专家系统软件[1−4]. 但总的来说,这些研究工作还很不完善,特别是自动建树方法和软件的通用性很不够,在系统模型描述、多参数相互影响、控制系统闭环回路和前馈的处理,以及部件故障多状态的处理等方面存在着不同程度的不足之处. 本文针对上述问题,在对建树过程规范化描述的基础上,阐述了多态树中对控制系统反馈、前馈回路和分流、汇流等复杂结构的处理方法.

2 控制系统故障树自动建造方法

为实现 FT 建造的自动化,首先要构造适宜的自动化算法,然后再以此算法为基础构造实用的软件. FT 自动建造算法的基本思路是,由所定义的顶事件(某一故障)出发,按故障的产生及传播机理,遍历系统模型,不断将导致局部故障发生的原因事件合成到总故障树中,直至底事件. 由于 FT 是系统处于失效状态的真实影像,因此自动建树方法要包括系统模型的建立和故障树合成算法两部分内容.

2.1 系统模型

按照一般系统论的观点,认为物理系统由部件(子系统)、系统结构功能关系、系统所

收稿日期 1995-09-11

处环境三部分组成,并可以通过输入输出变量来描述系统(或部件)的功能关系,从而可将故障看作输出变量偏离正常值或输入输出变量间正常功能关系的改变.其中变量所有可能发生的偏差与其正常值相比可划分为±10(超出控制范围无法补偿的正负大偏差)、±1(可被控制系统补偿的正负中等偏差)和 0(正常)五个水平.对于故障在系统中的传播,可看作变量偏差信号通过变量间的相互关系在变量间的传播.这种关系可通过传递系数来定量表示.其中+1 表示原因和结果变量的偏差呈同向变化关系;−1 表示原因和结果变量的偏差呈反向变化关系;0 表示正常关系被打破,原因和结果不再发生关系.通过上述对故障及其传播的量化描述,即可建立起规范化的部件模型和系统结构描述[5].

2.2　系统复杂结构及其对 FT 形态的影响

2.2.1　反馈控制回路

对反馈回路而言,如果在反馈支路中变量发生了偏差,将给控制器传递错误的控制信息,这样将产生不正确的控制操作.其对 FT 的影响详见参考文献[6].

2.2.2　前馈控制回路

在控制系统中,前馈控制包含对输入量进行补偿和按扰动进行补偿的两种回路控制形式.对于负前馈,从控制上说是不可能进行完全补偿的,然而通过负前馈的作用可使偏差减小以使系统达到正常的工作状态,从而消除故障.要使前馈消除可能造成的故障,必须保证控制支路和被控支路的部件不发生与传递偏差不相符的失效,同时还要求偏差不超过控制极限.所以系统存在前馈控制时,以被控量的偏差为顶事件的子故障树部分应呈现图 1 所示形态(设 x 为被控变量名).

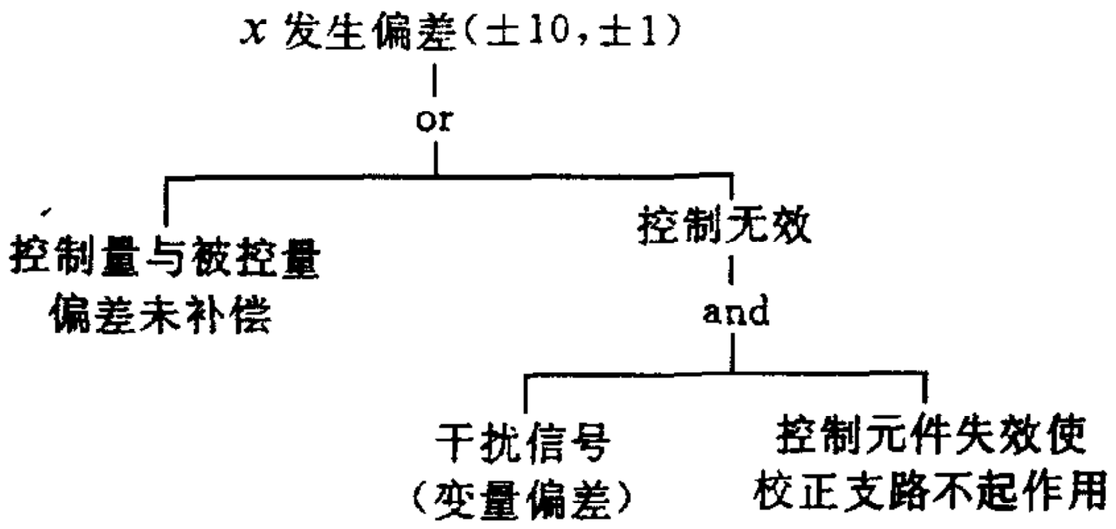

图 1　前馈回路子故障树

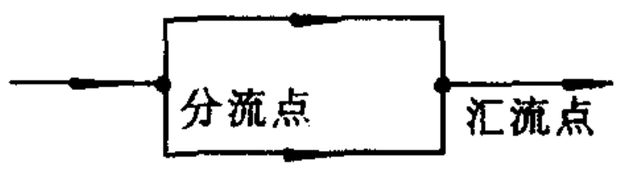

图 2　分流汇流结构

2.2.3　分流和汇流

分流和汇流一般是同时出现的,其一般形式如图 2 所示.这种结构一般需要提供两个特殊的部件模型,即分流点和汇流点模型.并联和余度是它的典型,其特点是变量在不同的支路上的分配关系往往具有复杂、特殊的形式,通常要在 FT 中引入“与”门(条件关系)和 K/n 表决门等.

明确了系统中的这些复杂结构后,就需要在自动建树中加以识别和处理,这样才能得到最终真实的 FT.在建立系统模型上采用的方法是,先不考虑系统的复杂结构,只建立局部的部件模型和部件联接模型,在建树时,再通过附加算法,自动识别系统结构并加以处理.这样,可以建立通用的部件模型库,对预先人工准备工作要求少,通用性比较好.

2.3　自动建树算法研究

2.3.1 中间树的生成[5]

中间树具有和故障树很相近的结构，只不过没有考虑顶事件的具体偏差，而是显示了所有可能导致顶事件变量发生的全部偏差所经过的条件和非条件支路. 当中间树中的支路发展到环境变量节点、部件内部失效的各种状态节点及在同支路中重复出现的变量节点时，不再继续发展. 节点变量的范围，限制在与其父节点相关的范围内.

中间树建立完成之后，再经过对系统复杂结构的识别和处理，即可转化为最终真实的FT.

2.3.2 系统复杂结构的识别和处理

(1)反馈回路及回流的处理. 在中间树的一条支路中，如果同一变量出现两次，则说明该支路表示了系统中的一个反馈回路或回流. 其处理方法详见参考文献[5].

(2)前馈回路和分流汇流的处理. 在中间树中，如果以某事件为根结点的两个不同支路内，同时出现了相同的事件或事件组合，则说明系统中存在着前馈回路或分流、汇流结构.

当上述两条支路的传递系数不相等且不为零时，说明此结构为一负前馈回路，其典型结构如图 3 所示. 它具有分工明确的两条支路——功能路和补偿控制路. 当功能路的输出误差超出一定范围时，触发补偿控制路对前者进行补偿，从而起到对后续子系统的保护作用，这种负前馈称为安全负前馈. 此外，还有从控制意义上讲的广义负前馈，它具有如下特点：①它的两条支路各自完成一定的功能，且互为保护路；②系统的输入信号同时加在两条支路的输入端，不存在补偿支路的起动问题. 因此，经这种负前馈作用后，被保护子系统的输入状态将视补偿的结果而定. 对于某些特定的比较监控系统而言，只有当两条支路补偿后的差值大于门限值时，才认为前馈回路输出故障，其偏差是严重偏差(±10).

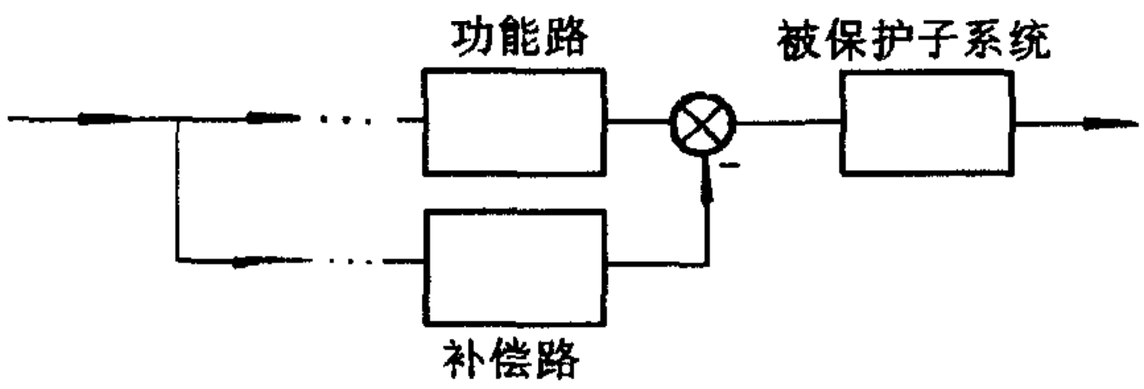

图 3 负前馈结构

为了对这三种负前馈回路加以区别处理，对于一般的广义负前馈，可在其比较输出部件模型中加入识别符 SS，当中间树中一基本事件下的两条支路都存在 SS 时，表明这两条

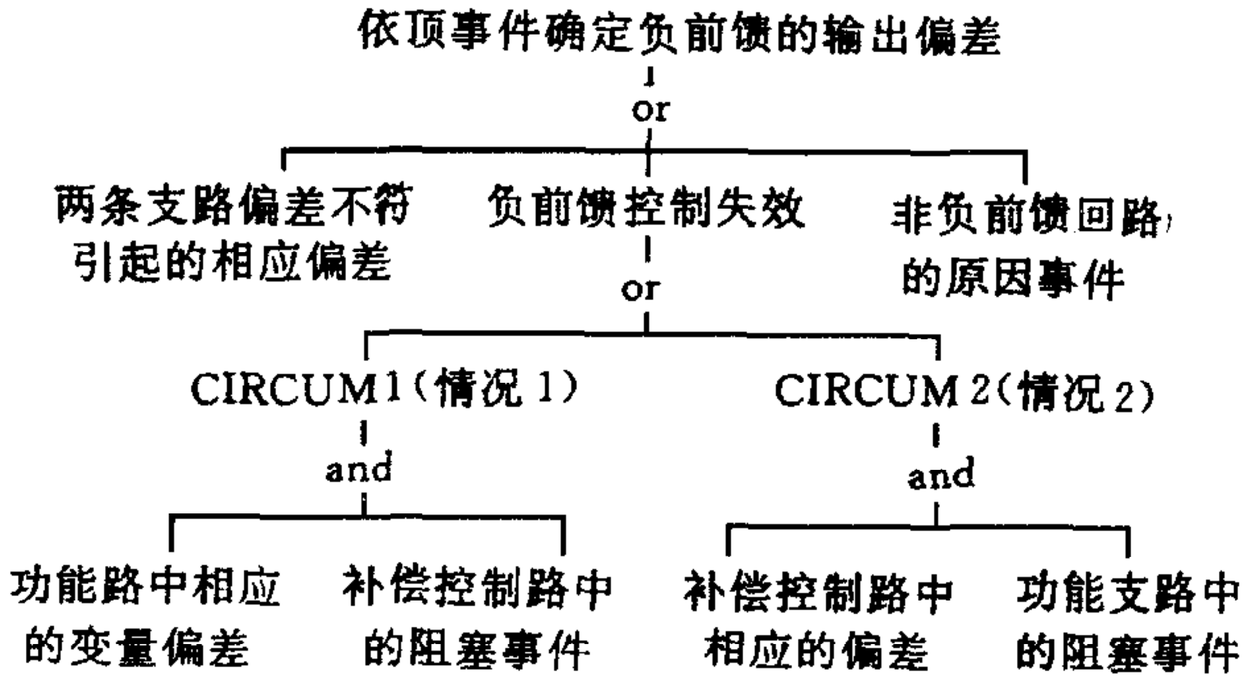

图 4

支路形成了一个一般广义负前馈回路.这时只需对中间树进行如图 4 处理,即可将它转变为真实 FT.

对于特殊比较监控的广义负前馈,其故障偏差只能为±10 时,可在其比较输出的部件模型中加入另一识别符 S.此种情况下,在 FT 生成时,只有引起负前馈输出的偏差为±10 时,才需进行图 4 所示的处理.

对于无识别符号的负前馈即为安全负前馈,其处理过程详见参考文献[5].

对于中间树中和负前馈结构相似的分流和汇流结构,可通过根结点下两条支路的传递系数相等且不为零来加以判断.其处理方法主要在于分流点和汇流点部件模型的构造上.对于一般分流点或汇流点的处理主要取决于系统的成功准则.如图 5 所示的两组泵列并联工作的情况.假设每组泵列最大能提供 $80m^3/h$ 的流量,当系统的成功准则是两组泵

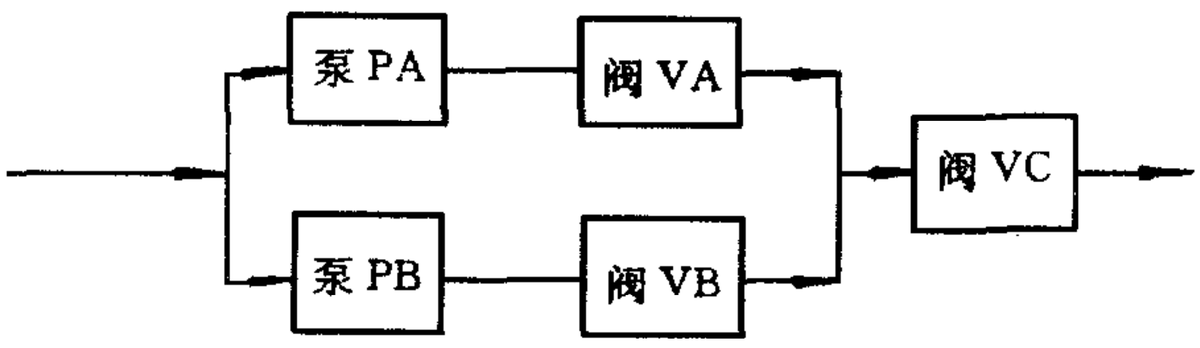

图 5　两组泵列并联工作

列向 VC 提供的流量不小于 $160m^3/h$ 时,对于顶事件 VC 阀门输入端口流量不足是由泵列 A 或 B 流量不足造成的.若系统的成功准则为两组泵列向 VC 提供的流量不小于 $80m^3/h$,则同样的顶事件是由泵列 A 和 B 同时流量不足造成的.在分流点的处理中也有类似情况.为此,在建树中需将相应的成功准则及处理方法加入系统建树判断之中.

在系统中,如果出现反馈和前馈回路同时控制同一被控量,则被控量的故障偏差是由两种回路分别失效形成的子故障树相“与”而造成的.

通过上述对系统中复杂结构的处理,再对中间树中的节点做简单的转换——将非条件节点转换为 FT 中的“或”门,条件节点转换为 FT 中的“与”门,非节点转换为 FT 中的“非”门.再按照顶事件所对应偏差直接搜索,并将所有无关的偏差信号都予以摒弃,即可得到真实的 FT.

3　结束语

本文所提出的在建树过程中对系统复杂结构的处理方法,充分考虑了各种实际控制系统中可能存在的问题.以此为基础形成的专家系统软件,可直接利用已有的部件模型库,按指定的顶事件状态自动生成的故障树,拓宽了自动建树软件的适用范围,具有较好的通用性.通过对某实际飞控系统进行的自动建树,验证了该方法的正确性和实用性.

参 考 文 献

[1] Poucet A. STARS: Knowledge based tools for safety and reliability analysis. *Reliability Engineering and System Safety*, 1990, **30**: 379—397.

[2] Schwarzblat M *etc*. PC-FTA: An expert system for fault tree construction. In: Proceeding of the international conference on PSAM, 1991: 793—798.

[3] Hideaki Takahashi *et al*. Development of expert system to support system reliability analysis. In: Proceedings of the international conference on PSAM, 1991: 929—934.

[4] Xie Gang *et al*. TREE-EXPERT: A tree-based expert system for fault tree construction. *Reliability Engineering and System Safety*, 1993, **40**: 295—309.

[5] Bossche A. Fault tree analysis and synthsis. NASA, N88—23521.

[6] 辛宇峰等. 一个智能化的故障树自动建造系统. 见: 第一届全球华人智能控制与智能自动化大会论文集(上卷), 北京: 科学出版社, 1993: 129—134.

RESEARCH ON AUTOMATIC FAULT TREE CONSTRUCTION FOR CONTROL SYSTEM

TAO JUN LI YINGHONG XIN YUFENG

(*First Department of the Air Force Institute of Engineering, Xi'an* 710038)

Abstract After describing the fault tree construction process canonically, an algorithm dealing with such complex structures as feedback loop, feedforward loop, divider and header in multistate fault tree automatic construction is presentd. The expert system software based on the algorithm can generate fault tree automatically according to the components' model library and the specified top event state. Consequently, either manual work or time is saved, and the popularization of FTA technique is promoted.

Key words Formal description, system model, automatic fault tree construction.