第 23 卷 第 3 期
1997 年 5 月

自 动 化 学 报
ACTA AUTOMATICA SINICA

Vol. 23, No. 3
May, 1997

控制系统故障树自动建造的一种方法[1)]

简志敏 胡东成 童诗白

(清华大学自动化系 北京 100084)

摘 要 提出一种改进的有向图法——一般有向图法. 使用这一方法,不但能较好地完成简单控制系统的自动建树,而且可以较好地完成有较复杂控制结构的控制系统的自动建树,克服了传统有向图法自动建树的困难.

关键词 故障树的自动建造,有向图法,控制系统,可靠性分析.

1 引言

自动建造故障树是故障树分析法研究中的一个重要分支. 自 1973 年以来,人们陆续提出了数种自动建造故障树的模型和相应的算法[1]. 在这些方法中,有向图法[2,3]深受重视. 在 Lapp & Powers 于 1977 年提出这一方法后,人们多次对其进行了修正和改进[4-10]. 然而,困难依然存在. 特别是在处理较复杂控制系统时,用有向图法自动建造故障树经常产生一些错误的结果. 为此,本文提出一种更加系统化和更加严格的有向图法,称之为一般有向图法.

2 一般有向图法的概念和约定

定义 1. 能充分描述元部件在正常情况下的功能特征以及当元部件在各种失效模式下的失效特征的元部件模型,称为该元部件的完全模型.

定义 2. 根据元部件的完全模型来构造的系统有向图模型,称为系统的一般有向图模型,简称系统的一般有向图.

定义 3. 在一般有向图中,表示过程变量的节点称为过程节点.

定义 4. 在一般有向图中,表示某个失效事件的节点称为失效节点.

定义 5. 在一般有向图中,每一个过程节点对应一个变量,称为过程节点变量.

定义 6. 在一般有向图中,每一个失效节点和每一个为失效事件的边增益条件均分别对应一个变量,称为失效变量.

如对于一个气压阀,在仔细分析了其功能和失效特征后,可以建立其完全模型,用一般有向图表示如图 1 所示. 其中节点 'M1', 'M2', 'P3' 为过程节点;而节点 'CLOSED', 'OPEN' 则为失效节点. 过程节点 'M1', 'M2', 'P3' 所对应的过程节点变量用过程节点

1) 得到国家自然科学基金的资助.

收稿日期 1994-06-24

名定义分别为 M1,M2,P3. 失效节点 'CLOSED', 'OPEN' 所对应的失效变量用节点名定义分别为 CLOSED,OPEN. 另外,失效变量 CLOSED,OPEN 在模型中还对应表示边增益条件的失效事件.

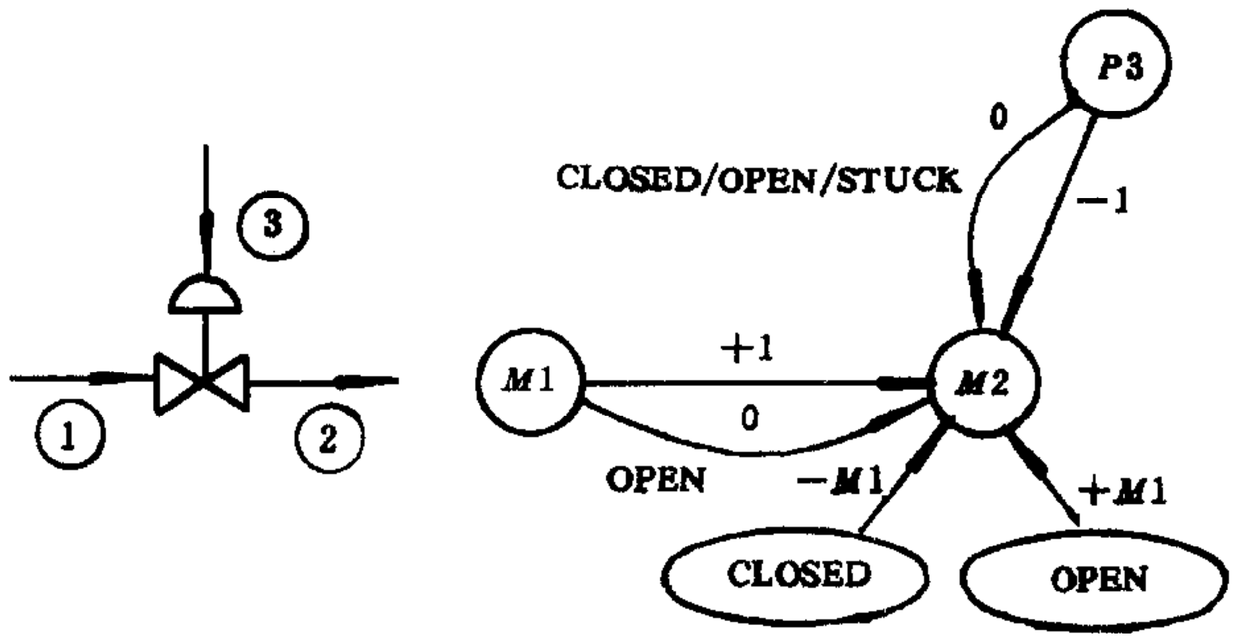

图 1　气压阀及其完全模型

约定 1. 元部件完全模型的边增益可以根据元部件建模的需要设定为过程节点变量.

约定 2. 过程节点变量是整型变量,其取值为$(-\eta,+\eta)$之内的相对整数(η是一个过程节点变量扰动远不能达到的一个相对正整数,在本文的讨论中,不妨定义为 100). 0 为正常值. 过程节点变量的扰动(偏差)以 1 为一个等级. ±1 表示扰动在一个控制环的控制之内,±2 表示扰动超出了一个控制环的控制范围,但在两个控制环的控制之内,以此类推.

约定 3. 失效变量是布尔变量,其取值有 0,1 两种形式,当失效变量取 0 时表示相应的失效事件没有发生,当失效变量取 1 时表示相应的失效事件发生了. 失效变量可以进行取反运算;失效变量与失效变量之间进行布尔运算;失效变量与过程节点变量可以进行代数运算.

在一般有向图法中,为了体现负反馈控制环对进入控制环的扰动消除作用,特定义一个变量来描述它.

定义 7. 在系统一般有向图模型中,每一个负反馈环定义一个变量与之对应,称为环变量.

对于负反馈控制环,在系统经过了调试阶段,进入生产阶段后,负反馈控制环有两种状态:正常作用,失去正常作用. 因此,在一般有向图法中,对环变量作如下约定:

约定 4. 定义每一个负反馈控制环的控制范围为 1,即环变量的取值有两种形式:0,−1. 当环变量取值 0 时,表明负反馈控制环失去了对扰动的消除作用;当环变量取值−1 时,表明负反馈控制环作用正常.

约定 5. 环变量等于负反馈环中各段增益之积,即

$$LOOP = \prod G_{loop}$$

其中 $LOOP$ 为环变量,G_{loop}为环中相邻两节点之间的增益(有条件或无条件).

在一般有向图法中,有一个非常重要的约定,这个约定是一般有向图法的核心,在作此约定前,先定义如下三个概念.

定义 8. 在一般有向图中,一条有向边的尾部节点称为该边的原因节点.

定义 9. 在一般有向图中,一条有向边的头部节点即该边所指向的节点,称为该边的结果节点.

约定 6. 一般有向图法将每一个结果过程节点看成是一个加法器. 如果一个过程节点没有负反馈环与之 相关,则其对应过程节点变量可由下式计算

$$EN = \sum CN * G.$$

其中 EN 表示某结果过程节点“EN”相应的过程节点变量；CN 表示 EN 的原因节点变量(“CN”可能是过程节点，也可能是失效节点)；G 是 CN 与 EN 之间的增益. 如果一个过程节点有负反馈环与之相关，则其过程节点变量可由下式计算

$$EN = J * \sum LOOP + \sum DCN * G^l.$$

其中 $LOOP$ 是与过程节点“EN”相关的负反馈环的环变量(所谓某过程节点与某反馈环相关，是指该过程节点是该反馈环的首节点，即该反馈环控制元部件的输出节点)；DCN 是进入反馈环的外部扰动节点变量；G^l 是外部扰动“DCN”传播到“EN”的路径上各边的边增益之积；J 是环变量的符号因子，表示负反馈控制环正常时的调整方向，常被定义为

$$J = \begin{cases} +1, & \text{when } EN > 0, \\ -1, & \text{when } EN < 0. \end{cases}$$

根据上述定义和约定，就可以建立能描述系统或部分系统的方程(组)了.

定义 10. 从一般有向图得到的，由过程节点变量、失效变量、环变量等组成的，描述了系统或系统某部分的功能和失效特征的(一组)方程，称为一般有向图方程(组).

在一般有向图法中，用一般有向图方程(组)来描述系统的控制环部分. 系统控制环部分故障(或扰动)传播的路径可由其一般有向图方程(组)解得.

值得指出的是，一般有向图方程的另一个重要的用途是可以被用来检查一个元部件的完全模型建立得正确与否. 另外，在一般有向图法中，还定义了与顶事件相关的如下两个概念.

定义 11. 顶事件定义于其上的过程节点，称为顶节点.

定义 12. 与顶节点对应的过程节点变量，称为顶变量.

3 基于一般有向图的故障树的建造

在为有复杂控制结构的系统建造故障树的过程中，对其控制环结构的处理是自动建造故障树的难点. 基于一般有向图建造系统中环结构故障树的基本思想为

1)根据系统的拓扑结构互连组成系统的元部件的完全模型构造系统的一般有向图；

2)根据一般有向图，建立一般有向图方程(组)；

3)根据顶事件或中间事件，解一般有向图方程(组)，得到顶事件或中间事件的割集和故障树.

一般有向图法建造故障树的算法如下：

(1)互连元部件的完全模型建立系统一般有向图；

(2)定义顶事件；

(3)将顶事件推入 STACKK 中；

(4)STACKK 空吗？是，停(故障树建造完毕)；否，从 STACKK 中弹出一个事件作为当前事件并置其变量为当前变量；

(5)当前变量是某反馈环的首变量或是某前馈环的终点变量？是，转(6)；否，转(8)；

(6)搜索与当前变量相关的环和当前变量对应节点的输入，列一般有向图方程组；

(7)以当前事件为边界条件解该方程组,并根据解画相应的故障树枝,转(9);
(8)用“直接原因概念”发展故障树;
(9)将非底事件原因事件推入 STACKK 中存储,转(4);
其中 STACKK 是一个执行“先入后出”原则的堆栈.

4　结论

虽然故障树的自动建造作为故障树分析技术的一个重要分支,多年来一直倍受关注,但也存在着争论[6,9].引起争论的重要原因在于故障树的自动建造本身发展不成熟,无法产生令人信服的、正确的故障树.本文用定量分析与定性分析相结合,提出的一般有向图法能较好地解决具有比较复杂控制结构的系统故障树的自动建造问题,克服了传统有向图法遇到的困难,是故障树自动建造技术一个有意义的进展.

参 考 文 献

[1] 简志敏. 控制系统故障树自动建造的一种新方法[学位论文]. 北京:清华大学自动化系,1995.

[2] Lapp A S, Powers G J. Computer-aided synthesis of Fault-trees. *IEEE Trans. Rel.*, 1977, **R-26**(1):2—13.

[3] Lapp A S, Powers G J. Up-date of lapp-powers fault tree synthesis algorithm. *IEEE Trans. Rel.*, 1979, **R-28**(1):12—14

[4] Lambert H E. Comments on the lapp-powers computer-aided synthesis of fault trees. *IEEE Trans. Rel.*, 1979, **R-28**(1):6—7.

[5] Allen D J, Rao M S M. New algorithms for the synthesis and analysis of fault trees. *Ind. Eng. Chem. Fundam.*, 1980, **19**:79—85.

[6] Andow P K. Difficulties in fault tree synthesis for process plant. *IEEE Trans. Rel.*, 1980, **R-29**(1):2—8.

[7] Kumamoto H, Henley E J. Automated fault tree synthesis by disturbance analysis. *Ind. Eng. Chem. Fundam.*, 1986, **25**:233—239.

[8] Allen D J. Digraphs and fault trees. *Ind. Eng. Chem. Fundam.*, 1984, **23**:175—180.

[9] Andrews A, Brennan G. Applications of the digraph method of fault tree construction to a complex control configuration. *Rel. Eng. & Sys. Safety*, 1990, **28**:357—384.

[10] Chang C T, Hwang H C. New developments of the digraph-based techniques for fault tree synthesis. *Ind. Eng. Chem. Res.*, 1992, **31**:1490—1502.

A NEW METHODOLOGY OF AUTOMATIC CONSTRUCTION OF FAULT TREES FOR CONTROL SYSTEMS

JIAN ZHIMIN　HU DONGCHENG　TONG SHIBAI

(*Dept. of Automation, Tsinghua University, Beijing* 100084)

Abstract　AGFT (Automatic Generation of Fault Trees) is the problem with which system reliability analysis are much concerned. This paper presented an improved Digraph, the General Digraph. By the General Digraph, you can construct fault trees automatically not only for simple control systems but also for complex control systems. It overcomes difficulties in using traditional Digraph to construct fault trees of complex control systems.

Key words Automatic construction of fault trees , digraph, control systems, reliability analysis.

简志敏 1967 年生. 1989 年毕业于华中理工大学电子与信息工程系,1991 年于武汉工学院获硕士学位,1995 年于清华大学自动化系获博士学位. 现在 IBM 中国研究中心工作. 主要研究兴趣为可靠性分析、数字图书馆.

胡东成 1946 年生. 清华大学自动化系主任、教授、博士生导师,中国自动化学会教育委员会主任委员,中国电子学会高级会员. 长期从事电子与自动化方面的教学与科研工作,主要研究方向为自动测试、故障诊断与可靠性.

IFAC TECHNICAL BOARD STRUCTURE
1996—1999

Chairman of the Technical Board	Vladimir Kucera	CZ
Vice-Chairmen:	Michael Masten	USA
	Luis Basanez	E
Members:	Peter Fleming	UK
	(responsible for liaison to publications)	
	and	
	Coordinating Committee Chairmen	
	as listed below	

Coordinating Committees (CC)
&
Technical Committees (TC)

CC on Manufacturing and Instrumentation	**Tian You Chai**	**PRC**
TC on Manufacturing, Modelling, Management and Control	A. Villa	I
TC on Robotics	F. Nicolo	I
TC on Components and Instruments	A. Ollero	E
TC on Low Cost Automation	A. Cipriano	Chile
TC on Advanced Manufacturing Technology	M. Zaremba	CDN
TC on Architectures for Enterprise Integration	T. J. Williams	USA
CC on Design Methods	**Alberto Isidori**	**I**
TC on Control Design	S. Engell	D
TC on Linear Systems	J. M. Dion	F
TC on Nonlinear Systems	T. Glad	S
TC on Optimal Control	R. Bars	H
TC on Robust Control	C. V. Hollot	USA
CC on Systems and Signals	**Han-Fu Chen**	**PRC**
TC on Modelling, Identification and Signal Processing	B. Wahlberg	S
TC on Adaptive Control and Tuning	R. Ortega	F
TC on Discrete Event Dynamic Systems	X. R. Cao	HK
TC on Stochastic Systems	G. Picci	I
TC on Fuzzy and Neural Systems	K. J. Hunt	UK
CC on Life Support Systems	**Yasushi Hashimoto**	**J**
TC on Modelling and Control in Agricultural Processes	I. Farkas	H
TC on Intelligent Control in Agricultrual Automation	H. Murase	J
TC on Modelling and Control of Biomedical Systems	E. J. Carson	UK
TC on Modelling and Control of Environmental Systems	A. Sano	J

(下转 381 页)