文章编号:1001 - 2486(2006)02 - 0111 - 06

基于故障树的系统安全风险实时监测方法*

董豆豆,周忠宝,冯 静,孙 权,周经伦
(国防科技大学 信息系统与管理学院,湖南 长沙 410073)

摘 要:当前的安全性分析方法大都属于预先安全性分析方法,即在系统使用前对系统进行安全性分析。但系统的动态特性,如组成部件工作状态的动态变化,使系统的安全性呈现实时变化。为研究系统的实时安全风险,提出了一种基于故障树的实时安全风险监测方法。该方法用故障树表示系统结构,建立系统安全风险评估模型,根据系统的技术状态参数与系统组件工作状态的对应关系,实时对系统的安全风险进行监测,并根据安全风险监测的情况,对安全风险变化原因做出解释,做到防患于未然。用一个具有前馈控制冷却系统的例子演示了该方法的有效性。

关键词:实时安全风险;故障树;监测;预先安全性分析
中图分类号:E917 文献标识码:A

Real-time Monitoring Method for System Safety Based on Fault Tree

DONG Dou-dou, ZHOU Zhong-bao, FENG Jing, SUN Quan, ZHOU Jing-lun
(College of Information System and Management, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: Most of the current methods for safety analysis belong to the scope of safety pre-analyzing, which analyzes the system safety before system being in service. But the system safety is full of variety because of the system's dynamic characteristic, such as the running status variation of system component. In order to know well the real-time safety risk, a real-time monitoring method for system safety is proposed. The safety risk model was established on the fault tree that was used to represent logic structure of system. The real-time safety risk was monitored according to the correspondence between technical status of system component and running status of system component. Simultaneously the method could account for the change of risks, thus ensuing the taking of precautions. Finally a case monitoring the safety risk for cooling system with pre-feedback was used to demonstrate the effectiveness of the method.

Key words: real-time safety risk; fault tree; monitoring; safety pre-analyzing

当前,安全性分析方法大都从系统研制初期的指标论证阶段开始进行,并贯穿工程研制。它用于检查系统或其设备在每种使用模式中的工作状态,确定潜在的危险,预计这些危险对人员伤害或对设备造成损坏的可能性,并确定消除或减少危险的方法,以便在系统设计时尽量消除事故隐患,或尽量减少事故发生的可能性,降低事故有害影响的程度[1]。从安全性分析方法的使用阶段来看,传统的安全分析方法基本上是预先安全性分析方法[2],即使动态的安全分析方法[3-5]也只是对系统运行中的动态行为进行预先分析。从本质上讲,动态安全分析方法只是对系统进行更为全面和准确的建模。这些预先安全性分析方法的主要目的是用于指导系统的设计和研制,而对系统运行时的安全性分析和预测考虑较少。

对于实时安全监测,当前也有许多方法,在文献[6]中,所涉及的众多的安全检测方法大都只是通过对系统重要部件的状态参数进行监测,由于这些监测的状态参数可以直接反映系统关键部件的工作状况,所以监测关键部件的状态参数可以间接达到监测系统安全的目的。但对于大型复杂系统,这种直接监测关键部件的方法会形成大量的监测点,使系统级的安全人员感到千头万绪,不能全面把握系统的安全性状况。而且,许多事故是由多种因素通过某种逻辑关系共同作用形成的。之所以造成这样的困境,是由于没有在系统层次研究系统的组成部件对系统风险的影响。

* 收稿日期:2005 - 10 - 20
基金项目:国家部委基金资助项目(2005AA845023)
作者简介:董豆豆(1976—),男,博士生。

为了从系统层次上研究系统组件对系统风险的影响,我们提出了一种基于故障树的实时安全风险分析方法,为系统的安全预测技术研究提供了一个有益的思路。该方法通过建立基于故障树的系统安全模型,通过系统的技术状态参数与系统工作状态的对应关系,实现对事故发生的风险概率进行预测。

1 安全风险监测的一般模型

“风险”这个词含义很多,由于应用背景的不同,人们对它有许多不同的定义,在文献[1]中给出了一个涵盖内容广泛的定义。该定义考虑了事故可能导致的后果、后果的效用以及导致事故的因果链。但由于后果的效用评价具有较强的主观性及导致事故的因果链通常容易得到,故着重研究系统中导致严重后果的可能性。为方便起见,将系统中导致严重后果的可能性称为系统的安全风险。更清晰地,系统的安全风险 $P(I_k)$ 是指系统中某种关键故障模式 $I_k(k=1,2,\cdots,m)$ 发生的概率。

通常情况下,系统的安全风险与系统组件的工作状态有重要对应关系,所以,用式(1)表示系统的安全风险与系统组件工作状态 X_i 的关系:

$$P(I_k)=f(X_1,X_2,\cdots,X_i,\cdots,X_n),\quad i=1,2,\cdots,n \tag{1}$$

式(1)表明:系统当前的安全风险与当前系统组件的工作状态构成一定的函数关系。这种函数关系可以用数学公式来表示,也可以用图形建模的方式表示。将式(1)称为系统安全风险的一般模型。从表面上看,该模型并没有反应系统的动态特性,如系统组件的个体品质、环境及人的影响。但实质上,系统的工作状态是系统动态特性综合的结果,是系统安全性的表征。

同时,从式(1)可以看出,对于简单的安全监测,系统的安全风险可能只与系统某一个组件的工作状态有关,如仅通过对烟尘含量的监测就可以知道是否发生了火灾;而更复杂的情况是,系统的安全风险与系统众多组件的工作状态有关,对于这种具体复杂关系的系统风险监测,则可以通过基于故障树的方法进行。

2 基于故障树的实时风险监测方法

2.1 故障树介绍

故障树分析(fault tree analysis, FTA)于1961年被提出来,由美国贝尔实验室首先用于分析“民兵”导弹发射控制系统,后来推广到多种类武器装备及核能、化工等许多领域。FTA分析是一种自上而下的分析技术,它可以对不希望事件进行并行和有序的综合分析,研究每种故障及其原因,以给出不希望事件在给定环境下可能发生的概率。FTA采用图形分析,建模直观。工程人员通过FTA可以方便地分析故障的原因、影响和系统各部件的相互关系。

在系统安全性分析中,系统中的不期望事件对应着系统中的故障模式。依据系统的逻辑组成,FTA能够分析系统中的故障模式。如果能够实时监测系统中关键的故障模式,便可以达到对系统风险实时监测的目标。并且,FTA能够得到部件的概率重要度 $I_i^{Pr}(t)$。系统某部件的概率重要度是指,当且仅当该部件发生故障系统就发生故障的概率。在进行实时风险监控时,可以实时分析系统部件的概率重要度,其值越大,则该部件越应引起关注。

系统的实时风险与系统组件的工作状态有着密切的关系。而故障树可以依据系统的逻辑结构构建系统不希望事件与系统组件的关系。如果对系统的不希望事件进行故障树分析,再依据构建的故障树实时监测系统组件的工作状态,则可以对系统的不希望事件进行实时监测。

2.2 基于故障树的实时监测方法

基于故障树的实时风险监测可按如下步骤进行:

(1) 分析系统中不希望事件对应的故障模式,找出对系统安全影响较大的关键故障模式,依据FTA建树规则和指南,建立以关键故障模式为顶事件的故障树;

(2) 在故障树中,建立底事件的工作状态与技术状态参数的对应关系,将底事件的技术状态参数映射成底事件工作状态的隶属度;

(3) 求得顶事件(对应着关键故障模式)的发生概率 P_{Top}。顶事件的发生概率,即对应着可能引起系统关键故障模式的风险;

(4) 依据实时得到的顶事件概率度量,对系统进行报警或控制;同时利用实时的概率重要度,分析底事件对系统的影响状况,指导系统风险的控制策略制定。

其中,(2)所述的内容,下面详细说明。关于求顶事件发生概率与概率重要度,参见文献[8-9]。顶事件发生的概率可用下式求出:

$$P_{\mathrm{Top}} = \sum_{i=1}^{m} (-1)^{i-1} \sum_{1 \leqslant j_1 \leqslant \cdots \leqslant j_i \leqslant m} P\left(\prod_{l=1}^{i} M_{jl} \right)$$

式中 M_{ji} 为系统第 j 个最小割集 M 中第 i 个组件所对应的底事件,m 为最小割集的数目。

概率重要度可以用下式求出:

$$I_i^{\mathrm{Pr}}(t) = \frac{\partial_g (P_{\mathrm{Top}}(t))}{\partial P_{\mathrm{Top}_i}(t)} = g(1_i, P_{\mathrm{Top}}(t)) - g(0_i, P_{\mathrm{Top}}(t))$$

式中 $P_{\mathrm{Top}}(t)$ 表示在 t 时刻系统顶事件发生概率,$g(1_i, P_{\mathrm{Top}}(t))$ 表示部件 i 失效时,系统顶事件发生的概率。

2.3 系统组件的工作状态与技术状态参数的对应关系

故障树中的底事件对应着系统组件的工作状态。如果系统组件的工作状态可以明确,故障树中的底事件也可以确定。而系统组件的工作状态与系统组件工作时的技术状态参数有密切关系。可以建立系统组件的工作状态与技术状态参数的对应关系,从而明确系统组件的工作状态。通过这种对应关系,可将组件当前状态参数转换成对应系统组件的工作状态的概率。由于传感器技术的发展,系统组件的技术状态参数可很容易地被监测到。在本文中,采用模糊集合理论[10]来建立技术状态参数与系统组件工作状态的对应关系。

设系统组件 A 的技术参数的集合为 T,其中,每一个技术参数 $t_i \in T(i = 1,2,\cdots,n)$;并且设系统组件的工作状态为 $S_k(k = 1,2,\cdots,m)$,则建立在 T 上的组件工作状态 S_k 所对应的模糊集 $\tilde{S}_k$ 为

$$\tilde{S}_k = \sum_{t_1,t_2,\cdots,t_n \in T} \tilde{S}_k(t_1,t_2,\cdots,t_n) \Big| \, t_1,t_2,\cdots,t_n \in T$$

这里,$\sum$ 并不表示求和的含义,而是模糊集合论中的一种习惯表示法,进一步可简写为

$$\tilde{S}_k = \sum_{t \in T} \tilde{S}_k(t) \Big| \, t$$

其中 $t = (t_1,t_2,\cdots,t_n)$。

在文献[11]中,将概率分为三类,分别是经典概率、频率概率以及主观概率,其中主观概率表示人对状态空间中事件元素发生的置信程度。由于 $\tilde{S}_k(t) \in [0,1]$,所以在进行系统风险评估时,可以将系统组件的工作状态 S_k 的隶属度 $\tilde{S}_k(t)$ 当作底事件的主观概率,进而求出顶事件发生的风险概率值。

3 例 子

用基于故障树的实时风险监测方法对一个具有前馈控制环的冷却系统[12]进行实时风险的监测。系统的示意图如图 1,该系统有一个泵唧水,使冷却水流过一个热交换器和一个阀门。酸液流入热交换器,被水冷却。如果内流液体温度过高时,阀门控制器便动作而加大阀门的开启度,增加冷却程度,保证输出的外流酸温度不至于过高。

通过分析,按照故障树建树原则和指南,建立如图 2 所示故障树。

为了方便表示与叙述,给出了故障树中底事件对应的代码,以及底事件的工作状态。这里假设所有底事件是二态的,见表 1,并在表中给出了各工作状态所对应的技术参数范围。

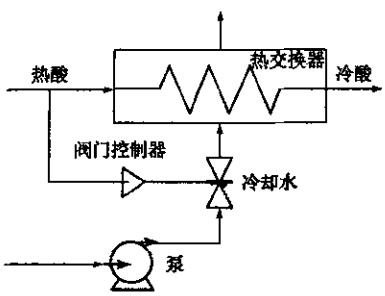

图1 具有前馈控制冷却系统示意图

Fig.1 Sketch diagram of cooling system with pre-feedback

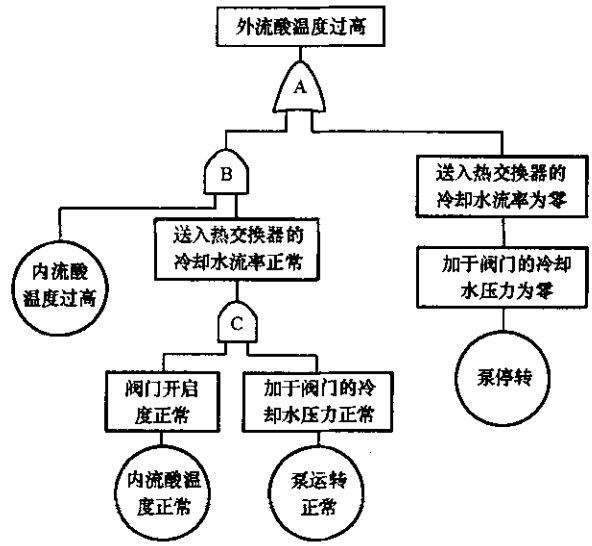

图2 含有前馈控制环的冷却系统故障树

Fig.2 Fault tree for cooling system with pre-feedback

表1 底事件代码与工作状态表

Tab.1 Table for basic events and their running status

代码	含义	状态	状态参数单位	工作状态
T	外流酸温度过高	高	℃	$x \geqslant 55$
		正常		$40 \leqslant x \leqslant 50$
A	内流酸温度过高	高	℃	$x \geqslant 100$
		正常		$60 \leqslant x \leqslant 90$
B	内流酸温度正常	正常	℃	$40 \leqslant x \leqslant 50$
		高		$x \geqslant 55$
C	泵运转正常	正常	r/min	$2800 \leqslant x \leqslant 2900$
		停转		$x \leqslant 1000$
D	泵停转	停转	r/min	$x \leqslant 1000$
		正常		$2800 \leqslant x \leqslant 2900$

依据冷却系统安全需求和仿真中获得的底事件各工作状态与顶事件对应关系,建立底事件对应部件工作状态关于部件技术状态参数的隶属函数 $T(x)$,$A(x)$,$B(x)$,$C(r)$,$D(r)$,如式(2)~(6)所示。

$$T(x)=\begin{cases}0 & 40\leqslant x\leqslant 50\\ \dfrac{x}{5}-10 & 50<x\leqslant 55\\ 1 & 55<x\end{cases} \tag{2}$$

$$A(x)=\begin{cases}0 & 60\leqslant x\leqslant 90\\ \dfrac{x}{10}-9 & 90<x\leqslant 100\\ 1 & 100<x\end{cases} \tag{3}$$

$$B(x)=\begin{cases}0 & 55<x\\ 11-\dfrac{x}{5} & 50<x\leqslant 55\\ 1 & x\leqslant 50\end{cases} \tag{4}$$

$$C(x)=\begin{cases}0 & x\leqslant 1000\\ \dfrac{x}{1800}-\dfrac{10}{18} & 1000<x\leqslant 2800\\ 1 & 2800<x\leqslant 2900\end{cases} \tag{5}$$

$$D(x)=\begin{cases}0 & 2800\leqslant x\\ \dfrac{28}{18}-\dfrac{x}{1800} & 1000<x\leqslant 2800\\ 1 & x<1000\end{cases} \tag{6}$$

以底事件所处状态为外流酸温度过高为例,说明隶属函数建立过程:当外流酸温度 $t\leqslant 50$℃时,底事件处于温度正常的工作状态,即外流酸温度正常,此时,将该时刻温度所对应的外流酸温度过高的隶属度设为 0;当温度 $t\geqslant 50$℃时,底事件处于温度过高的非正常工作状态,即外流酸温度过高。此时,将该时刻温度所对应的外流酸温度过高的隶属度设为 1;当 $50℃<t<55℃$,依据底事件的安全工作状态数据,设置其对应外流酸温度过高的隶属度。

由给出的隶属函数,根据当前底事件的工作状态参数得到底事件的发生概率(即底事件的隶属度),进而,依据故障树计算出顶事件发生概率。在表 2 中,给出了不同时刻底事件对应部件的技术状态参数以及顶事件的发生概率。

表 2 不同时刻下状态参数所对应的系统风险

Tab.2 System risk caused by status parameter at different time

时刻	参数组	状态名	状态参数值	隶属度	顶事件发生概率
T_1	第 1 组状态参数	A	98	0.8	0.80
		B	56	1	
		C	2799	0.9994	
		D	2799	0.0006	
T_2	第 2 组状态参数	A	98	0.8	0.61
		B	51	0.8	
		C	2440	0.8	
		D	2440	0.2	
T_3	第 3 组状态参数	A	99	0.9	0.91
		B	50.5	0.9	
		C	1180	0.1	
		D	1180	0.9	

如果系统风险的报警值 $W=85\%$,由于第 3 组状态参数所对应的系统风险概率 $W<91\%$,此时系统将会报警。同时,为了弄清楚系统风险过高的原因,可以借助故障树分析,得到此时底事件的概率重要度。此时的底事件的概率重要度如表 3 所示。

表 3 T_3 时刻各个底事件对应的概率重要度

Tab.3 Probability importance of every basic event at time T_3

时刻	参数组	状态名	概率重要度	顶事件发生概率
T_3	第 3 组状态参数	A	0.919	0.91
		B	0.081	
		C	0.009	
		D	0.009	

由于 $I_A^{\mathrm{Pr}}(t_3)>I_B^{\mathrm{Pr}}(t_3)>I_C^{\mathrm{Pr}}(t_3)=I_D^{\mathrm{Pr}}(t_3)$,所以,部件 A 的工作状态对系统安全影响较大,应当引起

足够关注。通过检修状态 A 所对应的部件,则可以有效防止事故出现,从而达到风险监控的目的。

4 结论

利用故障树对系统中多种风险因素的逻辑关系进行建模,提出了一种实时风险监测方法。该方法既可以监测系统的风险,又可以对形成风险的原因进行分析。同时,采用故障树建模具有直观简洁的优点,以其为描述工具进行实时风险监测,方便于工程的实现。对于安全状况只能通过间接测量系统的相关状态参数的系统,该方法尤为适用。然而,该方法的研究是在基于系统组成逻辑结构不变化的基础上进行的,是较为简单的一种情形。对于更复杂的情形,如当系统组件工作状态与系统风险的对应存在延时情形下实时风险的监测、系统逻辑结构动态变化时的实时风险的监测、系统中含有不可监测部件时的实时风险的监测,等等,我们将做进一步的深入研究。

参考文献:

[1] 周经伦,龚时雨,颜兆林.系统安全性分析[M].长沙:中南大学出版社,2003:14-19.

[2] Zhong M, Zhang X K, Wei X, et al. Safety Evaluation of Engineering and Construction Projects in China[J]. Journal of Loss Prevention in the Process Industries,2003,16:201-207.

[3] Marseguerra M, Zio E. Monte Carlo Approach to PSA for Dynamic Process Systems [J]. Reliability Engineering and System Safety, 1996,(52):227-241.

[4] Amari S, Dill G, Howald E. A New Approach to Solve Dynamic Fault Trees [A]. 2003 Proceedings of Annual Reliability and Maintainability Symposium[C], 2003:374-379.

[5] 支同祥.煤矿安全动态监控及决策信息系统研究[D]. 上海:同济大学机械工程学院,2003.

[6] 赵汝林.安全检测技术[M].天津:天津大学出版社,1999.

[7] 董豆豆,周经伦,冯静. 基于概率风险的系统安全性分析[J].国防科技大学学报,2005,27(1):98-101.

[8] 梅启智,廖炯生,孙惠中. 系统可靠性工程基础[M].北京:科学出版社,1987.

[9] 冯静,吴孟达. Profust 故障树建模与分析[J].国防科技大学学报,2001,23(1):85-88.

[10] 刘普寅,吴孟达. 模糊理论及其应用[M]. 长沙:国防科技大学出版社,1998.

[11] Tim B, Roger C. Probabilistic Risk Analysis: Foundations and Methods [M]. uk: Cambridge University Press, 2001.

[12] 亨利 E J.可靠性工程与风险分析[M].北京:原子能出版社,1988:68-72.

(上接第105页)

参考文献:

[1] 三轮修三,下村玄.旋转机械的平衡[M].北京:机械工业出版社,1992.

[2] 叶能安,余汝生.动平衡原理与动平衡机[M].武汉:华中工学院出版社,1985.

[3] 何川,毛乐山,等.一种快速跟踪带通滤波器的实现[J].振动、测试与诊断,2002,22(3):212-216.

[4] Bustamante L G, Soderstrand M A. High-range Switched-capacitor Tracking Filter[A]. Proceedings of IEEE International Symposium on Circuits and Systems[C],1999,2:65-68.

[5] 孙向东,王秀方.用开关电容电路技术实现的七阶椭圆函数滤波器[J].郑州轻工业学院学报,1998,13(1):45-49.

[6] 胡毓涛.动平衡测量中的滤波技术[J].电脑与信息技术,1997,5(4):33-35.

[7] 陈照章.跟踪滤波器的设计及其应用[J].仪器仪表学报,2001,(6):244-246.

[8] 陈怀超,丛培田.基于开关电容的自动跟踪滤波器的设计及研究[J].仪表技术与传感器,2003,(10):38-39.

[9] 江驹,沈勇璋,汪旭旦.智能化动平衡测量仪的研制[J].数据采集与处理,2000,15(4):476-480.

[10] 黄金法.开关电容滤波器 IC 发展概况[J].振动、测试与诊断,1991,11(2):53-62.

[11] 温熙森,陈循,唐丙阳.机械系统动态分析理论与应用[M].长沙:国防科技大学出版社,1998.

[12] 约翰逊 D E,约翰逊 J R,穆尔 H P.有源滤波器精确设计手册[M].北京:电子工业出版社,1984.