文章编号: 1001－2060(2010)06－0642－06

FSSS的故障树建模及可靠性分析

沈继忱[1], 李晓光[1], 李 旸[1], 鲁旭光[2]
(1.东北电力大学 自动化工程学院, 吉林 132012; 2.日照钢铁有限公司, 山东 日照 276806)

摘 要: 介绍了 FSSS作为一种安全仪表系统与基本过程控制系统的区别; 针对 FSSS进行故障树建模, 建立了炉膛安全监控系统各个部分之间的联系。通过故障树建模并分解为各个部分的故障数据, 并应用图形符号链接表示。由故障树可得出逻辑公式, 从而可以定量分析其可靠性。提供了一种从整体可靠性来评价系统的方法。

关 键 词: 故障树; 炉膛安全监控系统; 安全仪表系统; 可靠性

中图分类号: TP273; TK229 文献标识码: B

引 言

针对电力生产控制系统目前并没有固定的评价指标和规程, 国际电工委员会曾经出台过关于可靠性规范的两个标准 IEC60300和 IEC61580, IEC60300侧重于可靠性管理的方面, 与 ISO9000系列一起作为质量体系的管理认证, IEC61580将系统可靠性分为 4个安全度等级, 每个等级包括两个定量的安全要求, 即系统连续操作每小时故障概率 (PFH)和按要求模式执行指定功能的故障概率 (PFD); 将系统可靠性大致地分为几个档次, 用以评价系统的优劣。但是这种分析方法并不完善, 尤其是在系统的设计阶段, 准确定量的分析系统的可靠性数据是需要更多的参数和数值来进行改进和优化的。所以能够定量评价控制系统的可靠性的方法的研究是有需求的, 本文提供了一种通过故障树对控制系统进行建模分析的新思路。

1 FSSS系统简介

FSSS属于一种 (SIS)安全仪表系统, 设置它的目的是监视工业过程中潜在的危险状态, 并且发出警告信息或执行预定程序, 防止锅炉的危险事件发生。FSSS并没有改进生产过程的产量, 也没有提高生产过程的效率, 但是它通过减少损失节约了资金, 降低了风险成本。它的主要功能有主燃料跳闸 (MFT)、锅炉清扫和火焰检测等, 系统结构如图 1所示。

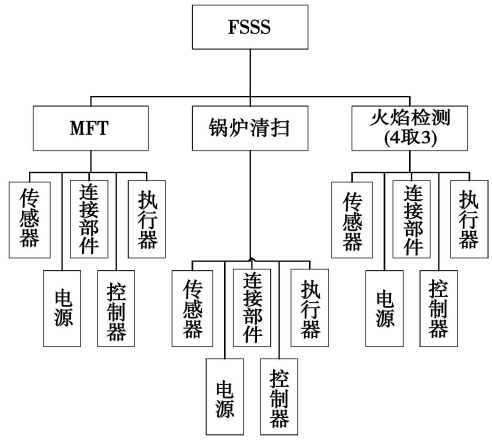

图 1 FSSS系统结构

2 安全仪表系统的特点

在控制系统中, 安全保护设备一般是和控制设备分离的。控制设备被称为过程控制系统 (BPCS), 而保护设备则被称为安全仪表系统 (SIS)。基本控制系统读取过程传感器的数据, 进行连续控制, 或顺序控制计算, 并向执行装置 (阀门或电机)发出指令。安全仪表系统读取传感器的数据, 进行计算或实现判别潜在危险工况的逻辑, 把结果输出送给执行机构。以避免出现危险工况。安全仪表系统可单独或同时保护人员、设备和环境, 如图 2所示。

基本控制系统 BPCS和安全仪表系统 SIS对可靠性和安全性的要求不同。基本控制系统强调可用性, 即在任何时候系统都能够正常工作的概率。基本控制系统追求的是可用时间最大化, 因为在许多过程控制领域, 非计划停机是一个损失非常大的事

收稿日期: 2009－11－17; 修订日期: 2010－01－15
作者简介: 沈继忱 (1954－), 男, 吉林长岭人, 东北电力大学副教授.

件。失效模式（安全或危险）是一个要考虑的问题，但是可用性是第一位的。而安全仪表系统则正好相反。它的设计必须保证系统在故障情况下是安全的。可用性是一个需要重点考虑的问题，但安全性是第一位的。

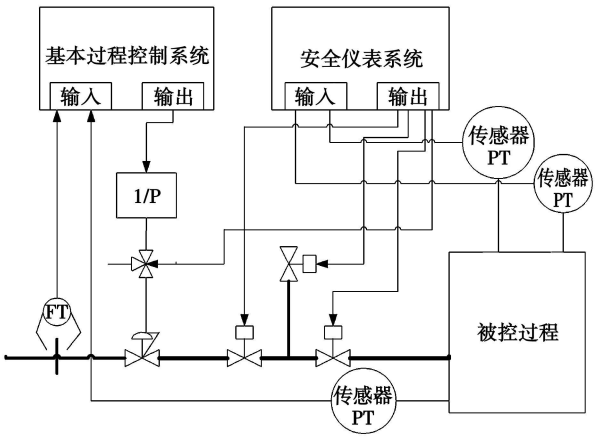

图 2　安全仪表系统与过程控制系统

所分析的炉膛安全监控系统是一种典型的安全仪表系统，当锅炉的燃烧系统非正常工作时，FSSS自动执行设定程序，保护系统设备的安全运行。从FSSS的结构可以了解到，对于FSSS的几个主要解决的逻辑部分之间是相互独立的，每一个实现功能的分系统都有自己的传感器、独立电源、控制器和执行器。因此，针对各个独立的分系统分别建立故障树。

3　故障树建模及分析步骤

故障树控制系统通过对可能造成产品故障的硬件、软件、环境和人为因素等进行分析，画出故障树从而确定产品故障原因的组合方式并确定其发生概率的一种分析技术。通过FTA得到的分析结果可以帮助判断潜在故障，从而改进维修方案。FTA的最终结果就是一张图，它是由一系列的符号组合表示的，可以表明由于那些事件的组合可能会导致系统故障。当一个故障树完成时，它可以描述在各种故障条件下，系统会发生什么情况；也可以在系统的设计阶段使用故障树对系统进行分析，分析结果可以帮助判断设计的合理性以及各种隐患，它也为更详细的可靠性和安全性分析提供了必要的文件。

故障树分析法的基本步骤为：

（1）了解系统，确定顶事件；

（2）建造失效树，并加以简化和规范化；

（3）定性分析，确定失效树的最小割集；

（4）收集定量分析用的数据，如底事件的失效概率、失效率、维修率等；

（5）定量分析，计算顶事件的发生概率和系统可靠度、评价顶事件的严重性与危害度，计算底事件和最小割集的重要度等；

（6）确定薄弱环节和关键元部件；改进系统的可靠性、安全性。

FTA分析中主要的工作体现在故障树的建模，即绘制故障树图上。在图中，使用了常用并易于辨识的符号来连接故障的顶事件和各级事件，常用符号如图 3所示。

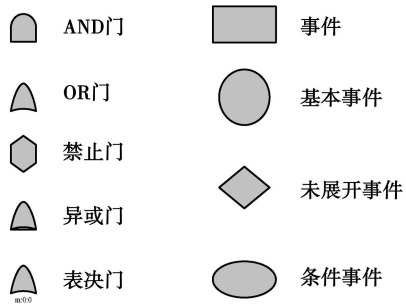

图 3　故障树常用符号

顶事件或者称为“最终故障”，用一个方框来表示。事件或最终故障是某些事件通过与、或关系联系在一起所形成的结果。菱形用来表示一个未展开事件或是不完整事件，它是指菱形框内事件包含着其它的与所分析问题不相关的事件。圆形代表基本事件，是指基本故障或引发事件，这些通常被认为是造成故障的根源，在故障树中位于故障树的最低端。

与门（AND门）表示当且仅当所有输入都存在时，输出才被激励。

或门（OR门）表示任何一个输入被激励，该或门的输出就会被激励。

禁止门表示所有输出都取决于禁止指令，当禁止指令允许输出时，输入信号才能参与运算。

表决门表示的是 n选 m，若总条件（n）中有 m件成立，则通过，输出信号。

4　MFT动作失效的故障树分析

主燃料跳闸（MFT）是燃烧管理器中的重要部分，它连续监视各种安全条件是否满足，一旦出现危险工况，就会切断所有进入炉膛的燃料，包括油和煤的输入。MFT的逻辑实现如图 4所示，在逻辑图

中,中间部分的 MFT代表 MFT动作,最上面一排表示能够引起 MFT动作的条件,最下面一排表示 MFT后产生的一系列动作。

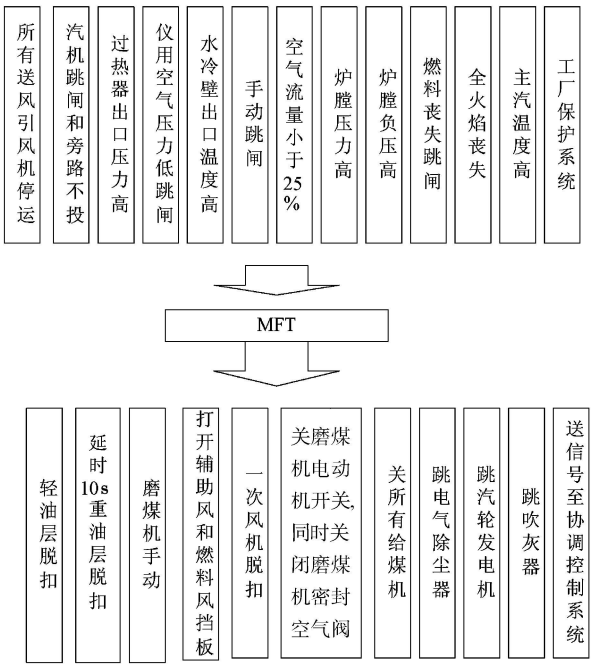

图 4 MFT(主燃料跳闸)的允许条件及产生结果

在这个分系统里,定义 MFT动作失效为顶事件,能够引起 MFT动作失效的条件大体可以分为 3部分:DCS故障、跳闸动作失效和引起 MFT的条件本身故障。

在 DCS故障中,传感器故障可导致系统所监测的条件无法传输或传输错误信息到主机;由于系统通信和软件引起的失误等其它事件统一归类到了通信故障中。在定量计算时,这两种故障的故障率数值可以直接使用 DCS设备说明书里提供的失效率,也可以分开采用传感器和 DCS的数据分开计算;因为 DCS本身失效率很低,必要时候可以忽略。

跳闸动作失效多数为机械故障,包括阀门、齿轮、轴承等。跳闸失灵等情况也归到一类。这些数据都可以根据设备的型号、批次确定故障率等参数。其中 MFT动作后会引起一系列的动作,作用是保护锅炉,避免炉内发生爆燃等严重事故。这些动作涉及到磨煤机、给煤机、电气除尘器等相关设备的可靠性,加上 MFT本身存在的失效几率形成跳闸动作故障分支。

引发 MFT动作条件中的部分条件涉及到送引风机、汽机旁路、过热器、火焰摄像头等相关设备。在图中简化列出了部分设备,考虑到这些设备的固有故障率可以直接代入,并没有进行故障树的继续分支,而这样已经能够满足组装产品设计的要求。

图 5为主燃料跳闸动作失效故障树。如图所知,故障树经过合并简化以后的最终结果省略了与门的使用,完全由或门连接表示,这将使针对系统的故障率的定量计算大大简化。在本树中,最底端的每一个事件都可以视为一个独立的最小割集,既每一个底端事件的发生都将导致故障树顶端的事件(不希望事件)发生。而通过或门的连接可以使顶事件的故障率的计算可由底端事件的故障率简单相加得到。

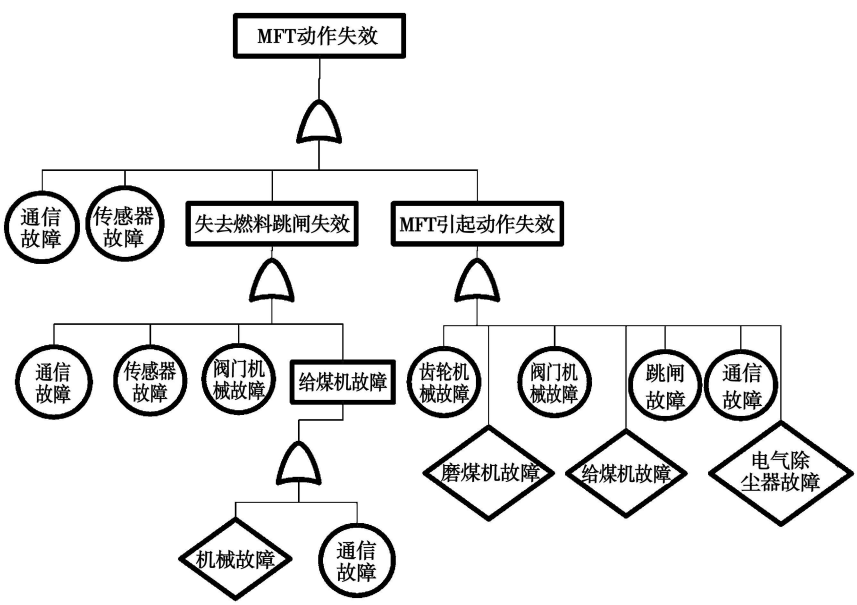

图 5 主燃料跳闸动作失效故障树

通过底端事件概率的大小, 以及底端事件能够给予系统造成的危害程度, 可以准确地计算并对比, 从而得到事故危害的严重性。越是严重的部位, 越是整个系统的薄弱环节, 这些就成为系统设计时需考虑的一些可靠性设计的相关环节。比如: 是否需要冗余, 是否采用部件降额使用, 是否需要耐环境的设计等。同样在生产过程中, 故障树结果也能给科学管理提供支持, 如合理的制定检修计划, 科学记录运行和故障数据等。

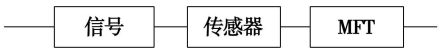

图 6　串联系统

发生 MFT之前的过程, 只有 3个步骤构成串联系统, 如图 6所示。系统可视为 3个部件串联组成。定义如下符号:

$R_{信号}$—触发条件所涉及的部件和设备正常工作的概率;

$R_{传感器}$—触发条件所涉及的传感器正常工作的概率;

R_{MFT}—主燃料跳闸动作所涉及部件和设备正常工作的概率。则针对系统有:

$$R_S = R_{信号} + R_{传感器} + R_{MFT} \quad (1)$$

针对相互独立事件有:

$$P(A \cap B) = P(A) \cdot P(B) \quad (2)$$

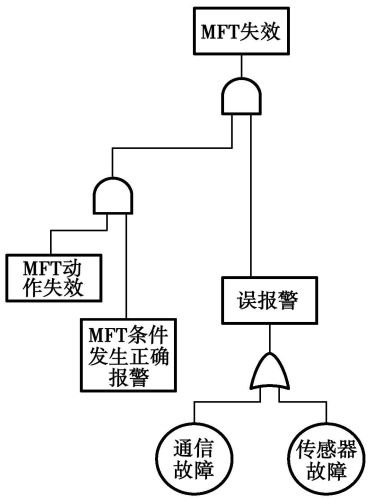

图 7　主燃料跳闸逻辑失效故障树

由于炉膛安全监控系统 (FSSS)是一个安全仪表系统 (SIS), 仅仅考虑到 MFT的动作失效并不能表示系统的可靠性, 因为 MFT不是一个生产过程, 它只有在过程控制中出现危险状况或警报时才会启动, 错误报警能够引起系统失效, 并产生误操作, 但是只要是 MFT所引发的动作能够实现, 功能就不是完全丧失, 所以, 针对 MFT的故障树应该是在发生报警的前提下进行进一步的计算。

如图 7所示 MFT失效, MFT动作失效与 MFT条件发生两个分支相互独立, 也应当使用或门连接。

由图 5建立的故障树中, 通过故障树向下行法求最小割集。

表 1　求主燃料跳闸动作失效故障树的最小割集

0	1	2	3
MFT动作失效 (T)	通信故障 (A_1)		
	传感器故障 (A_2)		
	失去燃料跳闸失效 (A_3)	通信故障 (B_1)	
		传感器故障 (B_2)	
		阀门机械故障 (B_3)	
		给煤机故障 (B_4)	机械故障 (C_1)
			通信故障 (C_2)
	MFT引起动作失效 (A_4)	齿轮机械故障 (B_5)	
		阀门机械故障 (B_2)	
		跳闸失效 (B_6)	
		通信故障 (B_1)	
		磨煤机故障 (B_7)	
		给煤机故障 (B_4)	
		电气除尘器故障 (B_8)	

得到的结果为:

$$T = \sum A_n = A_1 + A_2 + B_1 + B_2 + B_3 + C_1 + C_2 + B_1 + B_2 + B_4 + B_3 + B_6 + B_7 + B_8$$

表 2　主燃料跳闸逻辑失效故障树求最小割集

0	1	2	3
MFT失效 (X)	MFT动作失效	T	
	MFT条件发生 (S)	误报警 (S_1)	通信故障 (B_1)
			传感器故障 (B_2)
		正确报警 (S_2)	

$$X = T + X - T \cdot S = T + B_1 + B_2 + S_2 - TB_1 - TB_2 - TS_2$$

MFT动作失效和 MFT条件发生属于非互斥事件, 也就是说, 两个条件并没有冲突, 根据可靠性理论的近似计算, 则得:

$$X = T \cdot S_2 + S_1 = B_1 + B_2 + T \cdot S_1 = B_1 + B_2 + (A_1 + A_2 + B_1 + B_2 + B_3 + C_1 + C_2 + B_1 + B_2 + B_4 + B_3$$

$+B_6+B_7+B_8)\cdot S_2$

5 锅炉清扫的故障树分析

锅炉清扫是在锅炉点火前或熄火后进行，以除去炉膛、烟道以及管道中可能残存的可燃性混合物，防止点火时引起炉膛爆燃。图 8是锅炉炉膛吹扫的逻辑。

如图 8所示，在触发条件以左的部分可以看做一个整体，当所有条件均满足时，才能启动炉膛吹扫程序，任何一个相关部件的故障都可能引发系统失效，这也是典型的串联系统；在此例吹扫逻辑中，触发条件完全后，要求辅助风挡板置吹扫位（30%），关闭 SOFA挡板并置摆动喷嘴水平，在辅助风挡板和 SOFA挡板就位以后，才能发出吹扫请求。

由方框图可以初步判断，引发系统失效的故障模式可能有机械故障、逻辑故障、定时和通信故障等。

5.1 锅炉炉膛清扫逻辑设计与故障假设

以直吹式制粉系统为例，强制性连锁吹扫逻辑启动后假设存在以下故障可能：

（1）由该磨煤机供煤的所有燃烧器的点火器已投入，假设此时燃烧器会有极小的概率失效，引发原因可能有机械、电源等；

（2）证实点火器着火以后，启动一次风机，风机故障包括机械和电气等方面；失去一次风机或排粉机时，有关的燃烧器关断门或相当的设备应跳闸关闭，给煤机应跳闸；

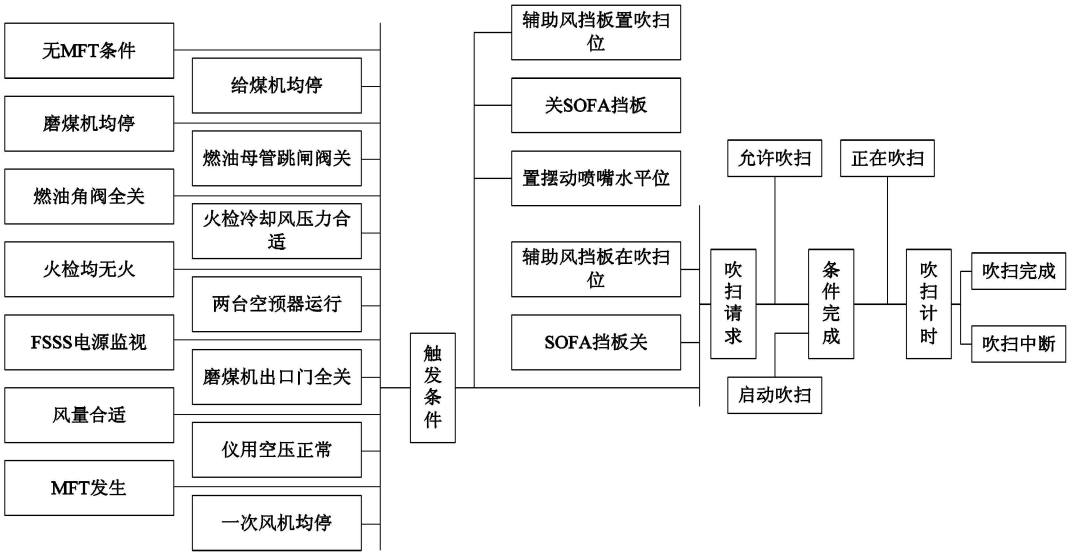

图 8 炉膛吹扫程序逻辑图

（3）可能会存在有磨煤机故障和给煤机故障，与风机故障相似，此时出现的故障应当属于串联系统结构的部分，即只要有一个部件发生故障，整个吹扫系统都将失效。磨煤机故障时，给煤机应跳闸和一次风关断门应关闭；给煤机故障时，应发出报警信号，并在给煤机启动条件没有重新建立之前，应一直处于闭锁状态。

5.2 锅炉炉膛清扫逻辑故障树建模与分析

由炉膛清扫的逻辑图可知，逻辑触发前的各种条件和吹扫逻辑本应使用与门（任何条件未达成均不能触发）连接，但是考虑到系统是属于安全仪表的范畴，当逻辑被启动以后，锅炉处在不正常运行的时期，操作人员本身会给予足够重视，存在人为失误的几率可视为零，在最终图中将结果简化为一个或门表示，如图 9所示。

6 火焰检测功能的故障树分析

火焰检测是锅炉安全系统中非常重要的组成部分，炉膛爆炸大部分是由于炉膛灭火，随后积聚起来的可爆性燃料空气混合物再燃烧而引起的。

一个高质量的火焰检测系统，包括设计和制造精良可靠的火焰检测器硬件及一个考虑周到、适用的火焰检测逻辑，可以作为锅炉安全系统的最后防线，火焰检测逻辑如图 10所示。能够及时可靠的测出“炉膛灭火情况”并通过“全炉膛灭火”的 MFT切

断一切燃料。整个火焰检测系统的故障可以分布到各个火焰探头的传感故障和相关设备的机械故障上，具体分析如图 11所示。

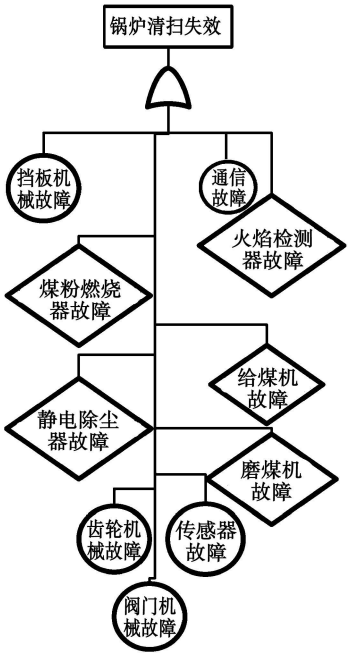

图 9　锅炉清扫失效故障树

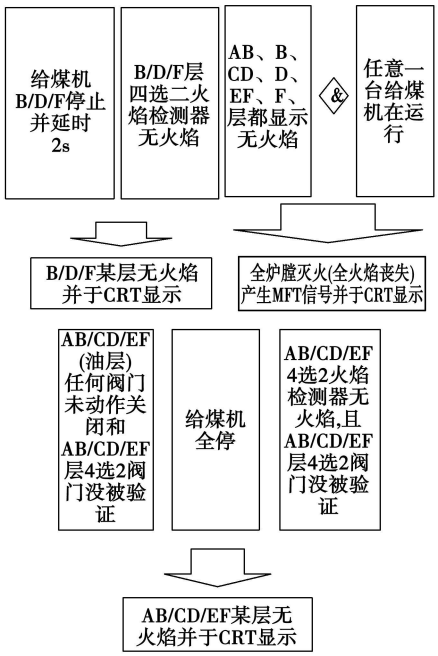

图 10　煤粉、油层和全炉膛灭火火焰检测逻辑

从图 10中可以了解到，有些情况下，1个火焰检测器出故障并不会影响整个系统的判断，在可靠性分析时，这种情况所引起的后果并不是非常严重，即低严重度底端事件，对于这个系统来说，火焰检测器的关键性较为次要。

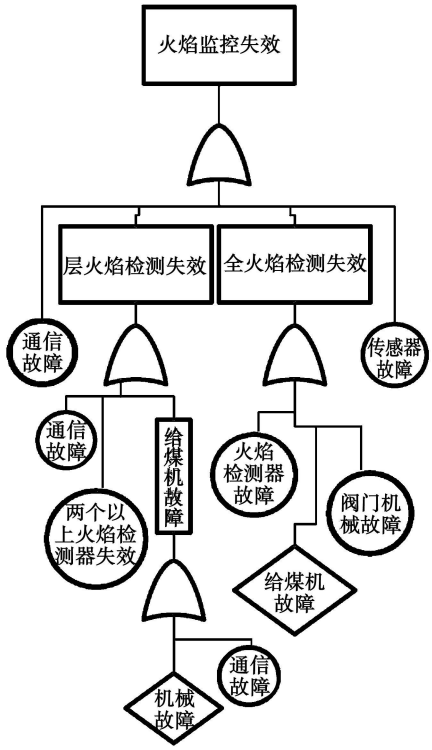

图 11　火焰监控失效故障树

7　结　语

以上所作的故障树，都为最终的简化结果，故障树中并没有考虑相关设备的冗余结构，在图中将最终结果简化表示为使用或门连接的树形结构，要想得到故障树顶端事件的最终故障率，只需要将逐层结果的实效概率值一一代入并相加就能分析出系统故障率。

这种方法分析手段清晰明了，能够准确确认系统的薄弱环节，并且摆脱了以往对于系统故障分析时抽象的数据统计，为解决系统的整体可靠性提供了新思路。

参考文献：

[1]　戈布尔·威廉. 控制系统的安全评估与可靠性[M]. 白　焰，董　玲，杨国田，译. 北京：中国电力出版社，2008.

（编辑　陈　滨）

炉膛压力对增压锅炉热力参数的影响 = Influence of the Furnace Pressure of a Turbocharged Boiler on Its Thermal Parameters[刊, 汉] / DU Xiao-jian, CHEN Ming, LIU Li-hua et al(CSIC No. 703 Research Institute, Harbin, China, Post Code: 150036)// Journal of Engineering for Thermal Energy & Power. — 2010, 25(6). — 635 ~ 638

Under the condition of the furnace pressure undergoing a change, systematically analyzed was the variation regularity governing the relevant thermal calculation parameters of a turbocharged boiler. A case calculation was performed of a certain type of turbocharged boiler and the curves of its flue gas flow velocities and furnace blackness changing with its furnace pressure were obtained. When its furnace pressure increases, its volumetric thermal load and furnace blackness will also increase. The flue gas temperature and linear flow speed at the outlet of the furnace etc will decrease and the convection heat exchange coefficient and other parameters of the flue gas, however, will maintain unchanged. Key words: turbocharged boiler, furnace pressure, thermal calculation, thermal parameter

锅炉钢材表面处理后耐磨损性能试验研究 = Experimental Study of the Wear-resistant Performance of the Steel Heating Surfaces of a Boiler After a Surface Treatment[刊, 汉] / ZHAO Xian-ping, YIN Xiang-de, LIU Shuai(College of Energy Source and Environment Engineering, Shanghai University of Electric Power, Shanghai, China, Post Code: 200090)// Journal of Engineering for Thermal Energy & Power. — 2010, 25(6). — 639 ~ 641

Experimentally studied was the performance of the commonly used alloy steel 12Cr1MoV to resist hot state flying ash erosion and wear at a temperature ranging from 300 to 450 ℃ on the heating surfaces of a boiler after a surface ion borotitanizing treatment. The research results show that the alloy steel 12Cr1MoV following the treatment has a relative surface mass wear-and-tear wastage less than that prior to the treatment, i.e. the wear-resisting property is improved. The relative surface mass wear-and-tear wastage will first decrease and then increase with an increase of the temperature. After the test, the test pieces were analyzed by using a SEM (scanning electron microscope) and a glow discharge spectrometric analyzer. It has been found that the thicker the test piece surface permeation layer, the higher the boron and titanium element content in the permeation layer and the more uniform the boron and titanium element distribution, then the better the wear-resisting property. Key words: utility boiler, heating surface, hot state flying ash, wear, ion borotitanizing

FSSS的故障树建模及可靠性分析 = Modeling of a FSSS (Furnace Safety Supervisory System) Fault Tree and Its Reliability Analysis[刊, 汉] / SHEN Ji-chen, LI Xiao-guang, LI Yang(College of Automation Engineering, Northeast Electric Power University, Jilin, China, Post Code: 132012), LIU Xu-guang(Rizhao Iron and Steel Co. Ltd., Rizhao, China, Post Code: 276806)// Journal of Engineering for Thermal Energy & Power. — 2010, 25(6). — 642 ~ 647

Described were a furnace safety supervisory system and its difference from a basic process control system when serving as a safety instrumentation system. A modeling of the fault tree of the system under discussion was performed and the relationship between various parts of the system was set up. Through the modeling of a fault tree, the above-

mentioned relationship was decomposed into fault data in various components and expressed by using an interlinking of graphic symbols. Moreover, logic formulae were obtained on the basis of the fault tree and thereby their reliabilities were quantitatively analyzed. The foregoing can provide a method for evaluating a system based on its overall reliability. Keywords: fault tree, furnace safety monitoring and control system, safety instrumentation system, reliability

多孔介质燃烧—换热器内燃烧和传热的数值模拟 = Numerical Simulation of Porous Medium Combustion-Combustion and Heat Transfer Inside a Heat Exchanger[刊, 汉] / XU You-ning, SHI Jun-rui, XUE Zhi-jia (Shenyang City Key Laboratory on Circulating Fluidized Bed Combustion Technology, Shengyang Engineering College, Shenyang, China, Post Code: 110136), XIE Mao-zhao (College of Energy Source and Power, Dalian University of Science and Technology, Dalian, China, Post Code: 116024) // Journal of Engineering for Thermal Energy & Power. — 2010, 25(6). —648 ~652

By establishing a two-dimensional numerical model, studied were the porous medium combustion-combustion and heat transfer inside a heat exchanger and the influence of the system configuration on the thermal efficiency and the pressure drop of a combustion-heat exchanger. The research results show that the longitudinal distance of the heat exchange tubes has a remarkable influence on the temperature distribution, heat transfer speed and pressure loss inside the heat exchanger. To decrease the longitudinal distance of the heat exchange tubes can increase the thermal efficiency and pressure loss. The horizontal distance of the heat exchange tubes, however, has a very little influence on the thermal efficiency and pressure loss. In addition, to increase the diameters of small balls may result in an increase of the thermal efficiency and a sharp decrease of the pressure loss. The effectiveness of the numerical model can be verified through tests. Keywords: numerical study, porous medium, combustion-heat exchanger

压力容器泄漏孔大小的压力变化率预估方法 = A Method for Pre-estimating the Size of Leakage Holes of a Pressure Vessel Based on Its Pressure Variation Rate[刊, 汉] / SHEN Yuan-sheng, LIU Zong-ming, ZHAO Wei-lin, et al (College of Material Science and Engineering, Jinan University, Jinan, China, Post Code: 250022) // Journal of Engineering for Thermal Energy & Power. — 2010, 25(6). —653 ~656

To pre-estimate the size of leakage holes of a pressure vessel, analyzed were the gas flow regularity inside the leakage holes and the gas parameter status characteristics inside the vessel. In this connection, three assumptions for the process were put forward and a mathematical model reflecting the equivalent radius of the leakage holes, established. On this basis, a method was proposed for pre-estimating the equivalent radius of the leakage holes based on the pressure variation rate. An experimental study has been performed of the pressure conditions in the vessel, which has a volume of 0.008 48 m^3 and three leakage holes with a radius of 0.4 mm. Furthermore, the radius of the leakage holes was calculated by using the mathematical model being established. The research results show that the calculated value of the radius of the vessel is in very good agreement with the actual one. This can provide important reference for further studying the leakage hole conditions and leakage regularities of various pressure vessels. Keywords: fluid dynamics, pressure vessel, leakage hole, equivalent radius, pressure variation rate