研究报告

基于可视化的事故树分析系统研究与开发

施式亮，卢本陶
（湖南科技大学能源与安全工程学院，湖南 湘潭 411201）

[摘要] 事故树分析是安全系统工程最重要的分析方法之一，它能对各种系统的危险性进行辨识和评价，不仅能分析出事故的直接原因，而且能深入地揭示出事故的潜在原因。用它描述事故的因果关系直观、明了，思路清晰，逻辑性强，既可定性分析，又可定量分析。基于可视化理论和技术，建立了事故树可视化模型，确定了系统功能目标，完成了系统结构设计，构造了事故树图形生成与事故树动态分析于一体的集成分析环境，开发出事故树计算机分析系统，为事故分析和安全评价提供高效、准确的技术和方法。

[关键词] 安全技术；安全评价；事故树；可视化；分析系统
[中图分类号] X913.4 [文献标识码] A [文章编号] 1009－1742（2004）11－0066－07

1 引言

安全、舒适和健康是人类生活和生产活动中追求的理想目标。安全系统工程是正在发展、完善并得到迅速推广应用的，并能保障该理想目标实现的最重要工程技术之一。它以安全生产过程中的人—机—环境等综合系统为研究对象，以消除和控制系统中的危险因素为目的，对系统安全问题，经过分析、识别、推理、判断，建立安全系统模型，用系统工程的方法进行综合分析与评价，并采取防范措施消除或控制系统中的不安全因素，杜绝系统事故的发生或使事故发生减小到最低限度，从而使系统达到最佳安全状态。危害辨识与安全评价是事故预防与控制的关键技术，事故树分析方法则是安全评价最重要的方法之一[1]。应用于实际工程的事故树结构复杂且庞大，传统的事故树分析方法，其结构的设计、生成、分析等环节依据人工方法进行。在计算机应用推广后，借助计算机进行事故树分析获得较大进展，但是大多是在事先编制好程序的基础上进行，整个过程处于“黑箱”之中，只有在获得结果后才可以进行分析、判断前期工作的合理性和准确性，不能实现事故树构造、分析、修改、再分析过程的“透明作业”，给事故分析和控制过程带来很大的困难，而且效率低下。计算机科学技术发展的重要分支学科——可视化理论与技术的诞生[2]，为开发基于可视化的事故树分析系统提供了良好的前提条件。

20 世纪 80 年代末出现的科学计算可视化，将科学计算的过程和结果转化为图象，使人与数据、人与人之间实现图象通信，对计算过程实现引导与控制并观察其影响，极大地提高了数据处理的速度和质量，实现了科学计算工具和环境的现代化。可视化（visualization in scientific compu-ting，ViSC）是计算机科学、计算机图形学、图形用户界面以及面向对象的程序设计技术有机结合的产物。美国自然科学基金会（NSF）于 1986 年为此专门召开了学术研讨会，并在会上提出了科学计算可视化（visualization in scientific computing，简称 ViSC），1987 年形成了正式的 ViSC 报告，从此诞生了一门崭新的交叉学科，解决对客观世界仿真、预处理、

[收稿日期] 2004－04－16
[基金项目] 国家自然科学基金资助项目（50274060），国家安全生产监督管理局科研计划项目（03－103），湖南科技大学博士启动基金资助项目（E50207）。
[作者简介] 施式亮（1962－），男，浙江天台县人，湖南科技大学能源与安全工程学院教授，博士

映射、绘制和解释的问题，它使得研究人员能够观察模拟和计算过程，并实现人机交互控制，从而使得该学科在诸多工程领域得到广泛的应用，而且应用研究方兴未艾[3,4]。

2　事故树分析（fauly tree analysis，FTA）方法简介

2.1　事故树分析概述

系统安全分析是从安全角度对系统进行的分析。它通过揭示可能导致系统故障或事故的各种因素及其相互关联来查明系统的危险源，以便采取措施消除或控制他们。目前人们已开发了数十种系统安全分析方法，在危害辨识中得到广泛应用的系统安全分析方法主要有安全检查表、预先危害分析、故障类型和影响分析、危险性和可操作性分析研究、事故树分析和因果分析[1]等。其中事故树分析是安全系统工程学科中最重要的技术和方法。

事故树分析（FTA）技术是美国贝尔电话实验室于 1962 年开发的，它采用逻辑方法，形象地对危险进行分析。其特点是直观、明了，思路清晰，逻辑性强，可以做定性分析，也可以做定量分析，体现了以系统工程方法研究安全问题的系统性、准确性和预测性，它是安全系统工程的主要分析方法之一。1974 年美国原子能委员会发表了关于核电站危险性评价报告，即“拉姆森报告”，大量、有效地应用了 FTA，从而迅速推动了它的发展和应用。

2.2　事故树分析程序和内容

事故树分析的基本程序主要有 9 个方面[5]，具体内容及其分析流程如图 1 所示。

1）*确定所分析的系统*　确定分析系统即确定系统所包括的内容及其边界范围。

2）*熟悉所分析的系统*　指熟悉系统的整个情况，包括系统性能、运行情况、操作情况及各种重要参数等，必要时要画出工艺流程图及布置图。

3）*调查系统发生的事故*　调查分析过去、现在已发生的和未来可能发生的故障，同时调查本单位及外单位同类系统曾发生的所有事故。

4）*确定事故树的顶上事件*　是指确定所要分析的对象事件。将易于发生且后果严重的事故作为顶上事件。

5）*调查与顶上事件有关的所有原因事件*。

6）*事故树绘图*　按建树原则，从顶上事件起，一层一层往下分析各自的直接原因事件，根据彼此间的逻辑关系，用逻辑门连接上下层事件，直到所要求的分析深度，形成一棵倒置的逻辑树形图，即事故树图。

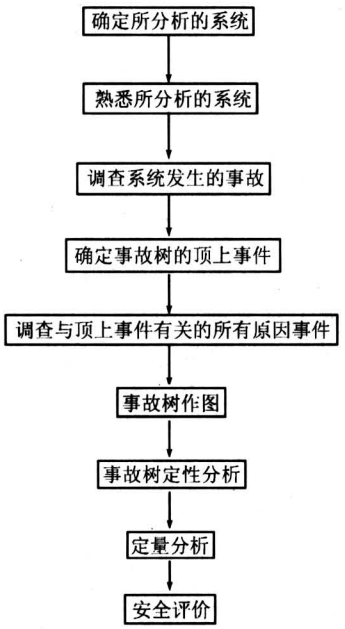

图 1　事故树分析流程

Fig.1　Flow chart of FTA

7）*事故树定性分析*　定性分析是事故树分析的核心内容之一。其目的是分析该类事故的发生规律及特点，通过求取最小割集（或最小经集），找出控制事故的可行方案，并从事故树结构上、发生概率上分析各基本事件的重要程度，以便按轻重缓急分别采取对策。

8）*定量分析*　定量分析包括：**a.** 确定各基本事件的故障率或失误率；**b.** 求取顶上事件发生的概率，将计算结果与通过统计分析得出的事故发生概率进行比较。

9）*安全评价*　根据上述事故定性分析和定量分析结果，评价目标系统该类事故的危险性，并从定性和定量分析结果中找出能够降低顶上事件发生概率的最佳方案，达到降低或消除事故的危害，保证系统安全。

3　事故树分析可视化理论模型

3.1　理论模型

为了表现可视化过程，必须对其核心部分进行抽象，其理论模型的建立必须是准确、完整和合理

的。可视化应用系统的开发以“可视化流水线(visulization pipiline)”[2,3]作为理论模型，如图2所示。

图2 可视化系统开发理论模型

Fig.2 Theoretical model of ViSC system

该模型将整个可视化过程划分为模拟、预处理、映射、图形和解释5个步骤。模拟部分是对物理现实的数学模拟；预处理和映射两部分通常组合在一起，是整个理论模型的关键；图形通过对形状、颜色、明暗甚至动画等处理手段，将系统分析过程以形象直观的方式提供给用户；解释是图形与数学分析的结合部，实现了图形与动态分析的有机综合。

3.2 系统开发过程必须解决的关键问题

系统开发的关键问题是构造集事故树图形生成与事故树动态分析于一体的集成分析可视化环境。随着计算机科学技术的不断发展，其强大的功能已成为人们共识，使用计算机对事故树进行分析，具有效率高、准确度高、使用方便、直观等特点，但必须解决好系统开发的关键问题，如系统安全特性和过程分析、安全分析方法选择、事故树分析理论模型确定、可视化实现的条件和步骤等，这些问题是开发基于可视化的事故树分析计算机软件系统的前提。事故树分析可视化系统开发模型如图3所示[1]，后续的系统研发均以该模型为基础。

4 事故树可视化分析系统功能目标

为了实现事故分析和安全评价的目标，事故树可视化分析系统应具有比较完善的功能，必须实现图形生成与事故动态分析的集成，这是系统开发的根本目的，系统的主要功能如图4所示。

1) 事故树图形生成 事故树的绘制的程序所需达到的目标是：选中菜单或工具栏的事故树绘制，即弹出对话框，输入该事件的标题。若是中间事件，选定该事件下的与、或门形式。若是基本事件，输入该基本事件的代号和该事件的发生的概率。输入完成后，系统会自动绘制出该图形，当不是顶上事件时，你需点击所要联接的门进行联接。这样系统会自动记录这此数据。如此逐步绘制，直到完成为止。

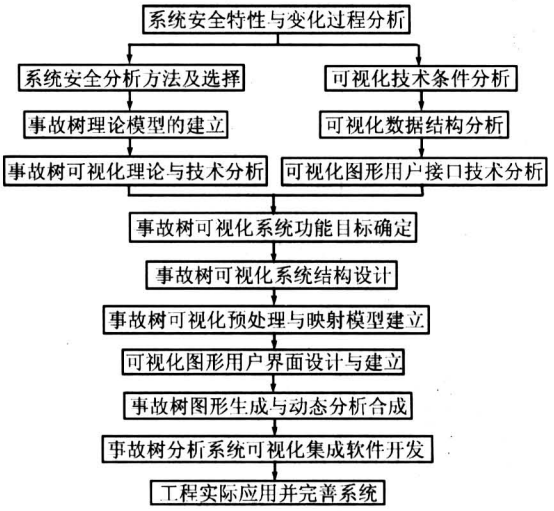

图3 事故树分析可视化系统开发模型

Fig.3 Development model of FTA ViSC system

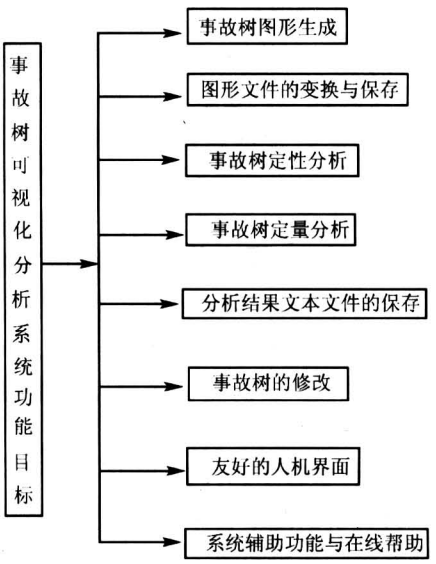

图4 事故树可视化分析系统功能

Fig.4 Function of FTA ViSC system

2) 事故树定性分析 系统应根据记录下的数据，对所绘制的事故树进行最小割集、最小径集、结构重要度的计算。

3) 事故树定量分析 系统应根据用户的数据，自动对所绘制的事故树进行顶上事件的发生概率的计算、概率重要度的分析、危险重要度的分析。

4) 事故树的保存和打开 系统应能够对用户所绘制的事故树进行保存和打开。

5) 事故树的修改 系统应能够对事故树进行修改。

6）*友好的用户界面和完善的在线帮助系统*

系统运行的人机界面必须友好，操作方便，且提供完善的在线帮助系统，以确保用户的高效使用。

5　系统设计简要说明

根据系统分析的结果，按照结构化的系统设计方案，根据图 4 的系统功能目标，系统结构由以下的子系统构成，在主模块的统一协调下实现系统的功能目标。限于篇幅限制，仅对系统的主要子系统设计进行描述。

5.1　事故树绘制子系统

该系统的主要功能是让用户绘制并生成所需的事故树结构。它包括绘制顶上事件、中间事件和基本事件。由于顶上事件和中间事件的绘制有很多相同之处，所以把这两者的绘制做成了一个按钮。当用户第一次点击该按钮时，系统会把该项作为顶上事件，其余的作为中间事件。

一个基本的事故树模型包括顶上事件、中间事件、基本事件、门和直线。因此事故树的绘制应包括这几个方面。通过对事故树的分析可以得出，门是连接在顶上事件或者中间事件之下的，因此在绘制顶上或者中间事件时，用户可以直接选择它所联接的门的种类，而不必去绘制门；同时只要用户指明事故树之间的联系，联线由系统自动生成。

为了能够更好地移动事件，对事件进行修改，响应来自系统的消息，事故树中的元素都是以控件的形式进行显示的，而不是直接在上面绘图。这样会使用户使用更加方便（当然如果用户想保存此图形，也可以把所绘制的事故树保存为图形文件）。所以对于用户绘制事故树不需要算法，只需显示和移动控件的操作。

5.2　事故树定性分析子系统

该系统的主要功能是对事故树进行定性分析，求该事故树的最小割集、最小径集以及结构重要度。

事故树分析中的割集是导致顶上事件发生的基本事件的组合，它是系统发生故障的必要且充分的条件。最小割集是导致顶上事件发生的最起码的基本事件的组合。一个最小割集就是导致顶上事件发生的一条途径，在事故树分析中占有重要地位。

求解方法有：布尔代数化简法、行列式法、结构法、质数法代入法和矩阵法。最小径集的求解是在事故树的对偶树（成功树）基础上进行，按照求解最小割集的算法求解。

基本事件的结构重要度就是根据结构分析确定各个基本事件对顶上事件发生的重要程度。结构重要度分析可以利用最小割集排出结构重要顺序。在求结构重要度之前，应首先要算出事故树的最小割集，所以先应调用上面所讲到的求割集的系统模块。

5.3　事故树定量分析子系统

该系统的主要功能是对事故树进行定量分析，用来求该事故树的顶上事件发生概率、概率重要度以及危险重要度。

定量分析是事故树分析中的重要内容，它可以按照已知的基本事件发生概率，求出顶上事件的发生概率，并将其和目标进行比较。若求出的概率大于目标值，则需要考虑采取措施改善系统的安全性。定量分析还可求算出概率重要系数和危险重要系数，从中可以知道各个基本事件对改进系统安全性所起的作用的大小，以便采取最有效的安全措施。

结构重要度分析是从事故树的结构上分析各基本事件的重要程度。如果进一步考虑基本事件发生概率的变化会给顶上事件发生概率以多大影响，就要分析基本事件的概率重要度。它能使我们知道减少哪个基本事件的发生概率可以有效地降低顶上事件发生的概率。所以它和结构重要度相比，能更真实地反映基本事件的重要程度。基本事件的概率重要是通过基本事件的概率重要系数表示出来的。顶上事件的发生概率 $P(T)$ 是各基本事件发生概率 $P(X_i)$ 的多重线性函数，把 $P(X_i)$ 看作自变量，将 $P(T)$ 分别对各个 $P(X_i)$ 求一次偏导数，即可得该基本事件 X_i 的概率重要系 数。

5.4　事故树的保存和打开子系统

该系统主要用于对用户所绘制的事故树进行保存和打开。为了尽可能满足用户的需求，保存和打开采用了多种文件形式。事故树修改系统能够更方便地为用户提供对事故树进行绘制和分析的功能。

系统应具备保存和打开事故树的功能，这样可以节省用户的大量时间，方便使用。要存储事故树，应该能保存全面反应事故树的信息，所以应定义一个数据结构来存储这些信息。详细的数据结构如表 1。

5.5　界面设计

1）*启动界面*　启动界面应美观大方、有文字说明，同时有显示当时程序进行的进度条。

2）*主界面*　主界面是程序运行的主要界面。主界面上有主菜单、工具栏、绘图区，同时还设有

垂直滚动条和水平滚动条。

表1 事故树可视化信息数据结构表

Table 1 Structure of information data of FTA ViSC

B_Top	是否为顶上事件
B_Mid	是否为中间事件
B_M	是与门还是或门
Behind(M)	该事件下面的事件
Treetop	在屏幕中的高度
Treeleft	距屏幕左边的距离
Index	该事件的编号
Treetag	该事件的代号
Title	该事件的标题
Top	该事件的顶上事件
Tagshow	是否显示该事件的代号

3) 人机界面的设计 从用户的应用需求出发，本系统采用了基于菜单选择、工具栏、对话框等友好的人机交互方式。在屏幕的最上方为主菜单区，显示本系统的主菜单，选择各菜单项后有可能出现相应的二级菜单。菜单的选择有2种：用鼠标单击和直接按菜单右边的热键。左边的工具栏用于绘制事故树和对事故树进行定性和定量分析，是用户使用最频繁的工具。当用户在此工具栏上进行操作时，有一彩色的正方形方块用来标示用户所选择的是哪一项。上方的工具栏是把主菜单中的一些常用的菜单项变成工具栏的形式，能够为用户提供方便。同时，为方便用户操作，系统提供了快捷键。

6 系统运行环境及应用实例

6.1 系统运行环境

该系统应用Visual Basic 6.0[6]语言作为开发平台。基于Visual Basic 6.0对运行环境的要求，并根据大多数用户所拥有计算机硬件设备的实际情况，系统选择Windows98/2000中文版作为系统开发、测试和运行的平台；硬件环境适应486或以上、内存16M以上以及硬盘空间100M以上的各类微型机。

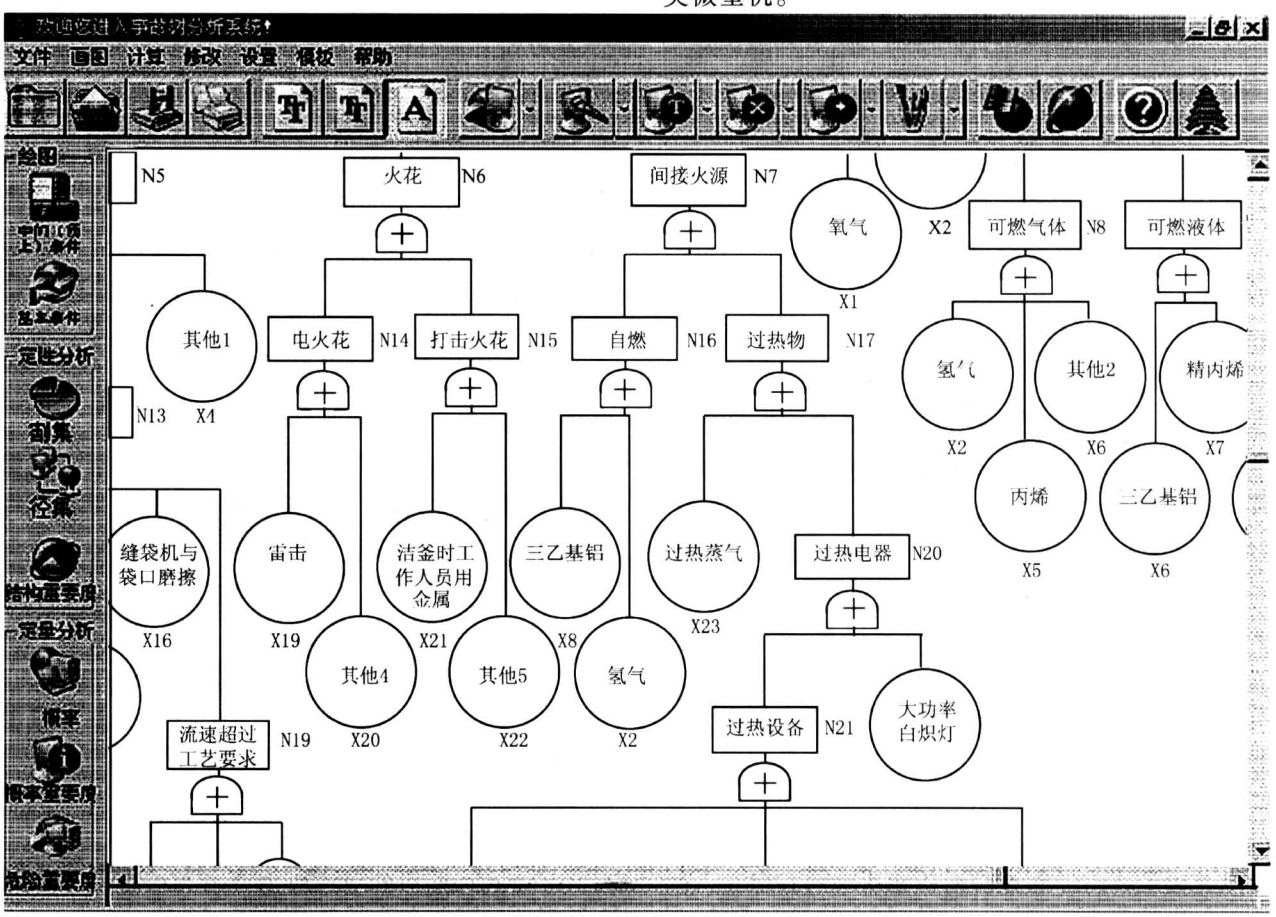

图5 事故树分析系统主界面

Fig.5 Mian windows of FAT system

6.2　系统运行及分析实例

根据系统开发的模型、原则和流程，进行软件程序的开发，并实现了系统的功能目标，并结合某化工企业的爆炸事故进行实际工程分析和应用。图 5 为系统主界面，即系统在可视化集成环境下的运行界面，也是事故树图形生成的主窗口；在图 5 所示窗口内完成事故树图形构造后，根据图 6 所示的选择窗口选择需要分析的项目及其相应的算法（图 7），进行实时分析并获得事故树定性分析结果，即事故树的最小割集（图 8）、最小径集及结构重要度等。由于篇幅所限制，无法对系统运行和分析的所有过程和界面进行说明。

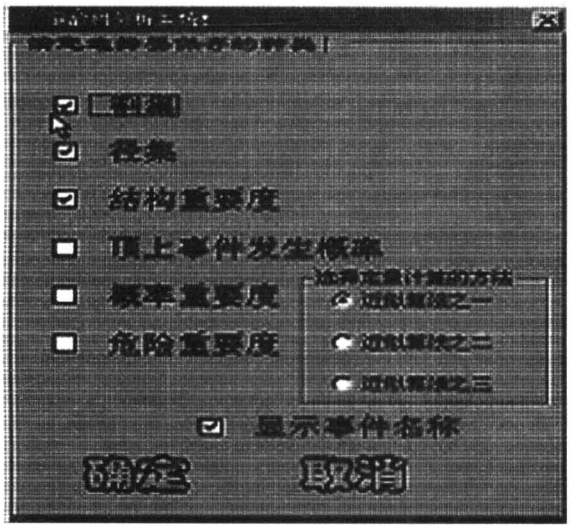

图 6　分析结果保存/选择界面

Fig.6　Saving windows of results

图 7　系统分析算法选择窗口

Fig.7　Select of arithmetic

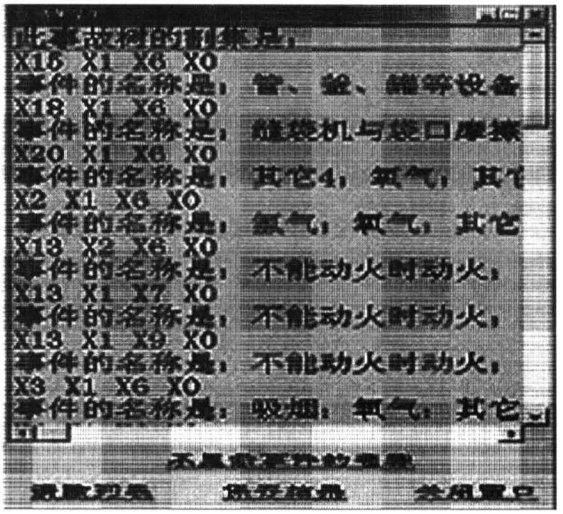

图 8　事故分析结果

Fig.8　Analysis results of FTA

7　结论

1）从系统开发完成后运行及实际应用过程和获得的分析结果来看，系统实现了设计的功能目标，实现了可视化环境下的事故分析和安全性评价，有方便、实用、高效以及准确性高等特点，具有推广应用价值。

2）系统具有较强的实用性。事故树可视化分析系统除了实现传统方法所要求的对事故树进行定性、定量分析功能外，最为关键的是实现了可视化环境下的事故树生成、修改和完善过程，实现图形生成与系统分析的集成功能，大大提供了事故分析的准确性，强化了事故的过程控制，为安全管理、监督部门和企业用户提高了先进的分析技术和手段。

（3）系统在 Windows 环境下开发完成，大部分功能用鼠标即可完成，操作方便，即使不懂计算机的用户也可按提示完成操作。系统还提供了完善的在线帮助功能，用户可以在使用过程中随时获得系统帮助。

参考文献

[1]　施式亮，刘宝琛. 矿井安全非线性动力学评价模型及应用研究 [D]. 长沙：中南大学，2000. 11～45

[2]　武　强，徐　华. 三维地质建模与可视化方法研究 [J]. 中国科学(D 辑)，2004，34 (1)：54～60

[3]　唐泽圣，孙延奎. 科学计算可视化理论与应用研究进展 [J]，清华大学学报，2001，41 (4)：199～202

[4]　唐泽胜. 三维数据场可视化 [M]. 北京：清华大学出版社，1999. 1～14

[5] 肖贵平，侯福均. 计算机辅助事故树分析中的图形输入法 [J]. 中国安全科学学报，2001，11 (4)：53～56

[6] 曹 青. Visual Basic6.0 程序设计教程 [M]. 北京：机械工业出版社，2002. 10～116

Development and Application of Fault Tree Ananlysis System Based on Visualization

Shi Shiliang Lu Bentao

(*Energy & Safety School Hunan University of Science and Technology, Xiangtan, Hunan* 411201, *China*)

[**Abstract**] The Fault Tree Analysis (FTA) is one of the most important methods in the safety system engineering. With FTA, the fatalness of the various kinds of system can be distinguished and evaluated, not only the direct causes of the accidents but also the potential causes can be deeply opened out. The consequences of accidents described with FTA are intuitional, intelligible, clear thingking and logical. The FTA can finish the qualitative analysis and the quantitative analysis. In this paper, the model of the Fault Tree visulization system is established based on the theory and technology of the visulization, the system functions are determined, the design of the system structure is finished and the FTA visulization system is developed. Furthermore, the integrated analysis environment that conbines the Fault Tree graph creation and Fault Tree dynamic analysis is constructed based on computer. The FTA visualization analysis system supplies high efficiency and correct technology and measures for accidents analysis and safely assessment.

[**Key words**] safety technology and engineering; safety assessment; FTA; visualization; analysis system

(cont. form p. 65)

Ignition of Diesel by Heated Surface

Li Yuanlong, Lu Shouxiang, Fan Weicheng

(*State Key Laboratory of Fire Science, University of Science and Technology of China, Hefei* 230027, *China*)

[**Abstract**] The ignition of leaked fuel of the diesel engine is studied experimentally. The critical ignition temperature is calculated statistically. The difference between the ignition temperature and auto－ignition temperature of diesel is much less than that of other fuels. The ignition mode is also much different from its counterpart. The paper describes the detailed boiling mode of the leaked fuel on a hot surface. The equation to get the mass flux of the fuel vapor is given.

[**Key words**] hot surface; ignition test; boiling