

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 12/24 (2006.01)

H04L 12/26 (2006.01)



[12] 发明专利说明书

专利号 ZL 01804602.9

[45] 授权公告日 2008 年 12 月 10 日

[11] 授权公告号 CN 100442700C

[22] 申请日 2001.2.2 [21] 申请号 01804602.9

[30] 优先权

[32] 2000. 2. 8 [33] US [31] 09/500,101

[86] 国际申请 PCT/US2001/003436 2001.2.2

[87] 国际公布 WO2001/059989 英 2001.8.16

[85] 进入国家阶段日期 2002.8.6

[73] 专利权人 哈里公司

地址 美国佛罗里达

[72] 发明人 凯文·弗克斯 隆达·汉宁

约翰·法莱尔 克里弗德·米勒

[56] 参考文献

the n - etwork vulnerability tool nvt a syst - em vulnerability visualization architectur - e. henning r foxk. proceedings of 22n. d national inform. ation systems secu. rity conference, Vol. 1 . 1999

审查员 孙玉芳

[74] 专利代理机构 中国国际贸易促进委员会专利
商标事务所

代理人 付建军

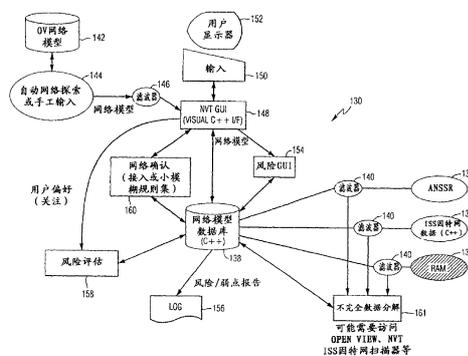
权利要求书 3 页 说明书 23 页 附图 14 页

[54] 发明名称

评估网络安全姿态并具有图形用户界面的系统

[57] 摘要

某个图形用户界面包含在计算机屏幕上，并用于确定网络的弱点姿态。 某个系统设计窗口显示某个网络图的网络图标，它们代表网络中包含的不同网络单元。 对应于网络中网络单元相互连接的方式，把各个网络图标连接起来。 网络的弱点姿态已经确定之后，该网络图中选定的部分变为不同的颜色，以表明该部分已经确定的弱点。



1. 一种包含图形用户界面的计算机系统，所述图形用户界面包含在计算机屏幕上并且用于确定网络安全姿态，所述图形用户界面进一步包括：

系统设计窗口，用于显示网络图的网络图标，所述网络图标代表网络中包含的不同网络单元，其中，把各个网络图标连接起来的方式对应于网络中网络单元相互连接的方式；

其中，在网络的安全姿态已经确定之后，该网络图中选定的部分变为不同的颜色，以表明该部分已经确定的弱点，

其中，网络的安全姿态是通过下列步骤确定的：

由完全不同的网络弱点分析程序产生一个系统对象模型数据库，它以对象/类层次表示和存放网络系统描述，因此该系统对象模型数据库支持完全不同的网络弱点分析程序的信息数据需求；

把系统对象模型数据库与完全不同的网络弱点分析程序使用面向目标的模糊逻辑判断规则获得的数据结果相关联，这些规则通过模糊推论网络规则和模糊证据推理规则而执行；

形成推论网络作为试探法规则的一个层次，它能够使用先验概率的专家知识传播概率，使得低级别的离散概率反映在高级别的网络弱点结论中；以及

弱点姿态窗口，显示用户可读的项目，表明脆弱的网络单元。

2. 根据权利要求1的计算机系统，其特征在于，对应的网络单元变为不同的颜色，表明脆弱的网络节点。

3. 根据权利要求1的计算机系统，其特征在于，所述图形用户界面进一步包括管理器窗口，所述管理器窗口用于显示网络单元的性质。

4. 根据权利要求1的计算机系统，其特征在于，所述图形用户界面进一步包括数据敏感度框，所述数据敏感度框具有用户选定的项目，以选择网络单元的敏感度。

5. 根据权利要求1的计算机系统，其特征在于，所述图形用户界

面进一步包括选择节点配置编辑框，所述选择节点配置编辑框含有用户可选择的弱点特征，以便选择网络节点的一种弱点特征。

6. 根据权利要求1的计算机系统，其特征在于，用变为不同颜色的箭头把图标连接在一起，以表明在网络单元之间存在着脆弱的连接。

7. 一种包含图形用户界面的计算机系统，所述图形用户界面包含在计算机屏幕上并且用于确定网络安全姿态，所述图形用户界面进一步包括：

系统设计窗口，用于显示网络图的网络图标，所述网络图标代表网络中包含的不同网络节点，其中，把各个图标连接起来的方式对应于网络中网络节点相互连接的方式；

管理器窗口，在其中显示和编辑网络节点的对应性质；

其中，在网络的安全姿态已经确定之后，选定的图标变为红色表明较高风险的节点，选定的图标变为黄色表明风险不太严重的节点，

其中，网络的安全姿态是通过下列步骤确定的：

由完全不同的网络弱点分析程序产生一个系统对象模型数据库，它以对象/类层次表示和存放网络系统描述，因此该系统对象模型数据库支持完全不同的网络弱点分析程序的信息数据需求；

把系统对象模型数据库与完全不同的网络弱点分析程序使用面向目标的模糊逻辑判断规则获得的数据结果相关联，这些规则通过模糊推论网络规则和模糊证据推理规则而执行；

形成推论网络作为试探法规则的一个层次，它能够使用先验概率的专家知识传播概率，使得低级别的离散概率反映在高级别的网络弱点结论中。

8. 根据权利要求7的计算机系统，其特征在于，管理器窗口进一步包括一个节点性质显示框，以便在网络设计选择时编辑网络节点的性质。

9. 根据权利要求7的计算机系统，其特征在于，所述图形用户界面进一步包括数据敏感度框，所述数据敏感度框具有用户选定的项目，以选择网络节点的敏感度。

10. 根据权利要求 7 的计算机系统，其特征在于，所述图形用户界面进一步包括选择节点配置编辑框，所述选择节点配置编辑框含有用户可选择的弱点特征，以便选择对应节点的一种弱点。

评估网络安全姿态并具有图形用户界面的系统

技术领域

本发明涉及网络领域，更确切地说，本发明涉及评估网络安全弱点的领域。

背景技术

当前正在开发的信息系统和计算机网络基础设施，建设时考虑了是什么构成了可接受的风险（或者适当的保护）。系统资产，比如计算机网络的硬件、软件和系统节点，必须受到与其价值相应程度的保护。另外，这些资产在失去其价值之前，都必须受到保护。在所处理数据的整个使用期限内，任何安全特性和系统体系结构也应当提供充分的保护。为了评估与网络相关联的任何风险是否可接受，安全工程师通常收集所有有关的信息，然后分析与网络相关联的风险。

风险分析是复杂和耗时的过程，它需要确定在网络中的暴露风险及其潜在的危害。例如，分析计算机网络中的安全风险时，安全工程通常遵循下列步骤：

1) 确认整个计算机系统的资产。

2) 确认资产的弱点。本步骤通常需要想象力，以预测对本资产会发生什么损害，来自何方。计算机安全的三个基本目标是确保保密、完整和可用。所谓弱点是可能导致失去这三种品质之一的任何情况。

3) 预测发生（利用）的可能性，也就是确定每次发生被利用有多么频繁。发生的可能性涉及现有控制的严格和某人或某物将会侵入现有控制的可能性。

4) 通过确定每次事故的预期成本，计算每年中任何显现的成本（预期年损失）。

5) 测定可应用的控制及其成本。

6) 计划控制的年节省额。

分析的最后一步是一种成本-效益分析，也就是，是实行一种控制的成本更低，还是接受损失的预期成本的成本更低？风险分析得出安全计划，它确定特定措施的责任以改善安全性。

今天，技术的飞速发展和功能日益增强的计算机的普及，为了得到低成本高效率的解决方案，必须使用现成商品(COTS: commercial-off-the-shelf)硬件和软件组件。对COTS的这种强烈的依赖性意味着，对大多数应用程序来说，商业等级的安全机制是充分的。所以，对于COTS组件相对较弱的组件，必须构筑安全体系结构，以建立有效的、任务关键的计算机系统。保险度较高的组件可以置于公共区或者说信息边界，形成基于飞地的安全体系结构，对信息保险实行彻底防御的措施。

系统建筑师可以利用某些设计工具，也就是软件程序，以协助使可用的保护机制最大化，同时保持不超出开发预算。当前一代的风险分析工具通常是单一卖主的解决方案，它只涉及风险的某个特定方面或者某些方面。这些工具往往属于以下三个范畴之一：

1) 根据数据库中明确指出的弱点进行工作并可能修复已知弱点的工具。对于数据库更新，这种类型的工具是卖主决定的，或者通过新的产品版本，或者通过预约服务。这个范畴中的实例包括ISS的因特网扫描器、Network Associates, Inc.的CyberCop和Harris的STAT。

2) 使用多种参数来计算风险指示器的单片工具。这些工具难以维护并很难与快速发展的威胁和技术环境保持最新。这个工具范畴的实例是Los Alamos Vulnerability Assessment (LAVA)工具。

3) 考察系统某个特定方面的工具，比如操作系统或数据库管理系统，而忽略其它系统部件。例如，SATAN分析操作系统弱点，但是忽略基础设施部件比如路由器。

为了单一的计算机网络分析而使用不同卖主的多种工具，是一项劳动密集型的任务。通常，安全工程师将不得不以多种格式多次输入系统（网络）的描述或者说表达。接着，对这些多种工具的结果输出，安全工程师必须手工分析、整理并汇总成网络安全姿态的单一报告。然

后,安全工程师可以完成风险分析(计算预期年损失、测定控制等等),并且接着重复该过程,分析另外的安全风险、系统性能、任务功能和开发预算。

同样,这些工具中,没有一种对系统使用“钻下”的集合“快照”方式或者说分层方式,以便于应付系统中多个层次(网络、平台、数据库等等)上的风险。在分析另外的安全风险、系统性能和任务功能时,这些工具对系统设计者没有提供多少帮助。却是提供了某个“风险解决方案”,它涉及给定工具设计来计算的风险的某个特定方面。为了开发综合的风险评估,安全工程师将不得不变得精通若干工具的使用并手动关联最终的输出。

第 22 届全国信息系统安全会议的会议论文集 1999, Vol.1, col.18-21, 97-111 页发表的会议论文 XP-001031508 公开了一种网络弱点工具(NVT)的概念,它应用了单一拓扑系统模型,该模型支持使用集成的知识引导和转化框架的多个弱点分析工具的信息需要。该系统导致了一种弱点/风险评估。这篇论文介绍了 NVT 的体系结构并且在有限的基础上讨论了使用模糊函数来映射某个已有的网络和形成一种内聚的弱点/风险评估。

这篇论文也公开了一种系统的图形网络图,它可以用颜色代码以不同的颜色来显示不同的风险。

US-A-5684957 公开了一种网络管理系统的分析,并且显示了网络中探测到的一个安全漏洞。

成功的风险分析的一个方面是完全和准确的数据累加,以产生分析工具所用的系统模型。许多目前的风险分析工具依赖用户、系统操作人员和分析师填写的测定结果,以采集数据,用于分析中所用系统模型的开发。另外,某个工具能够主动地扫描计算机网络,以测试系统组件的多种弱点。

然而,这些方法有缺点。文本的或者说基于测定结果的知识引导技术是劳动密集型的,对于分析师可能是繁重乏味的。许多现有的工具重复使用相同的信息来分析系统安全的不同方面。使用模型数据的

集中知识库会更加有利，它能够提供一个基础，为现有工具共享输入。这个知识库可以用于产生风险分析工具所用的数据集，使多个工具能够对同一个系统运行而不必分别进行输入，从而降低了操作员错误的可能性。使用多个风险分析推理引擎，或者说向后曲身，会使该系统的多个方面受到分析，而不必花费成本来开发一个工具进行所有类型的分析。通过使用多个工具，集成已有的信息和已知的评估结果，将对系统的安全姿态产生更加稳健和准确的描述。这些结果能够便利更多的已知系统设计中的决定，为其它的评价和比较提供框架。

发明内容

所以，本发明的一个目的是提供一种数据处理系统和方法，用于评估网络的安全弱点，而不必多次分析该网络。

根据本发明的第一方面，提供了一种包含图形用户界面的计算机系统，所述图形用户界面包含在计算机屏幕上并且用于确定网络安全姿态，所述图形用户界面进一步包括：系统设计窗口，用于显示某个网络图的网络图标，它们代表网络中包含的不同网络单元，其中，把各个网络图标连接起来的方式对应于网络中网络单元相互连接的方式；其中，在网络的安全姿态已经确定之后，该网络图中选定的部分变为不同的颜色，以表明该部分已经确定的弱点，其中，网络的安全姿态是通过下列步骤确定的：由完全不同的网络弱点分析程序产生一个系统对象模型数据库，它以对象/类层次表示和存放网络系统描述，因此该系统对象模型数据库支持完全不同的网络弱点分析程序的信息数据需求；把系统对象模型数据库与完全不同的网络弱点分析程序使用面向目标的模糊逻辑判断规则获得的数据结果相关联，这些规则通过模糊推论网络规则和模糊证据推理规则而执行；形成推论网络作为试探法规则的一个层次，它能够使用先验概率的专家知识传播概率，使得低级别的离散概率反映在高级别的网络弱点结论中；以及某个弱点姿态窗口，显示用户可读的项目，表明脆弱的网络单元。

根据本发明的第二方面，提供了一种图形用户界面，包含在计算机屏幕上并且用于确定网络安全姿态，包括：系统设计窗口，用于显

示某个网络图的网络图标，它们代表网络中包含的不同网络节点，其中，把各个图标连接起来的方式对应于网络中网络节点相互连接的方式；某个管理器窗口，在其中显示和编辑网络节点的对应性质；其中，在网络的安全姿态已经确定之后，选定的图标变为红色表明较高风险的节点，选定的图标变为黄色表明风险不太严重的节点，其中，网络的安全姿态是通过下列步骤确定的：由完全不同的网络弱点分析程序产生一个系统对象模型数据库，它以对象/类层次表示和存放网络系统描述，因此该系统对象模型数据库支持完全不同的网络弱点分析程序的信息数据需求；把系统对象模型数据库与完全不同的网络弱点分析程序使用面向目标的模糊逻辑判断规则获得的数据结果相关联，这些规则通过模糊推论网络规则和模糊证据推理规则而执行；形成推论网络作为试探法规则的一个层次，它能够使用先验概率的专家知识传播概率，使得低级别的离散概率反映在高级别的网络弱点结论中。

根据本发明的第三方面，提供了一种包含图形用户界面的计算机系统，所述图形用户界面包含在计算机屏幕上并且用于确定网络安全姿态的，所述图形用户界面进一步包括：系统设计窗口，用于显示某个网络图的网络图标，它们代表网络中包含的不同网络单元，其中，把各个网络图标连接起来的方式对应于网络中网络单元相互连接的方式，其中，在网络的安全姿态已经确定之后，该网络图中选定的部分变为不同的颜色，以表明该部分已经确定的弱点；其中，网络的安全姿态是通过下列步骤确定的：由完全不同的网络弱点分析程序产生一个系统对象模型数据库，它以对象/类层次表示和存放网络系统描述，因此该系统对象模型数据库支持完全不同的网络弱点分析程序的信息数据需求；把系统对象模型数据库与完全不同的网络弱点分析程序使用面向目标的模糊逻辑判断规则获得的数据结果相关联，这些规则通过模糊推论网络规则和模糊证据推理规则而执行；形成推论网络作为试探法规则的一个层次，它能够使用先验概率的专家知识传播概率，使得低级别的离散概率反映在高级别的网络弱点结论中；以及某个弱点姿态窗口，显示用户可读的项目，表明脆弱的网络单元。

根据本发明的第四方面，提供了一种图形用户界面，包含在计算机屏幕上并且用于确定网络安全姿态，包括：系统设计窗口，用于显示某个网络图的网络图标，它们代表网络中包含的不同网络节点，其特征在于，把各个图标连接起来的方式对应于网络中网络节点相互连接的方式；某个管理器窗口，在其中显示和编辑网络节点的对应性质；其中，在网络的安全姿态已经确定之后，选定的图标变为红色表明较高风险的节点，选定的图标变为黄色表明风险不太严重的节点；其中，网络的安全姿态是通过下列步骤确定的：由完全不同的网络弱点分析程序产生一个系统对象模型数据库，它以对象/类层次表示和存放网络系统描述，因此该系统对象模型数据库支持完全不同的网络弱点分析程序的信息数据需求；把系统对象模型数据库与完全不同的网络弱点分析程序使用面向目标的模糊逻辑判断规则获得的数据结果相关联，这些规则通过模糊推论网络规则和模糊证据推理规则而执行；形成推论网络作为试探法规则的一个层次，它能够使用先验概率的专家知识传播概率，使得低级别的离散概率反映在高级别的网络弱点结论中；以及某个弱点姿态窗口，显示用户可读的项目，表明脆弱的网络图标。

某个图形用户界面包含在计算机屏幕上，并用于确定网络的弱点姿态。某个系统设计窗口显示某个网络图的网络图标，它们代表网络中包含的不同网络单元。对应于网络中网络单元相互连接的方式，把各个网络图标连接起来。网络的弱点姿态已经确定之后，该网络图中选定的部分变为不同的颜色，以表明该部分已经确定的弱点。

在本发明的又一方面，对应的网络单元确定不同的颜色，表明某个脆弱的网络单元。图形用户界面也可以包括某个管理器窗口，以便显示网络单元的性质。某个数据敏感度框能够具有用户选定的项目，以选择网络单元的敏感度。图形用户界面也可以包括一个选择节点配置编辑框，它含有用户可选择的弱点特征，以便选择网络节点的一种弱点特征。可以用变为某个不同颜色的箭头把图标连接在一起，以表明在这些网络单元之间存在着脆弱的连接。

在本发明的又一方面，某个图形用户界面包含在计算机屏幕上，

并用于确定网络的弱点姿态。它包括某个系统设计窗口，以显示某个网络图的图标，它们代表网络中包含的不同网络节点。对应于网络中网络节点相互连接的方式，把各个网络图标连接起来。可以包括某个管理器窗口，可以显示和编辑网络节点的对应性质。网络的弱点姿态已经确定之后，选定的图标变为红色表明较高风险的节点，选定的图标变为黄色表明风险不太严重的节点。

管理器窗口进一步包括一个节点性质对话框，以便在网络设计选择时编辑网络节点的性质。图形用户界面也可以包括一个数据敏感度框，它具有用户选定的项目，以选择网络节点的敏感度。一个选择节点配置编辑框可以含有用户可选择的弱点特征，以便选择对应节点的一种弱点。

在本发明的又一方面，弱点姿态窗口可以显示用户可读的项目，表明脆弱的网络单元。这些用户可读的项目可以包括一张图，表明脆弱的网络单元，还可以包括电子表格，表明脆弱的网络单元。

附图说明

现在，以举例说明的方式，参考下列附图来介绍本发明：

图 1 是网络的一个示意框图，显示网络中常常发现问题的部位。

图 2 是网络的另一个示意框图，显示一个确定的弱点，由本发明的系统和方法定位。

图 3 是另一个框图，显示本发明之系统和方法的整个体系结构，并显示与网络某些数据库联用的滤波器。

图 4 是本发明之体系结构的另一个示意框图，显示模糊逻辑分析。

图 5 是另一个示意框图，显示本发明之数据处理系统和方法的高级别体系结构组件。

图 6 是本发明之数据处理系统的另一个高级别示意框图。

图 7 是图形用户界面的一个实例，它模拟网络为一幅图。

图 8A 和图 8B 显示打开的窗口，它们提供系统对象模型数据库建立时的数据设定。

图 9 是图形用户界面的一个实例，显示网络模型。

图 10 是一个图形用户界面，显示对网络安全姿态的多种报告选项。

图 11 是一个框图，显示本发明之数据处理系统和方法中所用的、面向目标的模糊逻辑处理的基本处理组件。

图 12 是本发明之数据处理系统和方法中所用的数据汇合的一个示意框图。

图 13 是另一个示意框图，显示本发明之数据处理系统和方法中所用的、基于目标的汇合规则。

图 14 是另一个框图，显示本发明之数据处理系统和方法的模糊逻辑处理中所用的基本处理步骤和组件。

图 15 是一个框图，显示缺陷树分析 (DPL-f) 的基本组件，用于证据累加和模糊证据推理的规则。

图 16 是一个框图，显示目标/类层次。

图 17 是一个框图，显示本发明的系统类图。

具体实施方式

图 1 展示了一个实例，常规网络 100 具有内部服务器 102，它们连接到外部路由器 104、通讯网络 105 和防火墙 106。内部路由器 108 连接到防火墙 106、分支部门 107，并连接到内部 LAN 网络组件 110 和远程访问服务器 112 和远程用户 114。

使用图 1 的实例，网络中经常发现的问题包括：宿主，比如内部服务器 102 运行不必要的服务，例如拒绝服务和匿名 FTP，或者误配置的网络服务器可能是某个内部服务器，例如 CGI 脚本、匿名 FTP 和 SMTP。内部 LAN 110 可能包括未打补丁的、过期的、脆弱的或者默认配置的软件和固件和薄弱的密码。LAN 也可能包括不适当输出的文件共享服务，比如 NetWare 文件服务和 NetBIOS。内部 LAN 110 也可能包括误配置的或者未打补丁的 Windows NT 服务器，以及缺少综合的策略、步骤、标准和方针而导致的问题。远程访问服务器 112 可能含有不安全的远程访问点，外部路由器 104 可能含有通过服务的信息泄漏，比如 SNMP、SMIP、指针、roosers、SYSTAT、NETSTAT、TELNET 标题、Windows NT TCP 139 SMB (服务器消息块) 和向未

命名服务器主机的区域传递。它也可能含有不适当的日志记录、监视和探测能力。分支部门 107 可能含有盗用的信任关系，比如 RLOGIN、RSH 或者 REXEC。防火墙 106 可能被误配置或者含有误配置的路由器访问控制列表。

尽管这些网络问题仅仅是网络 100 中发现的常见问题的一个实例，还有许多其它问题可能发生，正如本领域的技术人员所周知。

本发明是有益的，因为本发明的系统和方法使网络系统中的弱点能够得到确认。数据处理系统和方法的软件可以放置在某个用户终端 120 上，如图 2 所示，显示出内部 LAN 110 连接的节点 122 的某个确认的弱点。鉴于介绍的目的，本发明的数据处理系统和方法可以称为网络弱点工具 (NVT)，也就是，用户用来确定网络弱点和风险的工具。

形成本发明的 NVT 的数据处理系统可以加载到运行着 Windows NT 的奔腾 PC 平台上。这种类型的平台可以提供低成本的解决方案，并且支持很多种评估工具，在本说明书中也通常称为网络弱点评估或风险分析程序。这些网络弱点分析程序往往是安全工程师熟知的标准 COTS/GOTS 程序，并且包括 HP Open View，它能够实现网络自动探索或者手工网络模拟；Mitre 公司制作的 ANSSR (Analysis of Network System Security Risks: 网络系统安全风险的分析)——一种 GOTS 网络系统分析工具，能够进行被动数据采集和单次损失评估。NSA 的风险评估方法通称为 RAM (risk assessment model: 风险评估模型)，也可以用于 DPL-f 判断支持编程语言中，并且已经实现。RAM 也能够为事件树逻辑进行被动数据采集，对任务列表分配优先级，并且能够建立多重风险/服务的数学模型。

DPL (decision programming language: 判断编程语言) 是一种判断支持软件包，它便利复杂判断的模拟。它允许用户在判断过程中加入不确定性和灵活性。DPL 为建立模型提供了图形界面，并且执行对该模型的多种分析。DPL-f 包含 DPL 内建的功能，并且为构建缺陷树提供图形界面。这个特性允许模拟者产生缺陷树并把它们加入 DPL

模型中。DPL-f 也包含独特的分析工具。这些工具的能力包括明确地计算该树中任何事件的概率以及执行缺陷树特定类型的敏感度分析。DPL-f 为模型中加入时间序列提供了界面。这就允许模拟者解释贬值、资本增长或者其它时变量而不必改变模型的结构。DPL-f 提供带有附加功能的 RAM，便于快速缺陷树构建、嵌入式缺陷树的库、专家判断生成系统、割集的枚举和排序以及不同时间风险的图形描绘。

因特网安全系统公司 (ISS) 开发的 ISS 因特网扫描器能够进行主动数据采集，扫描网络中的主机、服务器防火墙和路由器，并评估网络、操作系统和软件应用程序的安全性和策略一致性。它允许随时快照和计算机网络一致性报告。这些程序是完全不同的网络弱点分析程序，本发明的 NVT 能够进行集成。

本发明的 NVT 是基于一种知识引导框架，它加入了网络布局的图形描述。这种布局用于获取网络属性，随后受到分析以确定安全弱点。

依据本发明 NVT 的系统和方法自动映射已有的网络，并且能够在图形用户界面上把已有的网络显示为一个模型，比如图 7 中所示的。例如，HP Open View 能够以图形方式描绘网络布局。一旦该软件获得了该网络的默认路由器的 IP 地址，本发明的 NVT 就能够使用 Open View 并搜索与该网络连接的计算机和其它设备。NVT 在网络上 ping 可能的 IP 地址，并且向其网络图加入它收到的不论什么响应信息，从而执行主动搜索。NVT 也提供了手工的方法，利用图形用户界面来画出提议的网络。如图所示，该图形用户界面支持拖放。可以定义系统的体系结构，包括对于其它设计或者节点编辑是决定性的安全信息，以提供完整逻辑网络规划所需的附加细节。用户也可以在图上使用某个子网图标来表示整个网络。

网络系统的描述完成之后，本发明的 NVT 在目标/类层次中表示和存放该描述，如图 16 和图 17 中的实例所示，下面将要解释。单个的拓扑系统对象模型支持完全不同的网络弱点分析程序（工具）的信息数据需求。结果的模糊逻辑处理使这些程序的结果能够进行相关处理，成为内聚的弱点/风险评估结果，以获得该网络的弱点姿态，如图

10 的图形用户界面中所示。该系统的这种单一表达简化了多种工具的使用，消除了重复的数据输入。它也提供了一种基础，使给定的弱点评估工具能够应付数据不完全的问题，同时也可以用于将来的知识交流。

图 3 在 130 中展示了本发明的整个网络弱点工具 (NVT) 和数据处理系统的一个实例，其中三个网络弱点分析程序 (工具) 展示为 ANSSR 132、ISS 网络扫描器 134 和 RAM 136。本发明的系统和方法产生了一个系统对象模型数据库 (网络模型 DB) 138，它表示一个网络并且支持网络弱点分析程序的信息数据需求。系统对象模型数据库 138 表示受评估系统或设计的单一表达，并应付一个网络的单一内部表达的需要，为网络弱点分析程序提供数据。

这个模型 138 使用面向目标 (OO) 的方法在类层次中提供可扩充的组件集，其组合可以表示一个网络。类层次提供一种方法来定义共享公共特性的组件，同时保留它有别于其它组件的特点。除了隐含的层次关系之外，面向目标的技术提供了一种包含机制，其中一个目标能够包含对任何目标的引用，包括它自己。这就提供了一种灵活的机制来表示任何实质的或者逻辑的实体。同时，面向目标的表达使它自己便于修改和扩充，对于每天都有变化和新技术的信息保险领域是非常理想的。

如图 3 所示，滤波器 140 与网络弱点分析程序 132、134、136 中的每一个相关联，只允许对应的网络弱点程序需要的数据输出到该工具 (程序)。这些滤波器是一个 C++ 的基类，它提供了一组虚方法，允许数据在 NVT 系统和一个程序之间移动。该滤波器也提供了一种方法，使 NVT 控制工具的执行以及完成工具需要的数据。NVT 把每个工具看作一个滤波器，调用滤波器内部适当的方法来执行所需的任务，包括初始化、运行、输入数据和输出数据。每个工具可以有具体的滤波器子类，为该工具提供具体定义每种方法的方式，同时仍然提供对 NVT 的通用的和明确定义的编程接口 (API)。这就允许在 NVT 之内对所有工具同样对待，使工具的增加和去除不影响任何已有的

NVT 节点。

使用滤波器技术在 DPL-f 和 NVT 之间建立通讯是直接了当的。分配给一个 DPL-f 滤波器的任务是建立和填充缺陷树的具体任务。作为分析工具，缺陷树能够把网络中的一个节点表示为显现的，并对某些事件提供一个概率值，比如拒绝服务、数据损失和数据损害。实际上，DPL-f 能够用作最终结果工具。

然后，用每个网络弱点分析程序来分析网络，以产生每个程序的数据结果。这些数据结果进行相关，以确定该网络的安全姿态。通过本发明的模糊逻辑处理能够进行网络确认，如下所述，系统 GUI 可以输入到用户显示器中。

通过自动网络探索或者手工输入 144，比如通过 HP Oper View，把网络概述为模型 142，适当的滤波器 146 允许系统 GUI 148 通过适当的数据输入在用户显示器上显示该网络模型，如图 7 所示。也可以使风险 GUI 154 直观地评估风险弱点、风险/弱点报告的日志记录 156、风险评估 158，作为 GUI 148 的部分，所有这些全都通过网络确认 160，使用接入或者模糊规则集，见下文更为详细的介绍。任何数据不完全的决定 161 都可以应付。

图 4 展示了与图 3 类似的一个高级别框图，显示系统对象模型数据库 138，它建立后可以与集成的应用程序编程接口 162 协同工作，允许把数据输入到多个工具 164 中，它们被展示为一个模型工具、探索工具和若干信息分析工具，形成整个系统结果数据库 166。应用程序编程接口 168 和图形用户界面 170 与模型数据库 138 协同工作。评价/评估管理器 172（管理者）与应用程序编程接口（API）174 和图形用户界面（GUI）176 协同工作，利用模糊逻辑处理对数据结果进行相关，模糊逻辑处理以虚线 178 标出，包括专家相关 180 和模糊推论和证据推理 182，以产生弱点结果 184 和图形用户界面（GUI）186 作为相关结果。尽管图 4 表示了显示不同组件实例的、高级别的模型，它仅仅是本发明的 NVT 系统和方法可以使用的高级别组件的一个类型的一个实例。

图 5 和图 6 展示了高级别模型的其它实例，显示了数据源 200(图 5)的基本成分和处理步骤，以及系统描述 202、单工具分析 204、多工具分析 206、工具至专家分析 208 和报告介质 210。工具至专家分析 208 可能包括 DPL-f 208a 作为数据事实库中模糊逻辑处理的一部分，以及使用 CERT 记号 208b 和专家系统 208c 作为专家相关。产生的报告输出可以包括图形用户界面上的图标、文本、EXCEL 电子表格、Access 文件和配置，如本领域的技术人员所周知。图 6 也展示了与图 5 类似的另一个高级别的模型，其中形成完整的系统对象模型和模糊逻辑处理所用的工具可能包括单工具处理和多工具相关。

图 7 至图 10 以更为详细的程度展示了图形用户界面 220，它能够包含在计算机屏幕上，并用于交互操作 NVT 和确定网络的弱点姿态。如图所示，图形用户界面 220 是一个标准型的 Windows™ 界面。系统设计窗口 222 容许网络图标 224 的显示，以形成一个网络图，该图表示了网络中包含的不同网络单元和节点之间的关系。对应于网络中网络单元节点相互连接的方式，把各个网络图标 224 连接起来。如图 7 所示，网络单元可以通过连接线 226 连接起来，该连接线表示实际网络单元和节点之间存在的相互连接。系统设计窗口 222 在左边显示了网络之间的一张图 230，有两个节点，在窗口的右边显示了一张网络图 232，展示了该网络模型的一张图。管理器窗口 234 是打开的，并且显示了网络单元的性质。

对于选定的网络单元，选择数据敏感度弹出窗口(框) 240 是用户通过菜单选项可选择的(图 8A)，并且具有用户选定的项目，以选择网络单元的敏感度。任何节点(图 8A 所示的实例中为节点 1)上数据的敏感度都可以利用适当的确认、随机和默认按钮选定为不分类、敏感、秘密、机密、绝密或者最高机密。

选定节点配置编辑弹出窗口(框) 250 显示在图 8B 中，可以含有用户可选择的弱点特征，以便选择网络单元或节点的一种弱点特征。图 9 也显示了带有中心集线器和相互连接节点的网络模型图。用户可以编辑管理器窗口 234 中的条目，它也允许通过适当的按钮选择，实

现网络探索。自然，可以根据需要选择和移动网络图标，以编辑和设计可选项。

在系统中的安全姿态建立之后，表示高风险网络单元，如集线器 252 的图标可以改变颜色，比如红色。其它选定的图标可以变为黄色，指明风险不太严重的节点，比如图 7 和图 9 中所示的 HP4 节点 254。围绕着网络的这些节点或部位的共享区域，颜色可以设定为红色或者黄色，以指明风险较高的弱点。连接线也可以变为红色或者黄色以指明单元之间的不良连接。

图 10 展示了弱点姿态窗口 270，以显示用户可读的图标，这些图标指明脆弱的网络单元和图标。整个系统模型显示为打开的系统设计窗口的一部分。另外，还展示了电子表格 272 和 NVT 风险评估图 274，后者有用于风险评估的滑动杆。还展示了风险分析窗口 276，显示了五个风险分析最高的单元。

图 16 以更为详细的程度显示了类层次，其中有类名 280（带有若干公有属性和若干私有属性）、聚合 282 和利用推广 290 的、源 286 和目标 288 的关联。图 17 展示了系统类示意图的一个实例，在框中标识了多种组件。自然，图 17 仅仅是本领域的技术人员熟知的系统类示意图，仅仅是本发明的系统和方法能够使用的一个实例。

现在以更为详细的程度参考图 11 至图 15，其中展示了面向目标的模糊逻辑判断的过程。如图 11 所示，使用某个应用程序编程接口和专家相关，把系统模型数据库 138 和各个网络弱点分析程序的结果 300 结合起来，通过数据模糊化，形成数据事实库 302。通过模糊推论网络规则 304 和模糊证据推理规则 306 执行面向目标的逻辑判断规则，根据预定的目标 308 确定网络的安全姿态。

本发明的模糊逻辑处理使用数据汇合、证据推理和推论网络技术。正如本领域的技术人员所熟知，证据推理是一种技术，其中收集支持和反驳给定假设的若干事实。结果就是以一定的可信度证明或者拒绝该假设。本发明的模糊逻辑处理使用证据推理从系统和工具对于每个标准的发现来累加证据，从而把系统评估数据合并成单一的参考点，

系统对特定标准的适应性。通过提供汇合所用的一套标准，系统约束汇合问题，缩小搜索范围。前面已经使用证据推理来执行第一级别的多探测器数据汇合，证据推理是模糊专家系统中普通的全局推理技术，比如本领域的技术人员所熟知的系统类型，如 NASA 开发的 fuzzyCLIPS。结果是一套模糊证据规则，其目的是为了给定的一组需求累加证据。这就由专家相关解决了可能是冲突的、含糊的和多余的数据，利用可用的数据得出结论，即使它是不完全的。

结果的准确性取决于可用数据的量和质，在应用模糊逻辑处理之前，可能需要对可用的数据进行附加的净化，同时也要维持数据的随机自然性质。这种净化使用推论网络，并且使用试探法提供一种有关概率的推理方法，从而消除对大范围先验知识的需要。目标和潜在安全的度量之间的关系促进了相互结合。正如本领域的技术人员所熟知，fuzzyCLIPS 使用模糊事实，它能够假设 0 和 1 之间的任何值。结果可视为以 0 和 1 为垂直边界的一个连续函数的二维图。

数据汇合用于系统目标数据库、数据结果数据事实库。智能数据汇合是一种多级别、基于多学科的信息处理，从多个智能源（以及可能的多种智能学科）产生有关某个实体的具体的和全面的、统一的数据（它的状况、功能和它受到的威胁），从而产生信息集成。数据汇合提供了基于可用输入的信息。智能数据汇合处理通常分为四个级别，见下面表 1 中的介绍。

表 1 智能数据汇合处理的级别和目的

数据汇合级别		描述
1	目标净化	<ul style="list-style-type: none"> ● 数据变换至一致的参考框架 ● 在时间方向净化和延伸，估计目标的位置、运动或属性 ● 数据分配至目标，以便应用估计处理 ● 净化目标鉴别的估计
2	状况净化	<ul style="list-style-type: none"> ● 在此环境的条件下，形成目标和事件之间当前关系的描述 ● 一个符号的推理过程，其中在操作问题的情况下，把固定的和追踪的实体的分布以及事件和活动与环境 and 性能数据相关联
3	威胁净化	<ul style="list-style-type: none"> ● 把当前的“状况”投影到将来，得出有关威胁、弱点和操作机会的推论
4	处理净化	<ul style="list-style-type: none"> ● 监控处理性能，以提供实时控制和长期改善所需的信息 ● 确认改善多级别汇合结果需要什么信息 ● 确定与源有关的数据需求，以便收集所需的信息 ● 分配和指挥源，以达到任务的目标

如上所述，NVT把来自多个源的多种数据类型与其它环境的信息相结合，以形成网络化系统的安全姿态的综合描述。NVT为用户提供给定系统或系统设计之弱点姿态的简单表达，并且使他们对于功能、性能和对策措施能够进行“如果……如何”的分析，以达到净化和改善系统或系统设计的目的。

在计算机安全工程中，探测器是多种弱点评估和风险分析的估计，与GUI一起采集用户需要的信息。这些工具的结果输出采用的形式既有定性的数据，也有定量的数据，不同的厂商使用的格式也不同。对于计算机安全工程，所关注的目标是网络（计算机系统）中的节点，也就是资产，包括硬件、软件和数据。所关注的状况是对计算机网络区段的安全系统中的弱点的评估，这些弱点可能会被利用来对保密性、完整性或可用性造成损害或损失。

评估计算机系统面对的风险包括评估面对的威胁、其发生（被利

用)的可能性和损失(或损害)的预期成本。最后,根据成本效益分析的结果,可以净化网络(计算机系统)。这就需要对于特定的弱点及其成本为适当的保护措施(控制或对策)的信息。成本效益分析力图确定使用某种控制或对策是否降低成本,或者接受该损失的预期成本。这就导致改善计算机网络系统安全的安全计划的制定。

对于本发明可以使用的计算机安全工程,表2包含了这种数据汇合处理的第一种划分的一个实例,具有四个处理级别,对应于表1中的四个级别。如图12所示,这项处理的输入包括对象模型数据库138、各个工具132、134、136的结果以及其它环境信息。不同的数据汇合级别1-4通常在320、322、324和326处表示。

表 2 计算机安全分析中数据汇合的内部处理级别

数据汇合级别		描述
1	节点数据 净化	<ul style="list-style-type: none"> ● 数据变换至一致的参考框架 ● 在网络节点级别（计算机安全数据汇合的目标）净化数据 ● 来自多个工具的数据：相关（分配到适当的节点）并可能在每个节点结合 ● 净化目标鉴别的估计：网络节点（工作站）是一种系统的系统，包括一种 OS、关键的应用程序、一个数据库和数据 ● 在这个级别的弱点分析尚不构成状况评估
2	网络区段 净化	<ul style="list-style-type: none"> ● 在网络区段级别（系统的系统级别）的状况净化 ● 在此环境（一个网络区段）的条件下，形成目标（节点）之间当前关系的描述 ● 一个符号的推理过程，其中把有关实体（节点、网络区段）和环境的信息与有关计算机安全目标、需求的证据相关联 ● 在网络区段级别使工具的结果结合 ● 所关注的状况是评估网络区段的弱点或暴露
3	风险净化	<ul style="list-style-type: none"> ● 净化暴露风险及其在计算机系统之内的潜在损害（风险） ● 把当前的“状况”（计算机网络系统的状态）投影到将来，得出有关威胁、弱点和操作机会的推论 ● 根据弱点、影响、环境、成本、威胁 ● 利用减少一个或多个弱点的控制标识来净化系统设计 ● 根据对策、组件、成本 ● 确认改善多级别汇合结果需要什么信息 ● 便利系统的长期改善

为了应付多个弱点评估和风险分析工具结果的合并问题，虽然本发明中使用的数据汇合提供了概念性的框架，还是要使用专家系统、推论网络和证据推理来实现汇合的概念及合并各工具的结果。模糊判

断技术尤其是模糊专家系统的灵活性，提供了应付这些问题的方法。模糊专家系统的主要好处是它能够使用和吸收多个来源的知识。

模糊逻辑提供了由不精确、不确定或不可靠的知识进行表示和推理的技术。与传统的专家系统类似，模糊专家系统也能够以如果/那么规则之体制的形式来表示知识，其中前项、后项或者二者兼而有之，是模糊的而不是明晰的。模糊逻辑用于确定模糊事实与规则匹配得如何，这种匹配在多大程度上影响该规则的结论。依据本发明，推论网络是试探规则的一种层次，它在无需先验概率的广泛知识的情况下能够传播概率（例如贝叶斯网络）。使用概率如何传播的专家知识，能够建立试探规则，在先验概率的知识有限时也可以得出结论。这就使得低级别的离散概率在较高级别的结论中准确地反映出来。低级别事件的概率（比如基于使用期限的密码损坏的概率）必须是对较高级别事件（密码的弱点）得出的任何结论的一部分。

最初的 NVT 研究使用证据的累加来修改模糊事实以及表示当前系统所需的状态变化。这种状态变化的模糊事实然后用于修改系统，新状态以不断循环的方式反馈到状态规则的变化中，以使用全局的贡献。FuzzyCLIPS 允许定义模糊事实类型，但是每种类型只能有一个事实存在。所以，每一个操控事实类型的规则实际上仅仅修改单一的事实，导致证据的累加。

全局贡献和证据累加导致 FuzzyCLIPS 的方法，它定义模糊事实来表示不同的弱点状态。这些事实将使用全局贡献和证据累加来获取反映受测试系统之弱点的最终数值，也就是证据推理。这种方法反映了模糊逻辑控制系统的明确定义的使用，把执行循环限制到有限的次数，而不是让它不断地运行。佛罗里达州 Melbourne 的 Harris 公司开发的 FuzzyFusion™ 将使用这种方法，按照网络安全专家的知识制定规则，并根据规则累加证据。确切地说，FuzzyFusion™ 将采用证据推理技术，其中收集的事实支持和反驳某个给定假设。结果就是以一定的可信度证明或者拒绝该假设。

最初的知识提取致使采用安全需求来累加证据，也就是某个系统

满足这些需求的程度。这表明了检验某个数据库（例如 AFCERT）的方法和检验安全需求之间强有力的相关，导致使用数据库和需求作为全局贡献来累加证据，如图 13 所示。这也表明了改变目标的粒度如何直接影响着评估的粒度，也就是评估只能细致到与目标相当。除了保持使用向前推论技术，证据累加也被视为面向目标的、获得结果的方法，现在将被措词为“基于目标的汇合”。

在计算机安全中，如何将模糊逻辑应用到合并工具的结果，一个实例使用 ANSSR 和 ISS 因特网扫描器结果的结合，它们是 NVT 的一个方面中目前使用的工具中的两种。这些工具的输出既有定量的（ANSSR），也有定性的（因特网扫描器）。模糊逻辑允许系统在同一个系统中同时表示这两种数据类型。然后用格式表示一个初始假设，用模糊逻辑收集反驳或支持该假设的证据。

对于这个实例，初始假设可能是，在某个现有的网络系统中审核是无效的。该系统的用户然后运用 ANSSR 和 ISS 因特网扫描器工具。如果 ANSSR 供应了一个数字 90（出自 100），该审核是充分的。模糊逻辑允许 NVT 将此视为对于审核是无效的这一初始假设的强烈的反驳证据。如果因特网扫描器供应的定性数据为 User Access 没有受到审核，模糊逻辑将此视为支持证据，它与 ANSSR 的证据相结合。工具使用完成后，对于审核有贡献的证据表示为单一的模糊事实，它提供了审核执行情况的一种度量。

对于在 NVT 之内使用的弱点评估和风险分析工具，佛罗里达州 Melbourne 的 Harris 公司开发的 FuzzyFusion™ 是整理和合并其结果而得出一个统一报告的一种方法。确切地说，FuzzyFusion™ 是用于执行第 1 和第 2 级别的汇合。FuzzyFusion™ 的完成要靠使用 FuzzyCLIPS 的模糊专家系统（面向目标的模糊逻辑判断规则），它结合了多种工具的输出、用户对系统风险和弱点的关注以及专家怎样理解每种工具的结果和这些如何归纳到一个较大的信息系统安全的描述。因此，NVT 用户获得给定计算机系统或者系统设计之安全姿态的简单表达，并且能够对于功能、性能和对策措施能够进行“如果……”

如何”的分析。

图 14 展示了 NVT FuzzyFusion™ 的组件体系结构，它用于执行计算机安全工程中最先的两个级别的数据汇合。如图所示，模拟安全专门技能的任务划分为分开的任务。专家相关的分离（数据框架合并规则）、模糊推论网络规则和模糊证据推理规则涉及脆弱的专家系统和计算量爆炸的问题。它把两类操作分离开，一类是低级别的数据相关和汇合，另一类是分解不明确的/有抵触的数据以及合并结果得出一个描述。这样应当使模糊专家系统比一个大而全的系统更加容易维护。下面介绍这个体系结构的单元。

数据模糊化 310 把各个弱点评估和风险分析工具的结果 132、134、136 转换为模糊事实，并把它们与公共系统模型（CSM），也就是系统对象模型数据库 138 一起存入（FuzzyCLIPS 的）事实库 302。（模糊化之后）各个工具的结果和 CSM 138 输出到专家相关处理 330（数据框架合并规则）以便根据安全专门技能分解系统信息和集成各工具的输出。专家意见可以用于确定由低级别事件引起的、具体的模糊数值。

专家相关 330（数据框架合并规则）是模糊专家规则的集合，用于执行节点级别的数据净化（第 1 级别）或者网络区段的净化（第 2 级别）。这些规则使用安全工程师的专门技能，对弱点评估和风险分析工具的（模糊化了的）输出进行相关和整理。这些规则使安全评估中广泛的经验发挥了加倍的作用，以便分解低级别的系统数据和各工具的结果。这些规则分解系统信息和集成各工具的输出。专家相关规则处理 330 也可以把 CSM 的低级别数据和各工具的结果变换为高级别的结论。例如，

如果根据这些旗标审核正在进行，
而且审核数据没有备份，
那么审核是不可靠的。

一套第 1 级别的汇合规则通过作用于事实库 302 中的模糊事实，能够整理每个节点的弱点，得出网络中每个节点的弱点等级。这个等级能够输入回到 NVT 进行显示。同样，一套第 2 级别的汇合规则能够整理每个网络区段的弱点，得出每个网络区段的弱点等级。这又可以输入回去进行显示。

然后数据进行模糊推论网络规则处理 304。在应用模糊证据推理规则 304 之前，可能需要对可用数据执行附加的净化，同时保持数据的随机自然性质。这种净化将使用推论网络，正如本领域的技术人员所熟知，它提供一种使用试探法推理概率的方法，从而消除对广泛的先验知识的需要。

模糊证据推理规则 306 是模糊专家规则的集合，用于从系统级别的观点，把各工具的结果合并成网络安全姿态较高级别的评估。这些规则提供了一种机制，把 CSM、各工具的结果和专家相关（数据框架合并规则）330 的结果合并成统一的报告。这也消除了由专家相关中使用的向前链接专家系统应付不完全和有抵触的数据的需要。

证据推理使用一种技术，其中收集事实来支持和反驳某个给定的假设。结果就是以一定的可信度证明或者拒绝该假设。对于每个标准，FuzzyFusion™ 使用证据推理来累加来自公共系统模型和工具发现的证据，从而把计算机网络系统评估数据合并成单一的参考点，使系统适应特定的准则。通过供应一套汇合准则，NVT 约束汇合问题并减小搜索空间，参见前文的基于目标的汇合。结果将是一套模糊证据规则，其唯一的目的是对于给定的一组需求累加证据。这就从专家相关（数据框架合并规则）330 分解了可能有抵触的、不明确的和多余的数据，并利用可用数据得出结论，即使该数据是不完全的。显而易见，结果的准确性取决于可用数据的数量和质量。

如上所述，模糊逻辑处理是面向目标的。证据累加处理的目标 350 可能取自安全需求数据库 352、计算机安全度量数据库 354 或者弱点数据库 356，比如由 AFCERT 组成的数据库。使汇合不超出预定的目标限定了计算时间。FuzzyFusion™ 的目标提供了获得 IA 度量的机制。

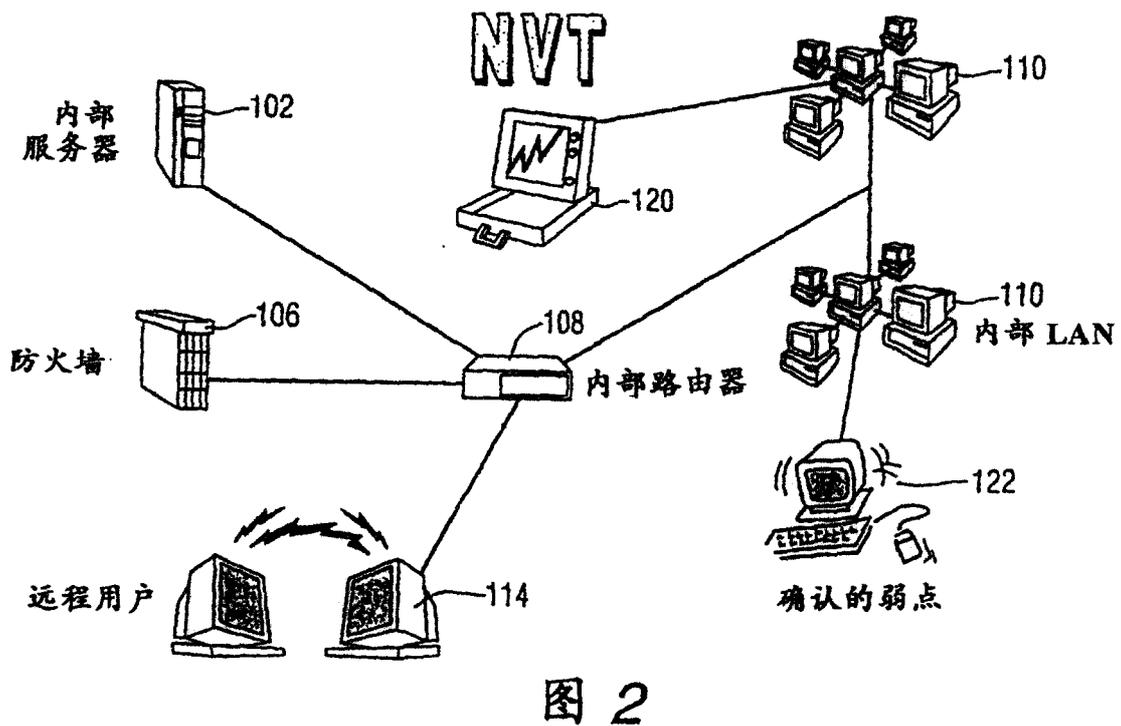
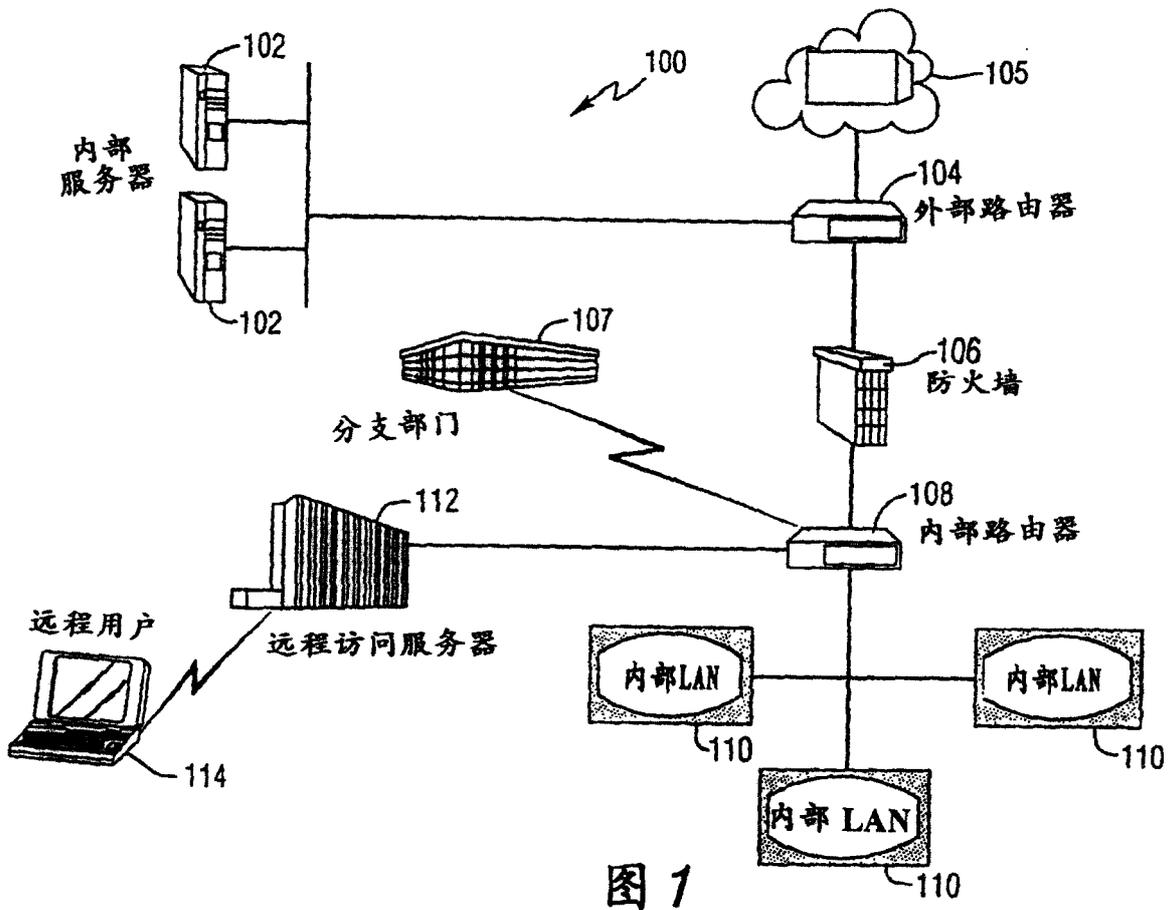
FuzzyFusion™ 的处理具有许多超过传统方法的优点。明确的专家系统会需要极为庞大的知识库以包含必需的数据，即便如此，仍然有不完全数据和有抵触结果的问题。贝叶斯和概率网络需要广泛的和往往是不可得的先验概率知识。算法解决方案不适合安全问题的随机的和试探的自然性质。

基于神经网络的专家系统比如 **FuzzyCLIPS** 要忍受执行时间的几何增长，这是基于系统中存在的规则和事实的数目。这就导致把分析划分到子网络中进行。**FuzzyFusion™** 将增加子网络和按比例分配功能。每个子网络的节点将作为一组来评价，然后再评价含有多个子网络的组。每个分析类型的规则分组到不同的模块，减小了神经网络的尺寸。除了缩短执行时间，这也引入了一种可伸缩的分析网络方法，它映射到 NVT 使用的网络模型。

如图 15 所示，其它可能的数据空间可能包括一个威胁知识数据库 360、成本数据库 362 作为第 3 级别汇合的一部分，以及对策知识库、组件数据库和成本数据库作为第 4 级别汇合的一部分。

本申请书与以下同时待审的专利申请有关，其标题为“**SYSTEM AND METHOD FOR ASSESSING THE SECURITY POSTURE OF A NETWORK (评估网络安全姿态的系统和方法)**”和“**SYSTEM AND METHOD FOR ASSESSING THE SECURITY POSTURE OF A NETWORK USING GOAL ORIENTED FUZZY LOGIC DECISION RULES (使用面向目标的模糊逻辑决策规则评估网络安全姿态的系统和方法)**”，它们在同一日期由同样的代理人 and 发明者提交，其公开文件这里引用作为参考。

受益于前文的介绍和附图提供的教导，本领域的技术人员将会想到本发明的许多修改和其它实施例。所以，应当理解，本发明不限于公开的具体实施例，上述修改和实施例将试图包括在有关权利要求书的范围之内。



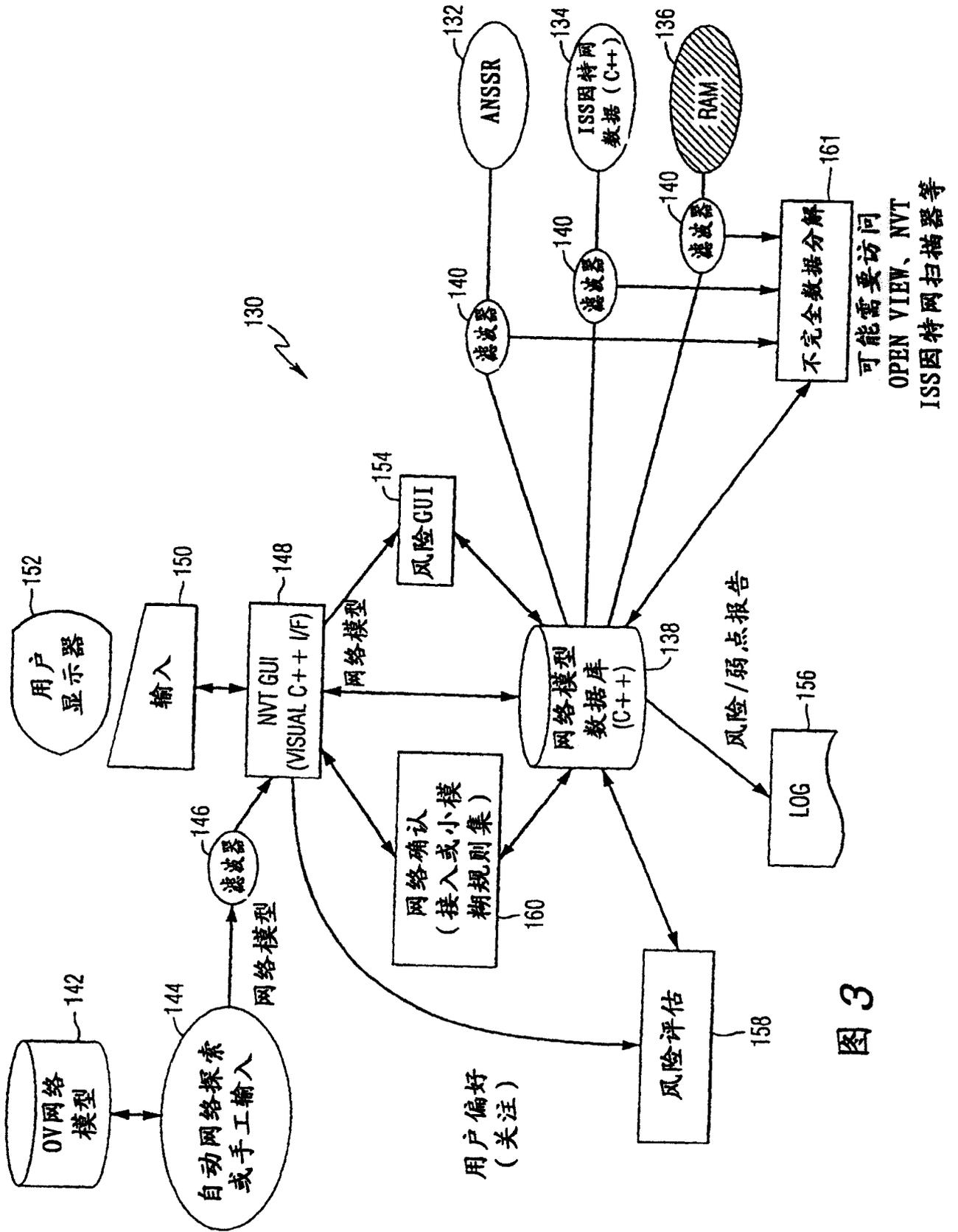
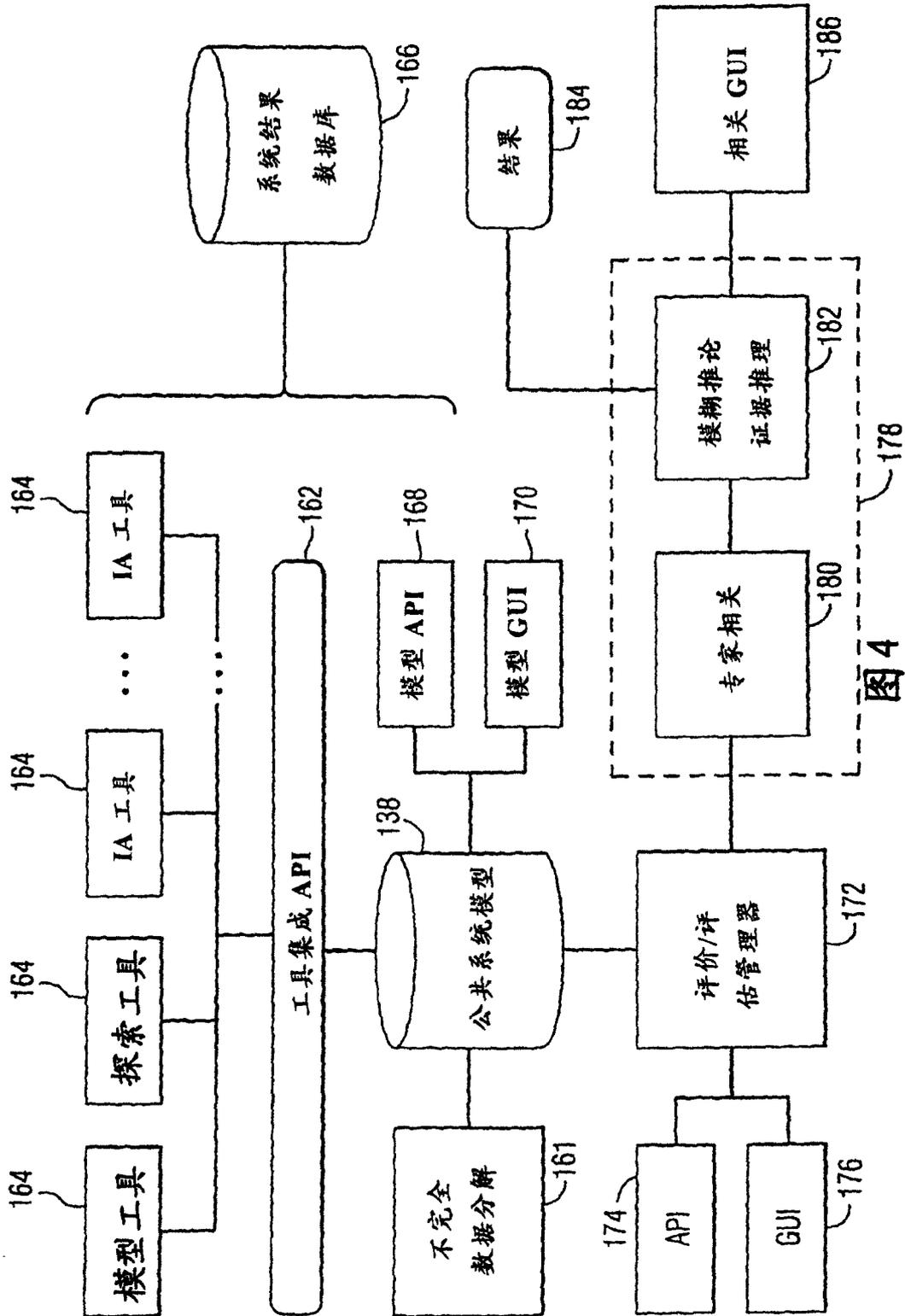


图 3



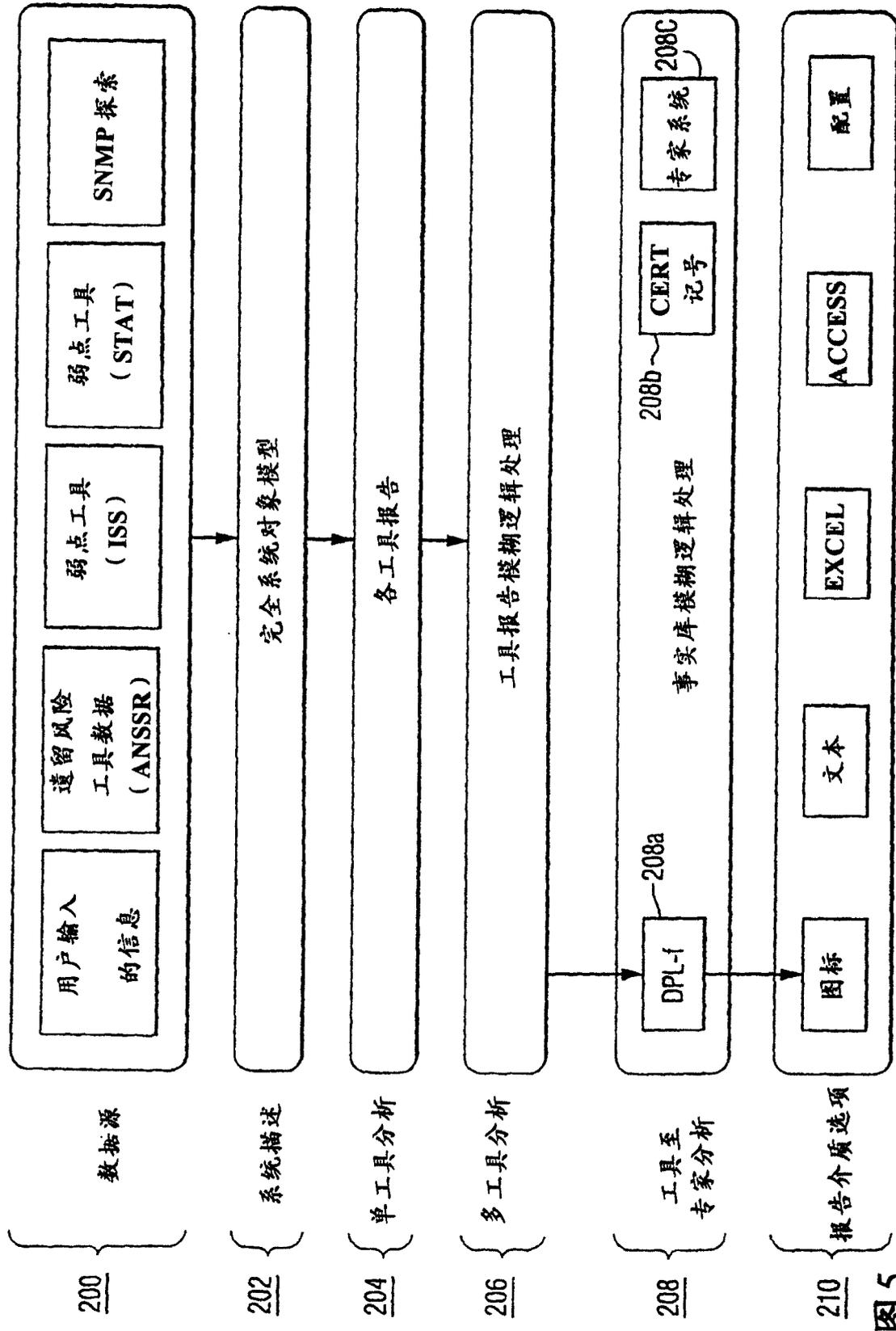


图5

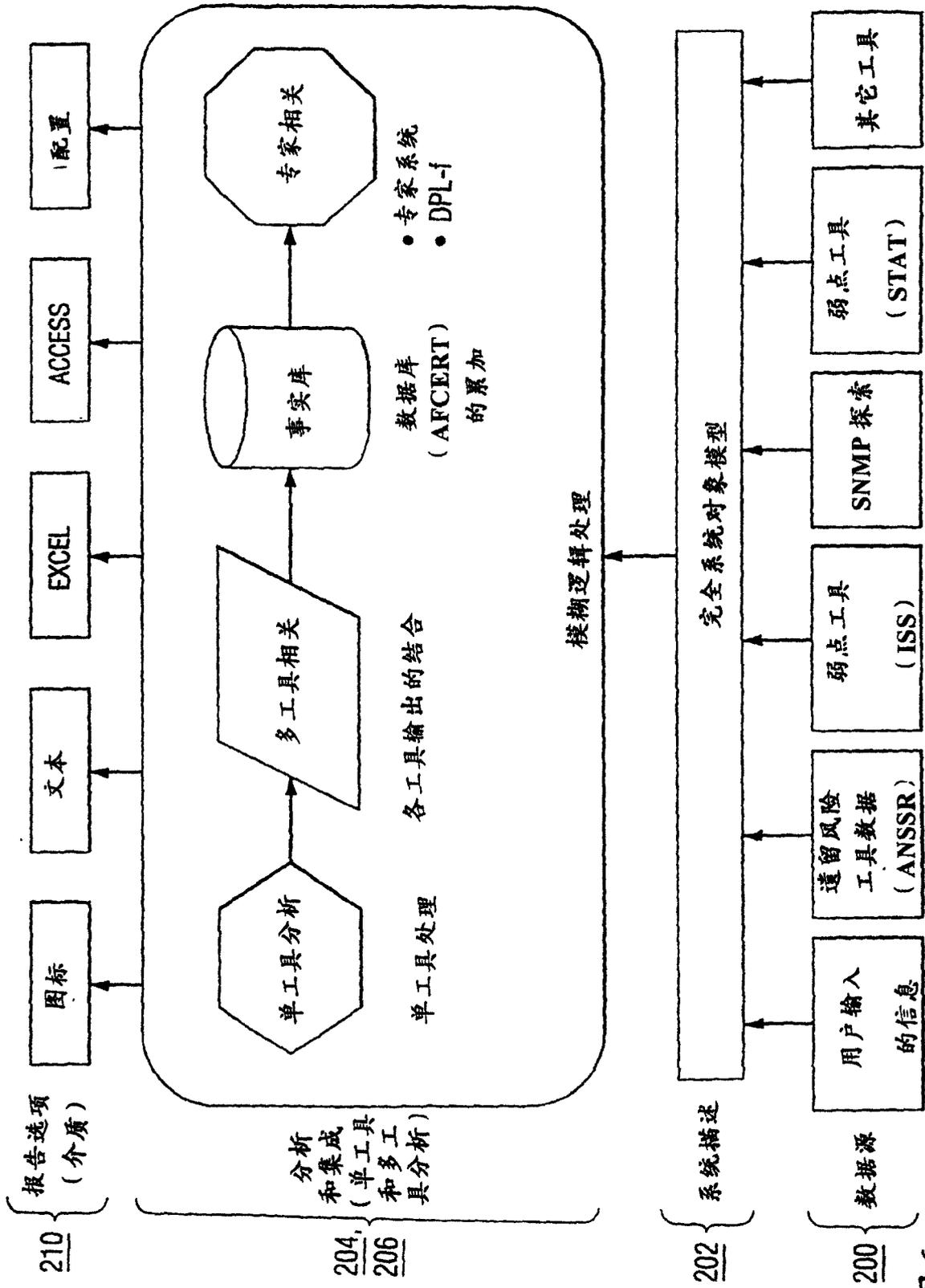


图 6

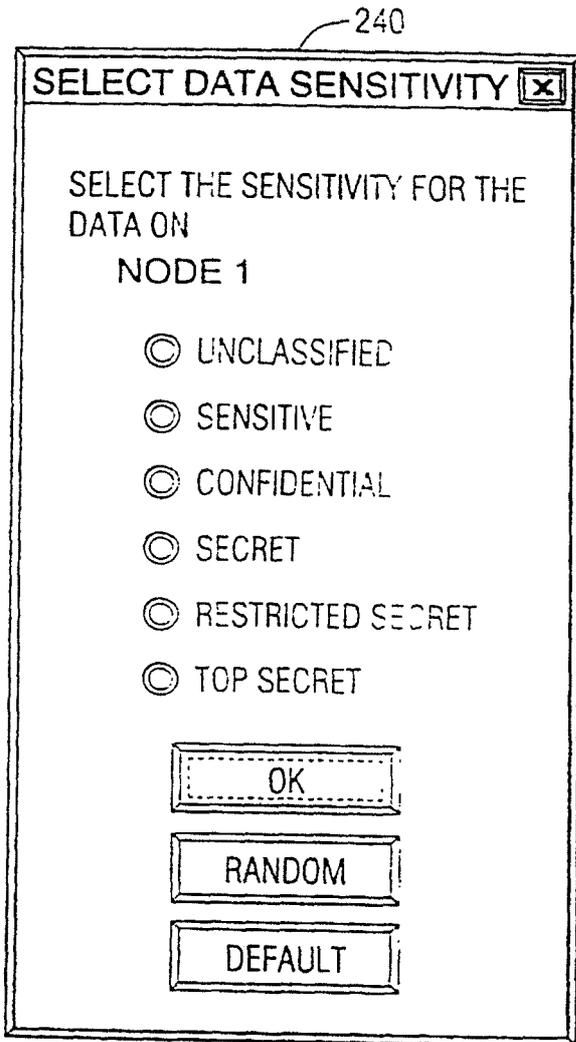


图 8A

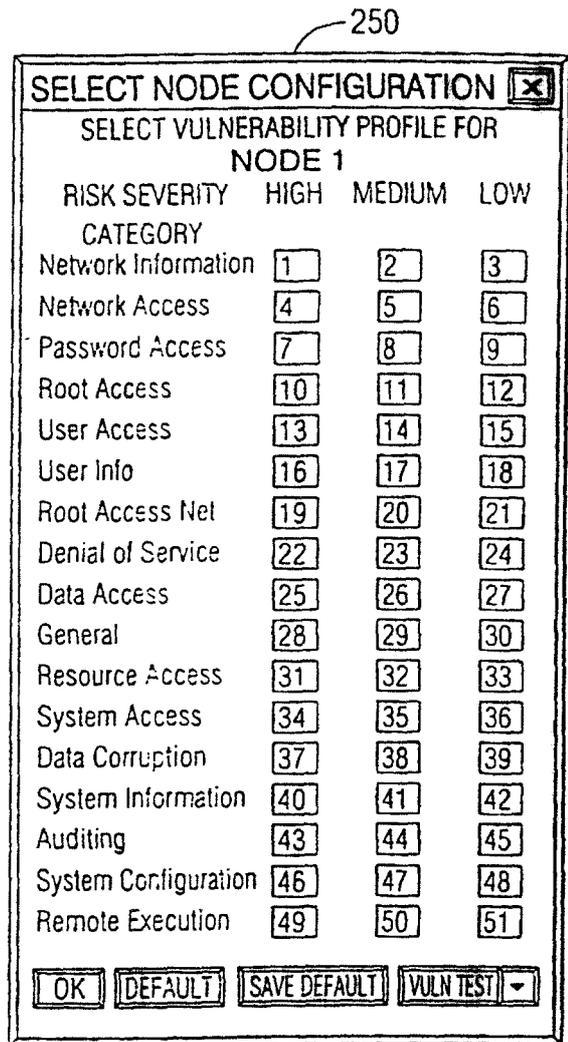


图 8B

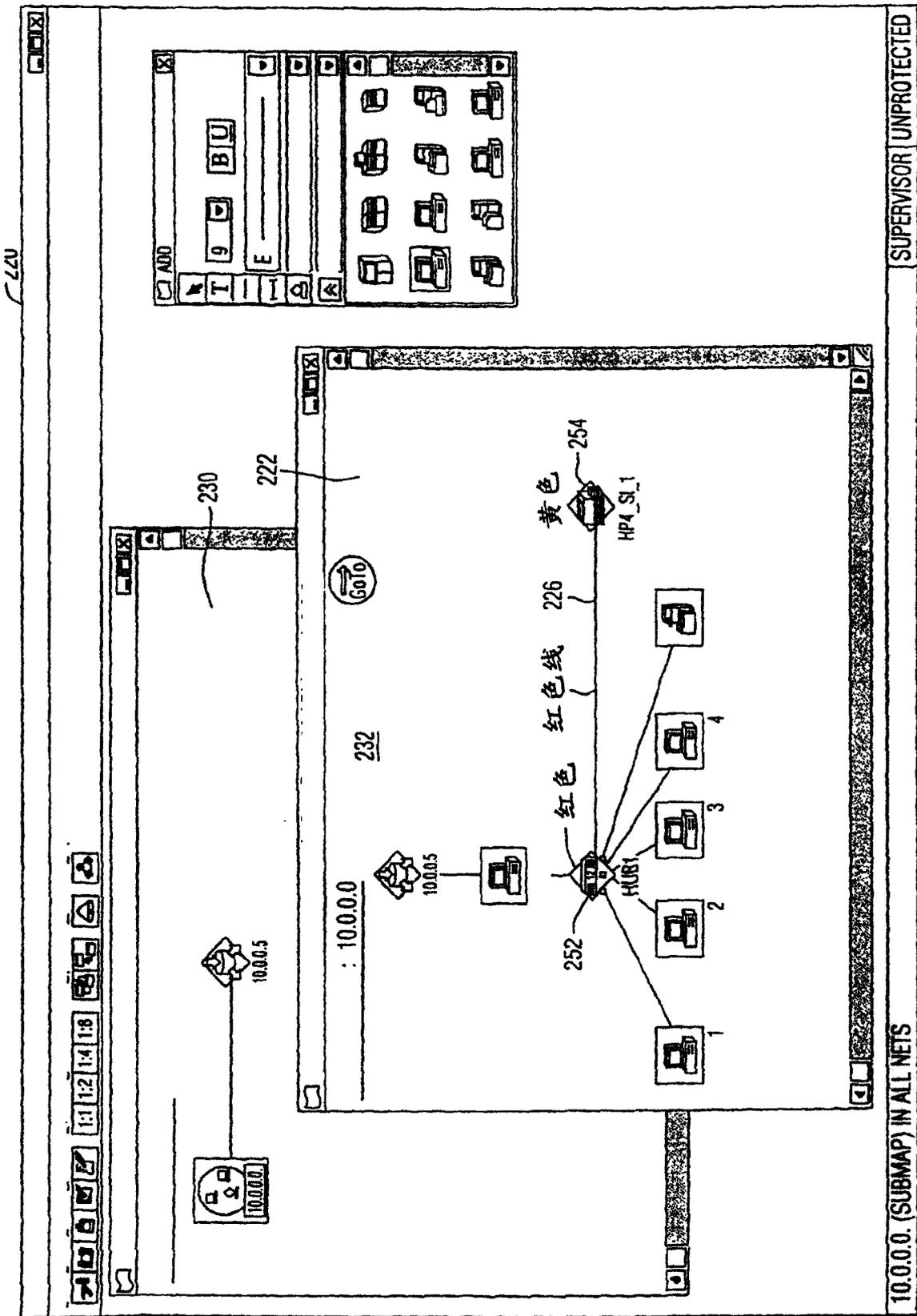


图9

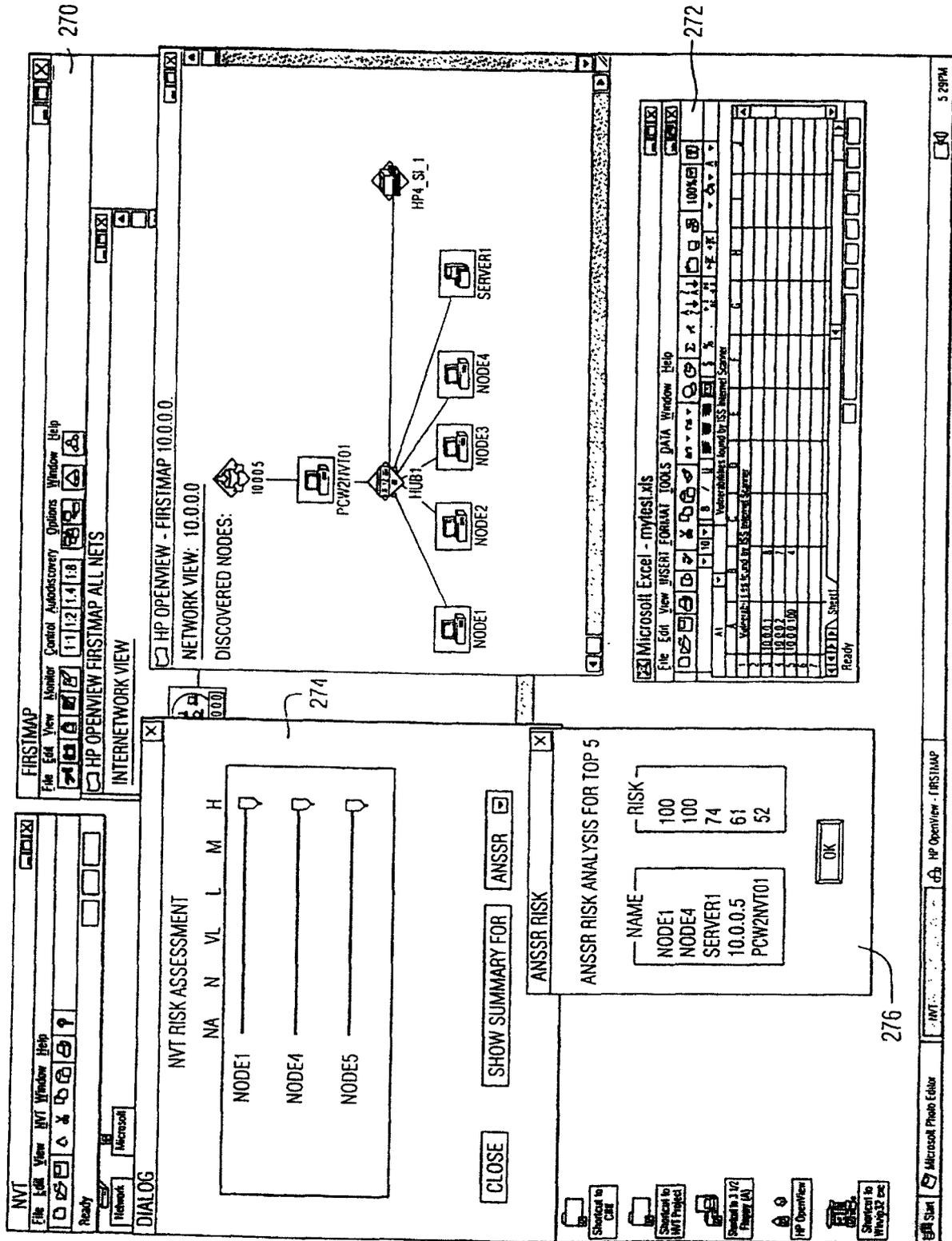


图 10

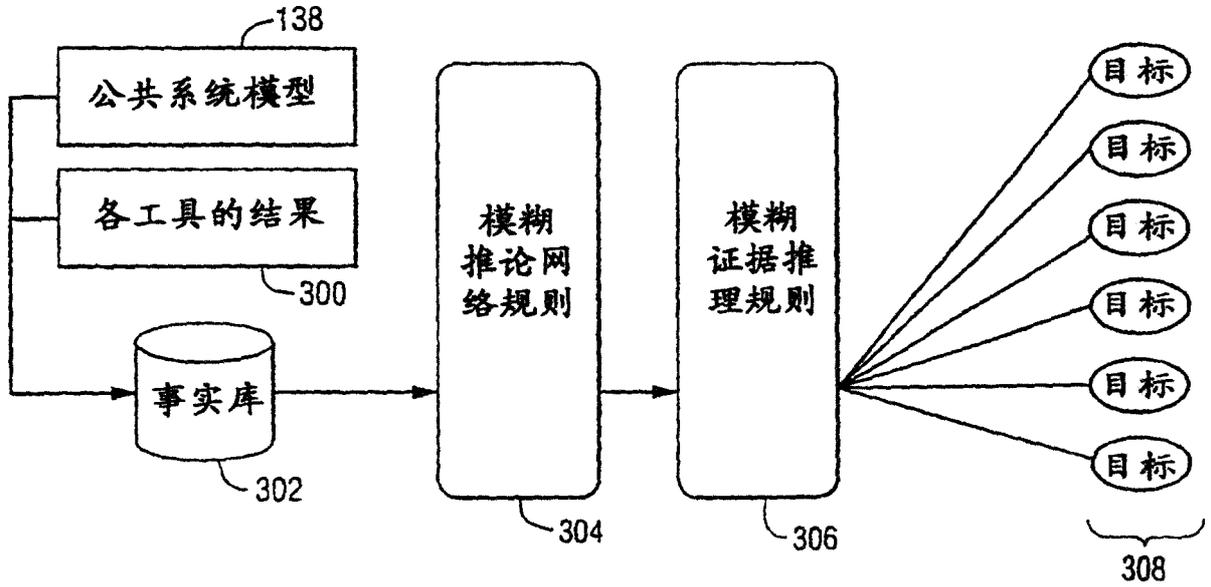


图 11

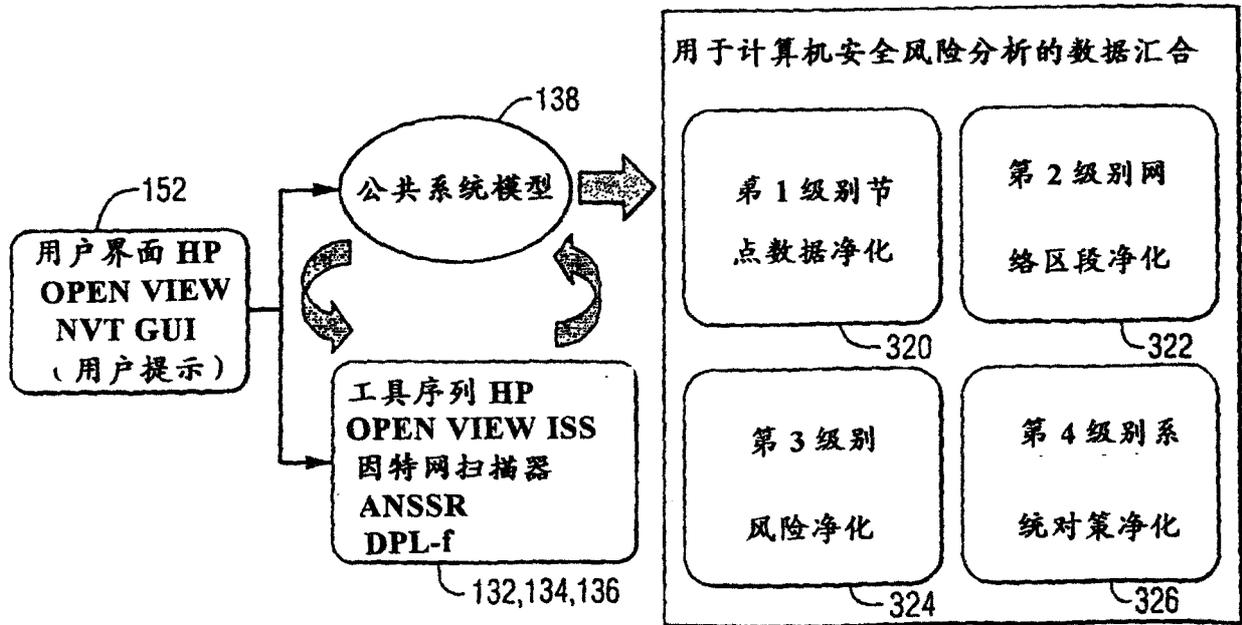


图 12

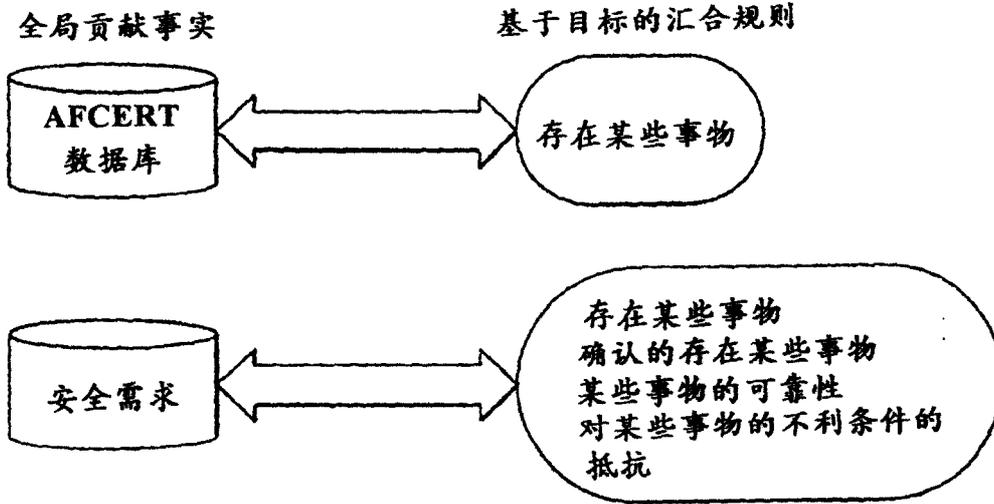


图 13

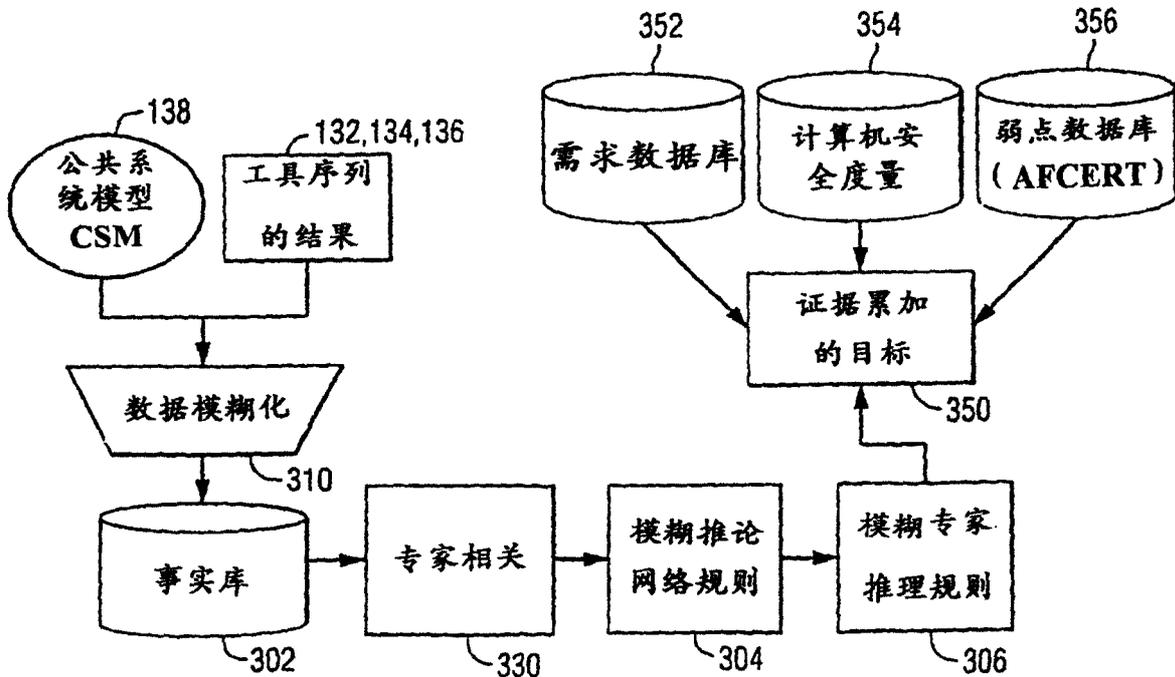


图 14

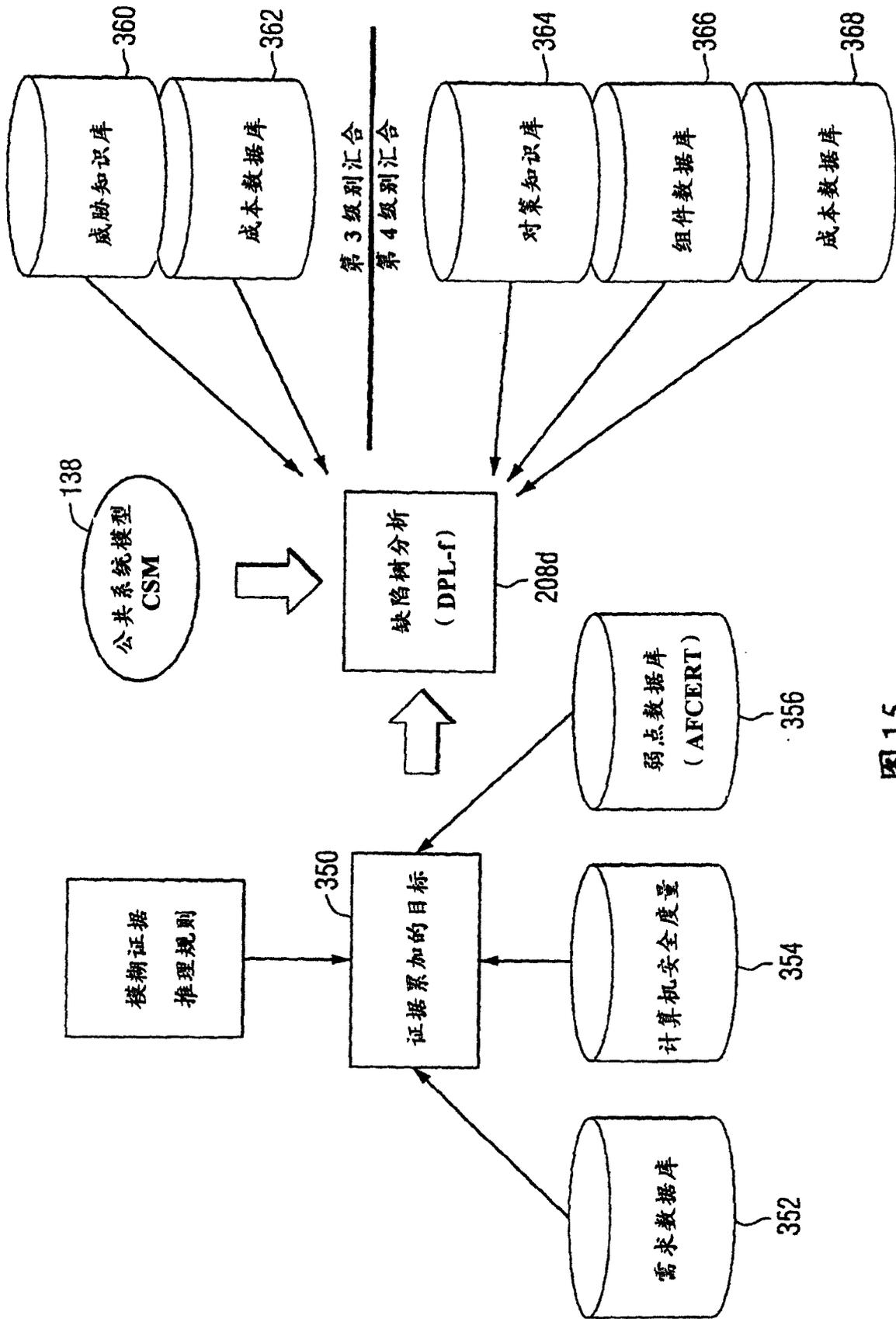


图15

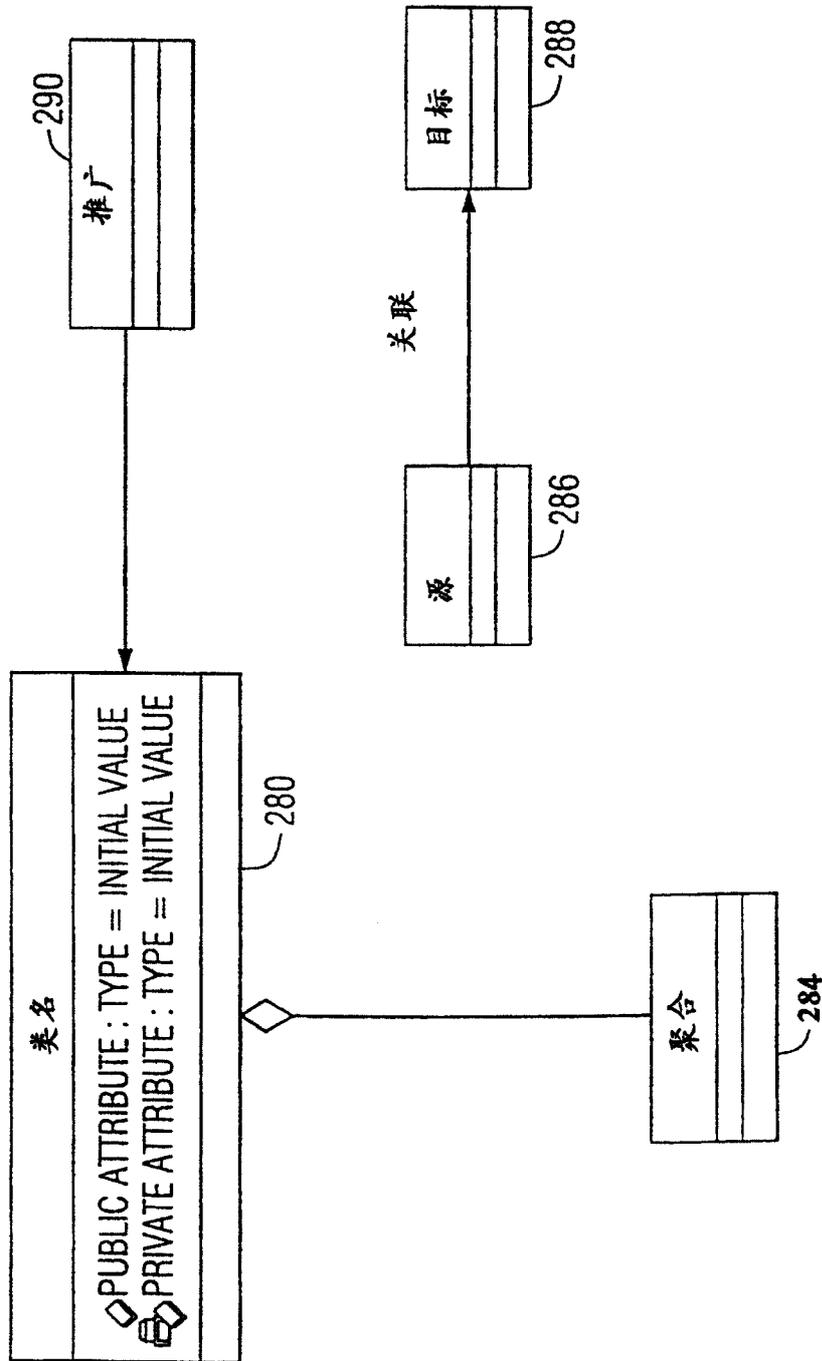


图16

