

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 12/24 (2006.01)

H04L 29/06 (2006.01)



[12] 发明专利说明书

专利号 ZL 01804680.0

[45] 授权公告日 2006 年 7 月 26 日

[11] 授权公告号 CN 1266879C

[22] 申请日 2001.1.26 [21] 申请号 01804680.0

[30] 优先权

[32] 2000. 2. 8 [33] US [31] 09/500,269

[86] 国际申请 PCT/US2001/002825 2001.1.26

[87] 国际公布 WO2001/059594 英 2001.8.16

[85] 进入国家阶段日期 2002.8.7

[71] 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 约翰·法莱尔

隆达·汉宁 克里弗德·米勒

审查员 孙文涵

[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 董 莘

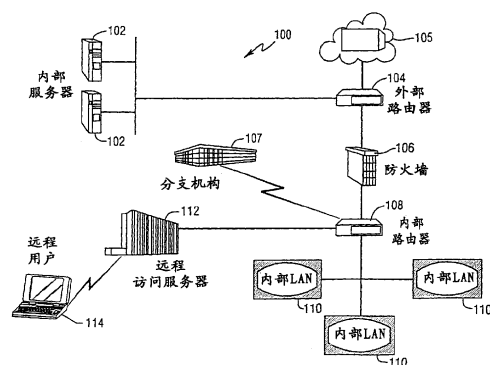
权利要求书 2 页 说明书 22 页 附图 14 页

[54] 发明名称

利用面向目标的模糊逻辑决策规则评估网络的安全姿态的系统和方法

[57] 摘要

一种方法和数据处理系统评估网络的安全脆弱性。系统对象模型数据库得以创建并支持完全不同的网络脆弱性分析程序的信息数据需求。从表示该网络的系统对象模型数据库只输出所需的数据到这些程序，程序接着分析网络以从每个程序产生数据结果。这些数据结果存储于数据事实库内的公共系统模型数据库。面向目标的模糊逻辑决策规则用于确定网络的脆弱性姿态。



1. 一种用于评估网络的安全姿态的方法，所述方法包括步骤：

根据完全不同的网络脆弱性分析程序来创建表示对象/类分层结构中的网络系统描述的系统对象模型数据库，其中所述系统对象模型数据库支持完全不同的网络脆弱性分析程序的信息数据需求；

从所述表示网络的系统对象模型数据库中仅仅输出所需的数据到每个对应的网络脆弱性分析程序；

利用每个网络脆弱性分析程序分析所述网络，以根据每个程序产生数据结果；

存储通过运行相应的网络脆弱性程序以及数据事实库中的公共系统对象模型数据库而得到的数据结果；

通过利用专家关联、模糊推理网络规则和模糊证据推理规则而运作的面向对象的模糊逻辑决策规则，将所述系统对象模型数据库与根据存储在所述数据事实库中的完全不同的网络脆弱性分析程序而得到的数据结果相关联；以及

通过利用关于任何概率是如何传播的专家知识，形成以可以传播概率的启发式规则的体系结构形式的推理网络，使得利用有限的先验概率知识得出多个结论，以便低级离散概率在网络脆弱性的高级结论中反映。

2. 根据权利要求1的方法，其特征在于，经过以程序形式的过滤器，从系统对象模型数据库中仅仅输出所需的数据，其中所述程序允许相应网络脆弱性程序所需要的数据输入到网络脆弱性分析程序。

3. 根据权利要求1的方法，其特征在于，经由综合应用编程接口输出所述系统对象模型数据库中的数据到网络脆弱性分析程序。

4. 根据权利要求1的方法，其特征在于，以图形用户接口上的网

络映像的形式显示网络图标。

5. 根据权利要求1的方法,其特征在于,建立类名的类分层结构,以定义共用公共数据和编程特性的网络脆弱性分析程序的组件。

6. 根据权利要求1的方法,其特征在于,运行网络脆弱性分析程序以获得关于网络系统细节、网络拓扑、节点级脆弱性和网络级脆弱性的数据结果。

利用面向目标的模糊逻辑决策规则 评估网络的安全姿态的系统和方法

技术领域

本发明涉及网络领域，本发明尤其涉及评估网络的安全脆弱性的领域。

背景技术

当前正开发的信息系统和计算机网络基础设施的建设正在考虑什么构成可接受风险（或足够的保护）。系统资产，如计算机网络的硬件、软件和系统节点，必须得到与它们的价值相符合程度的保护。另外，这些资产必须得到保护直到它们失去其价值。任何安全特征和系统体系结构也应在所处理数据的整个使用期限内提供足够的保护。为评估任何与网络相关的风险是否可接受，安全工程师典型地收集所有相关信息，接着分析与该网络相关的风险。

风险分析是一项复杂而耗时的工程，其对于确定网络内的暴露以及它们的潜在危害是必要的。举例来说，当分析计算机网络中的安全风险时，安全工程典型地遵循下面的步骤：

1) 确定整个计算系统的资产。

2) 确定资产的脆弱性。这个步骤典型地需要想象力以便预测对这些资产可能发生什么样的危害及其来源。计算机安全的三个基本目标是确保秘密、完整性和可用性。脆弱性是可能导致失去这三个特性中的一个的任何情况。

3) 预测事件（利用）的可能性，即，确定每个暴露将被利用的频率。事件的可能性与现有控制的严格程度，以及某人或某物可逃避现有控制的可能性有关。

4) 通过确定每个事件的预期成本计算每年的任何无覆盖成本（预

期年度损失)。

5) 调查可应用的控制和它们的成本。

6) 预测控制的年度节省。

该分析的最后一步是成本-效益分析,即,是实现控制花费较少还是接受预期的损失成本。风险分析导致安全规划,这个规划确定提高安全性的特定行动的责任。

目前,技术的快速发展和具有更强功能的计算机的大量出现使得能托管商业现有的(COST)硬件和软件组件的使用,作为成本有效的解决方案。这种强烈依赖于COTS隐含商业级的安全机制足以用于大部分应用。因此,安全体系结构必须构筑为用相对弱的COTS组件建立可操作、关键任务计算机系统。具有更高安全保证的组件可置于公共或信息边界,形成基于飞地(enclave)的安全体系结构,实现对信息安全保证的深度防护途径。

有一些设计工具,即,软件程序,系统设计师可用它来辅助最大化可用的保护机制,同时维持在开发预算之内。当前一代的风险分析工具通常为单厂商解决方案,其只处理特定一个或几个方面的风险。这些工具趋向归入下面三种类型的一种:

1)从备有大量文件的脆弱性数据库工作而且可能修复已知的脆弱性的工具。这种类型的工具对数据库更新依赖于厂商,或通过新产品版本或通过订购服务实现更新。这一类的例子包括ISS的Internet Scanner, Network Associates公司的CyberCop和Harris的STAT。

2)使用各种参数计算风险指标的单片电路工具。这些工具难于维护而且很难与当前迅速发展的威胁和技术环境保持同步。这种工具类型的例子有Los Alamos脆弱性评估(LAVA)工具。

3)检查系统特定方面,如操作系统或数据库管理系统,但忽略其它系统组件的工具。例如SATAN,分析操作系统的脆弱性,但忽略诸如路由器等的基础设施组件。

使用来自各个厂商的多种工具用于单个计算机网络分析是一种劳动密集性工作。典型地,安全工程师将必须多次以多种格式输入系统

（网络）的描述或表示。安全工程师接着必须手工分析、整理和合并这多个工具的输出结果为单个网络安全姿态报告。之后，安全工程师可完成风险分析（计算预期的年度损耗、调查控制等），接着重复该过程以分析安全风险、系统性能、任务功能以及研发预算中的选择对象。

同样，这些工具中没有一种对具有“下钻（drill down）”或分层次法的系统使用总体“快照（snapshot）”法，以便于如何在系统的不同层次（网络、平台、数据库等）上处理风险。在分析安全风险、系统性能和任务功能中的选择对象时，这些工具对系统设计师提供不了多少帮助。相反，“风险解决方案”得以提供，它能解决设计给定工具用于计算的风险的特定方面。为开发综合性风险评估，安全工程师将不得不精通各种工具的使用，以及通过手工方式使结果产生的输出相互关联。

成功的风险分析的一方面是完全和精确的数据积累以生成分析工具所使用的系统模型。许多当前的风险分析工具依赖于用户、系统操作人员和分析人员填写的调查表，以获得数据来开发在分析中所使用的系统模型。或者，工具可主动扫描计算机网络以测试对于系统部件的各种脆弱性。

然而，这些方法都有其缺陷。按原文或基于调查的知识征求技术为劳动密集型，而且可能对于分析人员来说很乏味。许多现有的工具重复利用相同信息来分析系统安全的不同方面。利用集中式建模数据的知识库更为方便，这可能提供在现有工具间共享输入的基础。这种知识库可用于生成由风险分析工具使用的数据集，允许多种工具在同一系统上运行而不用独立的输入动作，由此降低了操作人员出错的可能性。使用多种风险分析推理引擎，或桥（backbend），使得能分析系统的各个方面而无需开发一种工具来执行所有类型的分析的成本。综合信息和通过应用多种工具可得到的可靠的评估将产生更为健壮和精确的系统安全姿态画面。这些结果能促进更可靠的系统设计决策，提供用于可选评估和比较的框架。

发明内容

因此，本发明的目的是提供一种不必多次分析网络就能评估网络的安全脆弱性的数据处理系统和方法。

根据本发明，提供了一种用于评估网络的安全姿态的方法，所述方法包括步骤：

根据完全不同的网络脆弱性分析程序来创建表示对象/类分层结构中的网络系统描述的系统对象模型数据库，其中所述系统对象模型数据库支持完全不同的网络脆弱性分析程序的信息数据需求；

从所述表示网络的系统对象模型数据库中仅仅输出所需的数据到每个对应的网络脆弱性分析程序；

利用每个网络脆弱性分析程序分析所述网络，以根据每个程序产生数据结果；

存储通过运行相应的网络脆弱性程序以及数据事实库中的公共系统对象模型数据库而得到的数据结果；

通过利用专家关联、模糊推理网络规则和模糊证据推理规则而运作的面向对象的模糊逻辑决策规则，将所述系统对象模型数据库与根据存储在所述数据事实库中的完全不同的网络脆弱性分析程序而得到的数据结果相关联；以及

通过利用关于任何概率是如何传播的专家知识，形成以可以传播概率的启发式规则的体系结构形式的推理网络，使得利用有限的先验概率知识得出多个结论，以便低级离散概率在网络脆弱性的高级结论中反映。

根据本发明，还提供了一种用于评估网络的安全姿态的数据处理系统，包括：

用于分析网络的多个完全不同的网络脆弱性分析程序；

系统对象模型数据库，所述系统对象模型数据库包含表示对象/类分层结构中的、对应于被分析网络的网络系统描述的数据，其中所述系统对象模型数据库支持网络脆弱性分析程序的信息数据需求；

应用编程接口，用于将所述网络的系统对象模型数据库中的数据输入到网络脆弱性分析程序；

以程序形式的过滤器，所述程序允许每个对应网络脆弱性分析程序所需的数据将从所述系统对象模型数据库中过滤出，并且仅仅将所需的数据输出到网络脆弱性分析程序；

数据事实库，用于在分析所述网络以及公共系统模型数据库之后，存储通过运行相应的网络脆弱性分析程序而得到的数据结果；以及

模糊逻辑处理器，包括用于专家关联以及模糊证据推理的电路，用于通过利用专家关联、模糊推理网络规则和模糊证据推理规则而运作的面向对象的模糊逻辑决策规则，将所述系统对象模型数据库与根据存储在所述数据事实库中的完全不同的网络脆弱性分析程序而得到的数据结果相关联；并且通过利用关于任何概率是如何传播的专家知识，形成以可以传播概率的启发式规则的体系结构形式的推理网络，使得利用有限的先验概率知识得出多个结论，以便低级离散概率在网络脆弱性的高级结论中反映。

本发明的方法和数据处理系统现在就能评估网络的安全脆弱性。该方法包括创建表示网络的系统对象模型数据库的步骤。该系统对象模型数据库支持完全不同的网络脆弱性分析程序的信息数据需求。在该方法中，从表示该网络的系统对象模型数据库只输出所需数据到每个相应的网络脆弱性分析程序。使用该程序分析网络以从每个程序产生数据结果。存储来自各个网络脆弱性分析程序和数据事实库内的公共系统模型数据库的数据结果。接着应用面向目标的模糊逻辑决策规则到数据事实库以确定网络的脆弱性姿态。

在本发明另一方面，该方法包括步骤：经由与各自的网络脆弱性程序相关的过滤器从系统对象模型数据库仅输入所需的数据，以及经由综合应用编程接口输入。在本发明的再一方面，该网络可在图形用户接口上建模为映像。可建立类分层结构以定义共用公共数据和编程特性的网络脆弱性分析程序的组件。也可获得与网络系统细节、网络拓扑、节点级脆弱性和网络级脆弱性有关的数据结果。

更方便地，一种计算机程序驻留于媒体上且能被程序读出，它包括用以促使计算机创建表示网络的系统对象模型数据库的指令，该系统对象模型数据库支持完全不同的网络脆弱性分析程序的信息数据需求。一种计算机程序促使计算机从该系统对象模型数据库只输出所需的数据到每个相应的网络脆弱性分析程序，并利用每个网络脆弱性分析程序分析该网络以从每个程序产生数据结果。结果存储于数据事实库内的公共系统模型数据库。该计算机程序还创建指令以促使计算机应用面向目标的模糊逻辑决策规则到数据事实库以确定网络的脆弱性姿态。

一种数据处理系统评估网络的安全脆弱性，包括用于分析网络的多个完全不同的网络脆弱性分析程序。系统对象模型数据库表示将被分析的网络，而且支持网络脆弱性分析程序的信息数据需求。应用编程接口输入该网络的系统对象模型数据库到网络脆弱性分析程序。过滤器与该应用编程接口和每个相应的网络脆弱性分析程序相关，用于从系统对象模型数据库过滤数据并只输入所需的数据。

数据事实库存储和分析网络和公共系统模型数据库之后从各个网络脆弱性分析程序获得的结果，而模糊逻辑处理器通过利用多个模糊专家规则应用面向目标的模糊逻辑决策规则到事实数据库，用于合并来自网络脆弱性分析程序的结果以及确定网络的脆弱性姿态。

附图说明

下面通过举例参考附图详细描述本发明，其中：

图 1 是网络原理框图，示出了在网络中频繁发现问题的位置；

图 2 是网络的另一原理框图，示出了由本发明的系统和方法定位的识别脆弱性；

图 3 是本发明的系统和方法的总体结构的另一框图，示意了与网络模型数据库关联使用的过滤器；

图 4 是示意了模糊逻辑分析的本发明结构的另一原理框图；

图 5 是示意了本发明的数据处理系统和方法的高级体系结构组件

的另一原理框图；

图 6 是本发明的数据处理系统的另一高级原理框图；

图 7 是建模网络为映像的图形用户接口的例子；

图 8A 和 8B 是在系统对象模型数据库的建立中提供数据分解的开放窗口；

图 9 是示意了网络模型的图形用户接口的例子；

图 10 是示意了用于网络安全姿态的各种报告选项的图形用户接口；

图 11 是在本发明的数据处理系统和方法中使用的面向对象的模糊逻辑处理的基本处理组件的框图；

图 12 是在本发明的数据处理系统和方法中使用的数据融合的原理框图；

图 13 是在本发明的数据处理系统和方法中使用的基于目标的例子的另一原理框图；

图 14 是在本发明的数据处理系统和方法的模糊逻辑处理中使用的基本处理步骤和组件的另一框图；

图 15 是在用于证据积累和模糊证据推理规则的故障树分析 (DPLf) 中使用的基本组件的框图；

图 16 是示意对象/类分层结构的框图；

图 17 是示意本发明的系统类图的框图。

具体实施方式

图 1 示意了常规网络 100 的例子，它包括与外部路由器 104 相连的内部服务器 102、通信网络 105 以及防火墙 106。内部路由器 108 与防火墙 106、分支机构 107 相连，还与内部 LAN 网络部件 110 和远程访问服务器 112 及远程用户 114 相连。

利用图 1 的例子，在网络上经常出现的问题包括主机（如内部服务器 102）运行了不必要的业务，例如拒绝服务和匿名 FTP 或配置不当的 web 服务器，web 服务器可以为内部服务器，例如 CGI 脚本、匿

名 FTP 和 SMTP。内部 LAN 110 可包括没有打补丁的、过时的、脆弱的或缺省配置的软件和固件以及易攻破的口令。LAN 也可包括不当的输出文件共享服务,如 NetWare 文件服务和 NetBIOS。内部 LAN 110 还可包括配置不当或未打补丁的 Windows NT 服务器,以及由缺乏综合策略、程序、标准和原则导致的问题。远程访问服务器 112 可以有不提供安全保证的远程访问点,而外部路由器 104 通过下面的服务可能泄露信息,如 SNMP、SMIP、finger、roosers、SYSTAT、NETSTAT、TELNET banners、Windows NT TCP 139 SMB (服务消息块) 以及到非域名服务器主机的区域转换。它也可有不完整登录、监视和检测能力。分支机构 107 可能会有不适当的信任关系,如 RLOGIN、RSH 或 REXEC。防火墙 106 可能配置不当或有一个配置不当的路由器访问控制列表。

尽管这些网络问题只是在网络 100 找到的常见例子,本领域的技术人员知道还可能出现其它问题。

本发明的系统和方法使得能确定网络系统的脆弱性。数据处理系统和方法的软件可位于图 2 所示的用户终端 120,图 2 示意了在内部 LAN 110 连接的节点 122 所确定的脆弱性。为描述起见,本发明的数据处理系统和方法可称为网络脆弱性分析工具(NVT),即,用户用以确定网络脆弱性和风险的工具。

构成 NVT 的数据处理系统可装载于运行 Windows NT 的 Pentium PC 平台上。这种类型的平台可提供低成本的解决方案而且支持各种各样的评估工具,在通篇的描述中也称之为网络脆弱性评估或风险分析程序。这些网络脆弱性分析程序典型地为安全工程师所知晓的标准 COTS/GOTS 程序,而且包括 HP Open View,其允许网络自动发现或手工网络建模;Mitre 公司生产的 GOTS 网络系统分析工具 ANSSR (网络系统安全风险分析)允许被动数据收集和损失的单个出现。还可使用作为 RAM (风险评估模型)为大家熟知的 NSA 的风险评估方法,并可用 DPL-f 决策支持编程语言实现。RAM 还允许用于事件树逻辑的被动数据收集,优化任务列表以及允许具有多种风险/服务的数

学模型。它在整个时间过程是基于事件的。

DPL（决策编程语言）是促进复杂决策建模的决策支持软件包。它允许用户结合不确定性和灵活性到决策过程中。DPL 为建立模型提供了图形接口并对该模型执行分析。DPL-f 包含嵌入到 DPL 的功能并为故障树建立提供图形接口。这种特征使得建模人员能创建故障树并将它们结合到 DPL 模型中。DPL-f 还包含唯一分析工具。这些工具包括明确计算故障树中任何事件的概率以及执行故障树特定类型的灵敏度分析的能力。DPL-f 提供了用于结合时间序列到模型的接口。这使得建模人员能解释资产贬值、资产增值或其它时间-方位量而不用改变模型的结构。DPL-f 为 RAM 提供附加的能力，用于快速故障树建立、嵌入式故障树库、专家意见生成系统、割集（cut set）的列举和排序以及随时间过去的风险的图形描绘。

由因特网安全系统公司（ISS）开发的 ISS 因特网扫描器允许主动数据收集并扫描网络的主机、服务器、防火墙和路由器，以及评估符合网络、操作系统以及软件应用的安全和策略。它允许及时快照和计算机网络一致性报告。这些程序为本发明的 NVT 允许综合的完全不同的网络脆弱性分析程序。

NVT 基于知识征求框架，其结合了网络拓扑的图形描述。这种拓扑用于捕获网络属性并接着用于安全脆弱性分析。图形用户接口还用于提高网络模型的准确性。

根据本发明，NVT 的系统和方法自动映射现有网络而且能在如图 7 所示的图形用户接口上显示现有网络为一个模型。例如，HP Open View 可图形化描绘网络拓扑。一旦软件已经给出网络的缺省路由器的 IP 地址，本发明的 NVT 可使用 Open View 并搜索计算机和与该网络相连的其它设备。NVT 执行主动搜索，Ping 网络上可能的 IP 地址，并添加它接收的任何响应信息到其网络映像。NVT 还提供手控方法以绘制建议的具有所示图形用户接口的网络以支持拖放（drag and drop）。可定义系统体系结构，包括用于可选设计或节点编辑的安全关键信息以提供所需的附加细节以准备完整的逻辑网络规划。用户还

可通过使用子网图标在图上表示整个网络。

如图 16 和 17 的例子所示，当完成网络系统的描述时，NVT 以对象/分层结构表示和存储该描述，这将在下面解释。单个拓扑的系统对象模型支持完全不同的网络脆弱性分析程序（工具）的信息数据需求。这些结果的模糊逻辑处理允许修正来自程序的结果为有结合力的脆弱性/风险评估以获得网络的脆弱性姿态，如图 10 的图形用户接口所示。系统的单个表示简化了使用多种工具并取消了冗余数据输入。它还提供了用于定位对于给定脆弱性评估工具和未来知识协商能力的不完全数据的问题。

图 3 在 130 示意了本发明的总体网络虚拟化工具（NVT）、数据处理系统的例子，在此，三个网络脆弱性分析程序（工具）示意为 ANSSR 132，ISS 因特网扫描器 134 和 RAM 136。本发明的系统和方法创建系统对象模型数据库（网络模型数据库）138，它表示网络而且支持网络脆弱性分析程序的信息数据需求。系统对象模型数据库 138 表示所评估的系统或设计的单个表示，而且定位网络的单个内部表示的需要以提供数据给网络脆弱性分析程序。

该模型 138 使用面向对象（OO）的方法以类分层结构提供一个扩展组件的集合，该类分层结构可组合用以表示网络。类分层结构提供了定义具有共用公共特性的组件的方法，同时保持区别于其它组件的特性。除了隐含的分层结构关系，面向对象的技术提供了封装机制，其中对象可包含对任何对象（包括其本身）的引用。这就提供了用于表示任何物理或逻辑实体的灵活机制。同时，面向对象的表示自身具有准备好修改和扩展以及理想地用于每天都会出现变化和新技术的信息安全保证领域。

如图 3 所示，过滤器 140 与每个网络脆弱性分析程序 132、134、136 关联而且只允许相应的网络脆弱性分析程序所需的数据输出到该工具（程序）。过滤器为 C++ 基类，能提供一组虚拟方法以允许数据在 NVT 系统和程序之间移动。过滤器还为 NVT 提供一种方法以控制工具的执行和完成工具所需数据。NVT 将每个工具视为过滤器，调用

过滤器内的适当方法以执行期望的任务，包括初始化、运行、输入数据和输出数据。每个工具可有具体的过滤器子类，而且提供专用于该工具的方法以定义每个方法，同时能为 NVT 提供通用的和定义明确的编程接口（API）。这使得所有工具在 NVT 内能得到相同处理，使得不用改变任何现有 NVT 代码就能添加和卸载工具。

利用过滤器技术在 DPL-f 和 NVT 之间建立通信是简单明了的。DPL-f 过滤器的任务是建立和繁殖故障树的细节问题。作为分析工具，故障树能表示网络中的节点为已出现的，而且为诸如拒绝服务、数据丢失和数据泄露等事件提供概率值。实际上，DPL-f 可用作最终结果工具。

接着利用每个网络脆弱性分析程序分析网络以从每个程序产生数据结果。相互关联这些数据结果以确定网络的安全姿态。网络验证可通过下面将讨论的本发明的模糊逻辑处理发生，而且系统 GUI 可为用户显示的输入。

网络的概观通过自动网络发现或手工输入 144（如通过 HP Open View）创建为模型 142，而且适当的过滤器 146 允许系统 GUI 148 经由适当的数据输入 150 显示图 7 所示的网络模型给用户显示 152。利用下面将详细描述地插件程序或模糊规则集，还可能具有风险 GUI 154 以虚拟地评估风险脆弱性、风险/脆弱性报告的日志 156、作为部分 GUI 148 一部分的风险评估 158，所有这些都通过网络验证 160。任何不完全的数据分解 161 也可得以处理。

图 4 示意了类似于图 3 的高级框图，示出了可建立的系统对象模型数据库 138，并结合综合应用编程接口 162 一同工作以允许输入数据到各种工具 164，这些工具示意为能产生总体系统结果数据库的建模工具、发现工具和信息分析工具。应用编程接口 168 和图形用户接口 170 与模型数据库 138 一道工作。评价/评估管理器 172（管理员）协同应用编程接口（API）174 和图形用户接口（GUI）176 工作以使数据结果与模糊逻辑处理相互关联，如虚线 178 所示，包括专家关联 180 及模糊推理和证据推理 182 以便为关联结果产生脆弱性结果 184

和图形用户接口 (GUI) 186。尽管图 4 表示的高级模型示出了不同组件的例子, 但只有一种类型的高级组件的一个例子可用于本发明的 NVT 系统和方法。

图 5 和 6 示意了其它高级模型的例子, 其中示出了数据源 200(图 5) 的基本组件和处理步骤, 以及系统画面 202、per 工具分析 204、多工具分析 206、工具-专家分析 208 以及报告媒体 210。工具-专家分析 208 可包括 DPL-f 208a, 作为数据事实库中的模糊逻辑处理的一部分, 并使用 CERT 注解 208b 和专家系统 208c 用于专家关联。可生成的报告包括在图形用户接口上输出的图标、文本、EXCEL 电子表格、Access 和配置, 这是本领域的技术人员所了解的。图 6 也示意了类似于图 5 的另一高级模型, 其中用于形成完整系统对象模型和模糊逻辑处理的工具可包括单独的工具处理和多工具关联。

图 7-10 详细示意了图形用户接口 220, 它可包含于计算机屏幕而且用于与 NVT 交互并确定网络的脆弱性姿态。如图所示, 图形用户接口 220 为标准类型的 WindowTM 接口。系统设计窗口 222 允许显示构成网络图的网络图标 224, 网络图表示网络中包含的不同网络单元和节点的关系。相应于网络单元是如何与网络互连的, 对应的网络图标 224 以一种方案被联接在一起。如图 7 所示, 网络单元可以经由连接线 226 连结在一起, 连接线 226 示出了实际的网络单元和节点间存在的互连。系统设计窗口 222 在左侧示出了具有两个节点的网络间视图 230, 而在窗口的右侧示出了网络视图 232 以示意该网络模型的映像。管理员窗口 234 被打开并显示网络单元的属性。

选择数据敏感度的弹出窗口 (方框) 240 是用户可选择的, 通过菜单选项选择的网络单元 (图 8A), 而且具有用于选择网络单元灵敏度的用户选择的数据项。在任何节点上 (在图 8A 所示的例子中的节点 1) 的数据灵敏度可以选择为公开 (unclassified)、敏感 (sensitive)、机密 (confidential)、极机密 (secret)、受限机密 (restricted)、绝密 (top secret), 并有 “OK”、“RANDOM”、“DEFAULT” 三个按钮。

选择节点配置编辑弹出窗口（方框）250 在图 8B 示意，它具有用户可选择的脆弱性简表（profile）用于选择网络单元或节点的脆弱性简表。图 9 还示出了带有中心集线器和互连节点的网络模型图。有可能用户可编辑管理员窗口 234 入口，这也使得能通过选择适当的按钮发生网络发现。自然地，如果需要可以选择和移动网络图标以编辑和设计选择对象。

通过系统建立了安全姿态后，表示高风险网络单元（集线器 252）的图标可改变颜色，如红色。其它选择的图标可变为黄色以指示风险较低的节点，如图 7 和 9 中所示的 HP4 节点 254。有可能该网络的节点或部分周围的阴影区可以被涂以红色或黄色指示更高的风险脆弱性。也有可能连接线变为红色或黄色以指示单元之间的不良连接。

图 10 示意了脆弱性姿态窗口 270，用于显示指示脆弱的网络单元和图标的用户可读取图标。整个系统模型示出为部分开放系统设计窗口。然而，示意了电子表格 272 和具有风险评估滑动条的 NVT 风险评估图表 274。还示意了风险分析窗口 276，其示出了头 5 个风险分析单元。

图 16 详细示意了一个类分层结构，具有作为公用属性和私有属性的类名 280、资源 286 的聚集 282 和关联 284 以及具有归纳结果 290 的目标 288。图 17 示意了各种以框图区分的组件的系统类图的例子。自然，图 17 只是本领域的技术人员知道的一个系统类图，它是可用于该本发明的系统和方法的一个例子。

现在详细参考图 11-15，这些附图示意了面向目标的模糊逻辑决策的执行。如图 11 所示，系统模型数据库 138 和来自各个的网络脆弱性分析程序的结果 300 利用应用编程接口和专家关联结合在一起，以通过数据模糊化形成数据事实库 302。面向目标的模糊逻辑决策规则通过模糊推理网络规则 304 和模糊证据推理规则 306 运算，以基于预定的目标 308 确定网络的安全姿态。

模糊逻辑处理使用数据融合、证据推理和推理网络技术。本领域的技术人员知道，证据推理为一种收集支持和驳斥给定假设的事实的

技术。该结果就是具有某种置信程度的假设的肯定或否定。本发明的模糊逻辑处理采用证据推理以从系统和工具为每个准则的搜索中积累证据，从而合并系统评估数据为单一参考点，合并系统的一致性为特定准则。通过提供一组融合规则集，系统就能抑制融合问题并简化搜索库。证据推理之前已用于执行级别 1 多探测器数据融合，而且是模糊专家系统中的公共全局推理技术，如本领域技术人员所知道的由 NASA 开发的模糊 CLIPS 的系统类型。其结果为一组模糊证据规则，其目的是为给定的一组需求积累证据。这就解决了专家关联的潜在的不一致、模棱两可和冗余数据，即使数据不完善也可利用可用数据得出结论。

结果的精确性视可用数据的数量和质量而定，而且在应用模糊逻辑处理之前必须对可用数据执行附加的改进，这也保持了数据的概率论的性质。这种改进使用推理网络并提供利用直观推断法提供有关概率的推理方法，从而无须大量的先验知识。目标和潜在的安全规格之间的关系促使相互间交叉结合。本领域的技术人员知道，模糊 CLIPS 利用模糊事实，它可假定 0 和 1 之间的任意值。结果可视为由 0 和 1 为界的连续函数的二维曲线。

数据融合利用系统对象数据库、数据结果数据事实库。智能数据融合是基于多级、多学科的信息处理，以从多个智能源（可能是多个智能学科）产生信息的综合，以生成有关实体（其状态、能力和强加的威胁）的特定和全面的、统一的数据。数据融合基于可用的输入提供信息。智能数据融合处理典型地分为 4 个级别（如表 1 所述）。

表 1 智能数据融合过程的级别和目的

数据融合级别		描述
1	对象改进	• 将数据转化为一致的推理框架 • 及时改进和扩展，估计对象位置、运动学或属性 • 为对象分配数据以允许应用估计处理 • 改进对象识别的估计
2	状态改进	• 开发环境语境中的对象和事件之间的当前关系的描述 • 符号、推理过程，由此固定和被跟踪的实体、事件及活动的分配与运行问题的语境中的环境和执行数据相关联
3	威胁改进	• 设想当前的“状态”为未来的情形并得出关于威胁、脆弱性和运行时机的推理
4	过程改进	• 监测处理性能以便为实时控制和长期的改进提供信息 • 确定需要什么信息以改进多级融合产品 • 确定源特定数据需求以收集所需信息 • 分配和引导资源以实现任务目标

前面指出，NVT 结合来自多个来源的多种类型的数据与其它上下文信息，以形成网络化系统的安全姿态的综合概观。NVT 为用户提供给定系统或系统设计的脆弱性姿态的简单表述并使它们为改进和改善系统或系统设计的目的能执行功能、性能和防范交易的“假定方案（what if）”分析。

在计算机安全工程中，探测器为各种脆弱性评估和风险分析工具，它与 GUI 一起从用户收集所需的信息。从这些工具得到的输出在来自不同厂商的各种格式中采用定性的和定量的数据形式。对于计算机安

全过程来说，所研究的对象是网络（计算系统）中的节点，即，包括硬件、软件和数据资产。所研究的状态是评估计算机网络段的安全系统中的弱点，这些弱点可被利用以引起损害或秘密、完整性或可用性的损失。

评估计算机系统面临的风险涉及评估面临的威胁、它们出现（非法利用）的可能性以及预期的损失（或损害）成本。最后，网络（计算系统）可基于成本-效益分析的结果改进。这就需要有关适合于特定脆弱性和它们的成本的保护措施（控制或对策）的信息。成本效益分析寻求确定使用控制或对抗的成本是否更低，或是否接受预期的成本损失。这就导致开发一种安全策略来改进计算机网络系统的安全。

表 2 包含利用对应表 1 中 4 个级别的 4 个处理级别，用于本发明可使用的计算机安全工程的这种数据融合处理的第一划分的例子。如图 12 所示，这个过程的输入将由对象模型数据库 138、来自个别的工具 132、134、136 的结果以及其它语境信息组成。不同数据融合级别 1-4 通常在 320、322、324 和 326 指示。

表 2 用于计算机安全风险分析的数据融合的初始处理级别

数据融合级别		描述
1	节点数据改进	• 将数据转化为一致的推理框架 • 改进网络节点级的数据（用于计算机安全数据融合的对象） • 来自多个关联的（分配给适当节点）或可能在每个节点结合的工具的数据 • 改进对象识别的估计-网络节点（工作站）为复合系统，由 OS、关键应用、数据库和数据组成 • 在此级别的脆弱性分析还未构成状态评估
2	网络段改进	• 在网络段级别（复合系统级别）改进状态 • 开发该环境（网络段）语境中的对象（节点）之间的当前关系的描述 • 符号化、推理过程，由此有关实体（节点、网络段）的信息和环境与有关计算机安全目标、需求的证据相关联 • 在网络段级别结合工具结果 • 所研究的状态为网络段的脆弱性或暴露的评估
3	风险改进	• 改进计算机系统内的暴露和它们的潜在危害（风险） • 设想当前的“状态”（计算机网络系统的状态）为未来的情形并得出关于威胁、脆弱性和运行时机的推理 • 基于脆弱性、利害关系、语境、成本、威胁 • 用降低一个或多个脆弱性的控制识别改进系统设计 • 基于对策、组件、成本 • 确定需要什么信息来改进多级融合产品 • 促进系统的长期的改善

虽然在本发明中使用的数据融合提供了用于定位从多个脆弱性评

估和风险分析工具合并结果的问题的总体框架，但专家系统、推理网络和证据推理用于实现融合概念和合并工具结果。模糊决策技术，尤其是模糊专家系统的灵活性提供了定位这些问题的手段。模糊专家系统的主要好处是其使用和吸收来自多种来源的知识的能力。

模糊逻辑提供了用于从不精确、不确定或不可靠的知识中表示和推导的技术。类似于传统的专家系统，模糊专家系统能以 IF/THEN 规则的系统形式表示知识，在这些规则中前提、后果或二者是模糊而不是明确的。模糊逻辑用于确定模糊事实与这些规则的匹配程度，以及这种匹配影响规则的结论的程度。根据本发明，推理网络为启发式规则分层结构，它能传播概率而无需扩展的先验概率知识（例如，Bayesian 网络）。启发式规则可利用有关概率是如何传播的专家知识开发，允许用有限的先验概率知识得出结论。这导致低级的离散概率在高级结论中准确地被反映。低级事件的概率（如基于寿命的口令妥协的概率）需要成为在高级事件（口令的脆弱性）得出的任何结论的一部分。

NVT 的最初研究使用证据的积累来修改模糊-事实，并在当前系统所需的状态下表示这种变化。这种状态改变模糊-事实接着用于修改系统，而且新状态利用全局影响在无尽的周期中反馈到状态规则的变化中。模糊 CLIPS 允许定义模糊-事实类型，但每个类型只有一个事实将始终存在。因此，控制那个事实类型的每个规则实际上修改单个事实，导致证据的积累。

全局影响和证据积累已导致模糊 CLIPS 方法学，其定义表示不同脆弱性状态的模糊-事实。这些事实将使用全局影响和证据积累来获得反映经测试系统的脆弱性的最终值，即，证据推理。这种方法反映了模糊逻辑控制系统的意义明确的使用，限制该执行为有限数量的周期而不是允许它连续运行。FuzzyFusion™ 已由 Melbourne, Florida 的 Harris 公司开发，而且将使用这种方法从基于来自网络安全专家知识的规则中积累证据。特别是，FuzzyFusion™ 将应用证据推理作为一种技术，其中收集的知识支持或否定给定假设。该结果是具有一定置

信度的对假设的肯定或否定。

最初的知识提取已导致使用安全需求来积累证据，即系统满足需求的程度。这就证实了验证数据库（例如，AFCERTS）和验证安全需求的方法之间的强烈关联，导致使用数据库和需求作为积累证据的全局影响事实，如图 13 所示。这还示意了目标的粒度直接影响评估粒度的变化程度，即，评估将只能描述得象目标那样具体。证据的积累被视为面向目标的实现方法以获得结果，同时保持前向推理技术的使用，当前将称之为“基于目标的融合”。

在计算机安全中，模糊逻辑如何与合并工具结果应用的一个例子是使用来自 ANSSR 和 ISS 因特网扫描器的结果的结合，这两个工具当前用于 NVT 的一个方面内。工具的输出都是定量（ANSSR）和定性的（因特网扫描器）。模糊逻辑使得系统能在同一系统内表示这两种数据类型。接着，用公式表示初始假设，而且模糊逻辑用于收集证据以反对或支持该假设。

对这个例子来说，初始假设可以是在现有网络系统中审核无效。系统用户接着执行 ANSSR 和 ISS 因特网扫描器工具，如果 ANSSR 提供数量 90（100 范围内），那么审核是充分的。模糊逻辑允许 NVT 解释这种情况为对审核无效的初始假设的强烈否定的证据。如果因特网扫描器提供用户访问没有被审核的定性的数据，那么模糊逻辑将此解释为支持证据，它与来自 ANSSR 的证据结合。当这些工具运行结束时，用于审核的起作用的证据表示为单个模糊事实，它提供对审核实现程度的度量。

由 Melbourne, Florida 的 Harris 公司开发的 FuzzyFusionTM 是用于整理和合并 NVT 内应用脆弱性评估和风险分析工具的结果到统一报告中的工具。特别是，FuzzyFusionTM 开发用于实现级别 1 和 2 的融合，FuzzyFusionTM 是通过利用采用模糊 CLIPS 的模糊专家系统（面向的对象的模糊逻辑决策规则）实现的，模糊 CLIPS 结合了各种工具的输出、用户关心的有关系统风险和脆弱性、以及每个工具的结果的专家理解和这些结果是如何适应更大的信息系统安全画面的。因此，

NVT 用户获得给定计算机系统或系统设计的安全姿态的简单表述，而且能为功能、性能和防范交易执行“假定方案”分析。

图 14 示意了用于实现计算机安全工程的最初两个级别的数据融合的 NVT FuzzyFusion™ 组件结构。如图所示，建模安全专家的任务被分为离散的任务。专家关联（数据框架合并规则）、模糊推理网络规则以及模糊证据推理原则的分离定位了脆弱的专家系统和计算爆炸的问题。它还分离来自模糊/不一致的数据分解的低级数据关联和融合，以及合并结果为一个画面。这应导致模糊专家系统比一个大型的综合系统更容易维持。这种结构的单元在下面描述。

数据模糊化 310 将来自各个脆弱性评估和风险分析工具 132、134、136 的结果转换为模糊-事实，并随同公共系统模型（CSM）（即系统对象模型数据库 138）一起存储到该（模糊 CLIPS）事实库 302。各个工具结果（模糊化后）和 CSM 138 输出用于专家关联处理 310（数据框架合并规则）以分解系统信息和基于安全专家经验综合工具输出。专家意见可用于确定归因于低级事件的特定模糊值。

专家关联（数据框架合并规则）330 为模糊专家规则集合以执行节点级的数据改进（级别 1）或网络段的改进（级别 2）。这些规则利用来自安全工程师的专家经验关联和合并来自脆弱性评估和风险分析工具的（模糊化）输出。这些规则平衡了安全评估上的广泛经验以分解低级系统数据和工具结果。这些规则分解系统信息并综合系统输出。专家关联规则处理 330 还可转换来自 CSM 的低级数据和工具结果到高级结论中。例如，

如果用这些标志进行审计，
并且审计数据没有备份，
那么，审核是不可靠的

通过事实库 320 中的模糊-事实工作，级别 1 融合规则集可整理每个节点的脆弱性，结果产生网络中每个节点的脆弱性等级。这个等级

可输入回 NVT 用于显示。类似的，级别 2 融合规则集可整理每个网络段的脆弱性，结果产生每个网络段的脆弱性等级。这可再次输入回去用于显示。

这些数据接着受模糊推理网络规则处理 304 的控制。在应用模糊证据推理规则 304 之前有必要对可用数据执行附加的改进，同时保持数据的概率论的性质。这种改进将使用如本领域的技术人员知道的推理网络，这将提供使用启发式的有关概率推理的方法，从而无需大量的先验知识。

从系统级的观点来看，模糊证据推理规则 306 为模糊专家规则的集合以合并各个工具结果到更高级别的网络安全姿态评估中。这些规则提供了合并 CSM、工具结果、以及来自专家关联（数据框架合并规则）330 的结果到统一报告中的机制。这也使得无需处理来自专家关联中使用的前向联接专家系统的不完善和不一致的数据。

证据推理使用的技术中收集事实以支持和反对给定假设。该结果是具有置信程度的对假设的肯定或否定。FuzzyFusion™ 采用证据推理从公共系统模型和每个标准的工具结论中积累证据，从而合并计算机网络系统评估数据到单个参考点，合并系统的一致性为特定准则。通过为融合提供一组准则，NVT 限制了融合问题并缩小了搜索空间，在这之前称为基于目标的融合。该结果将是一组模糊证据规则，其唯一目的是为给定的一组需求积累证据。这解决了来自专家关联（数据框架合并规则）330 的潜在的不一致、模棱两可和冗余数据，即使数据是不完善的也能利用可用数据得出结论。显然，该结果的精确性视可用数据的数量和质量而定。

前面指出，模糊逻辑处理是面向目标的。证据积累处理 350 的目标可从安全需求数据库 352、计算机安全度量数据库 354 或脆弱性数据库 356（如 AFCERT 构成的数据库）导出。边界融合到预定目标限制了计算时间。FuzzyFusion™ 目标提供了获得 IA 度量的机制。

FuzzyFusion™ 处理相比传统实现方法有许多优点。明确的专家系统将需要非常大的知识库来包含必要的数据库，而且仍然存在数据不完

善和结果不一致的问题。Bayesian 和概率网络需要大量而且经常不可用的先验概率知识。算法解决方案不适合安全问题的概率性和启发式特性。

基于神经丛的专家系统，如模糊 CLIPS，忍受着因基于当前系统中大量的规则和事实的执行时间呈几何增长。这导致插入分析到子网。FuzzyFusion™ 将增加子网和缩放能力。每个子网的节点将计算为组，接着计算子网的各组。为每种分析类型分组规则为不同模型将减小神经丛网络的尺寸。还将缩短执行时间，这还将引入映射到 NVT 使用的网络模型的分析网络的可缩放方法。

如图 15 所示，其它可能的数据空间可包括威胁知识数据库 360、作为级别 3 融合一部分的成本数据库 362 和对策知识库 364、组件数据库 366 以及作为级别 4 融合一部分的成本数据库 368。

一种评估网络的安全脆弱性的方法和数据处理系统。建立系统对象模型数据库并支持完全不同的网络脆弱性分析程序的信息数据需求。只有来自表示网络的系统对象模型数据库的所需数据才被输入到该程序，该程序接着分析网络以产生来自每个程序的数据结果。这些数据结果存储在公共系统模型数据库中和数据事实库内。面向目标的模糊逻辑决策规则运用于确定网络的脆弱性姿态。

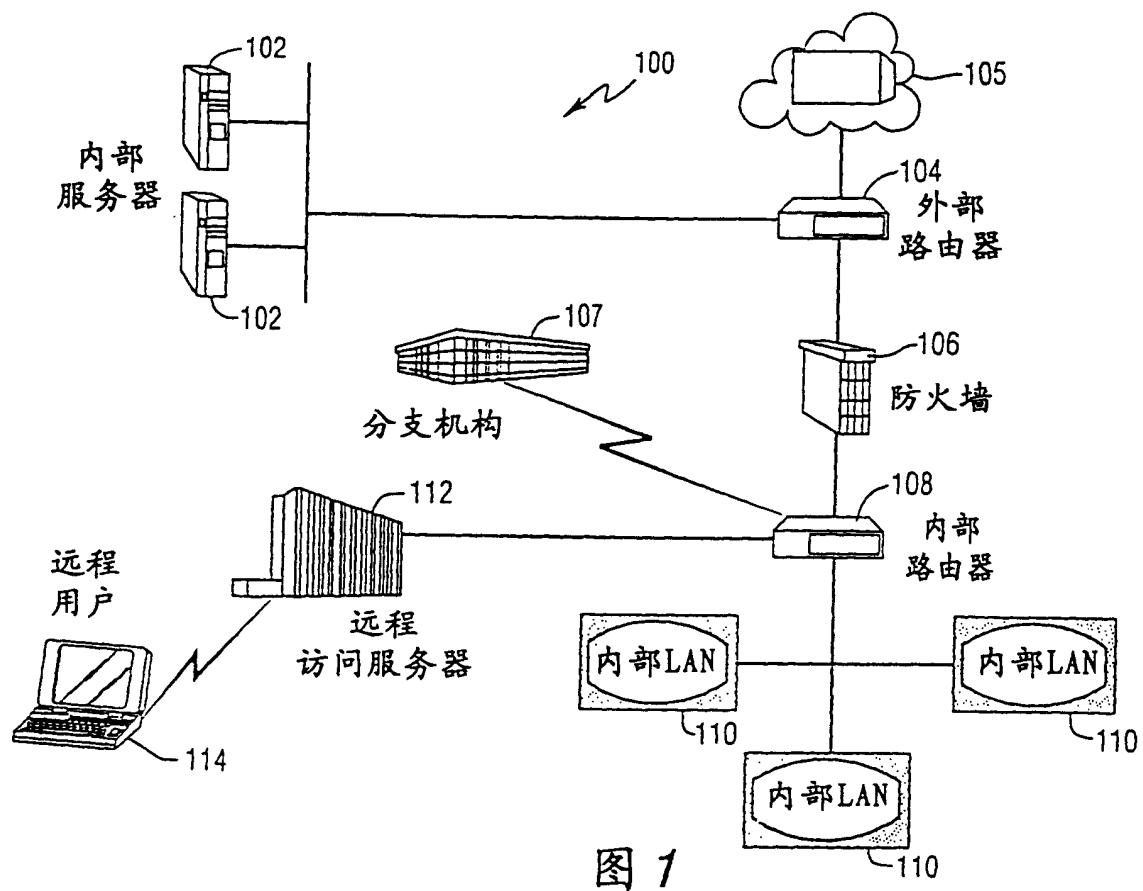


图 1

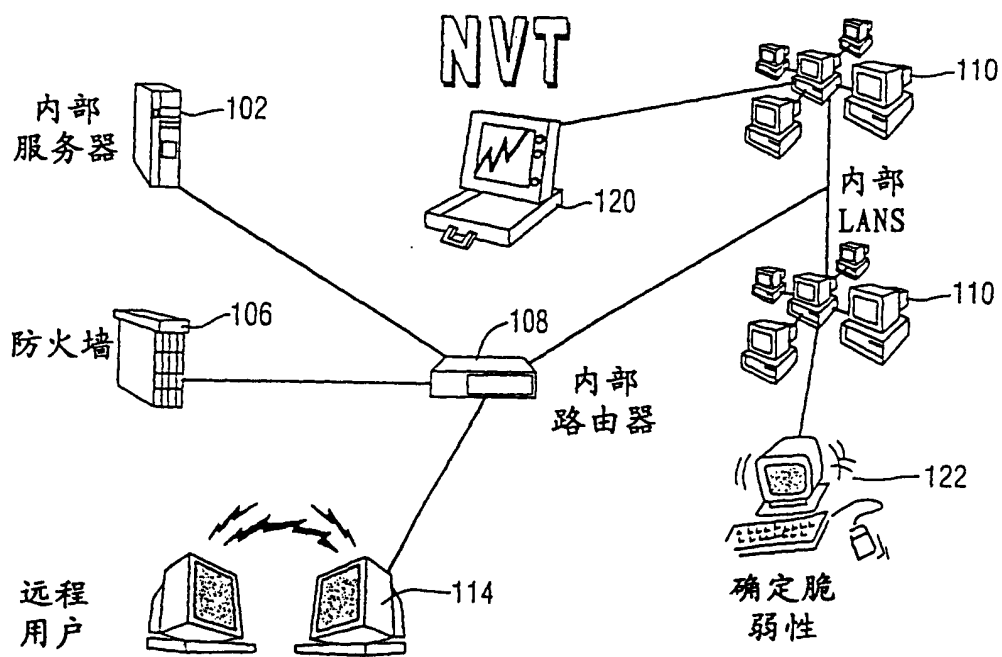
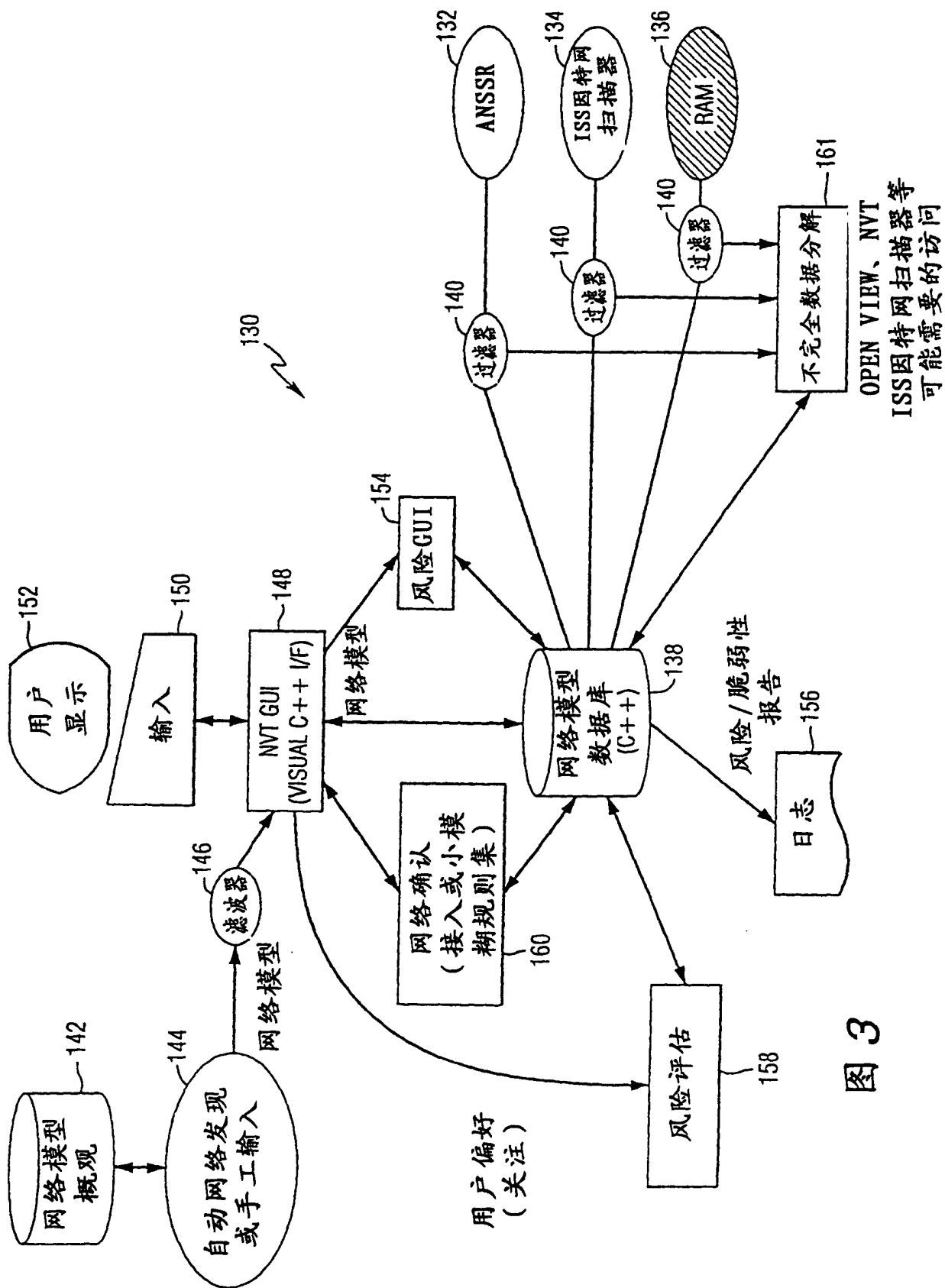


图 2



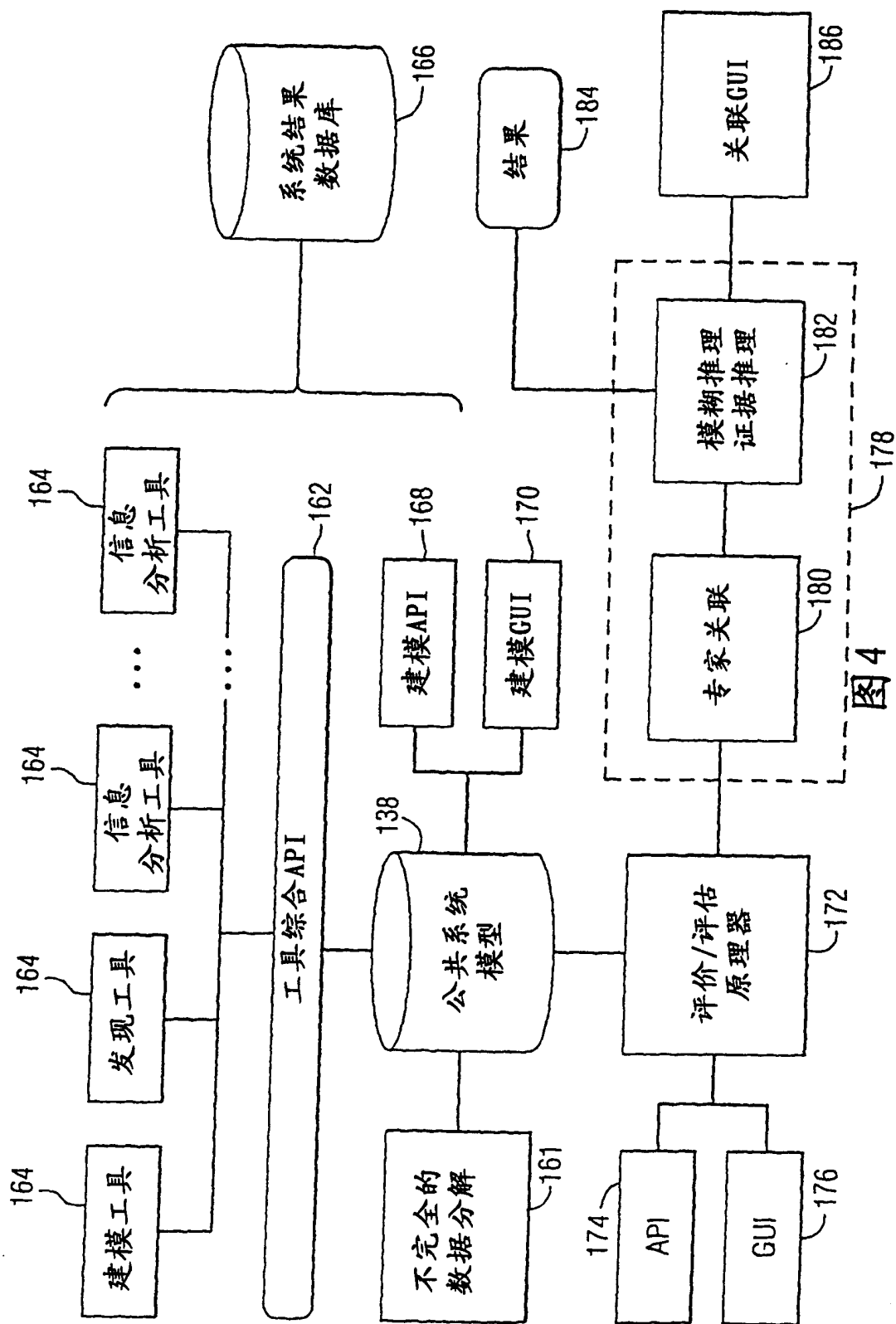
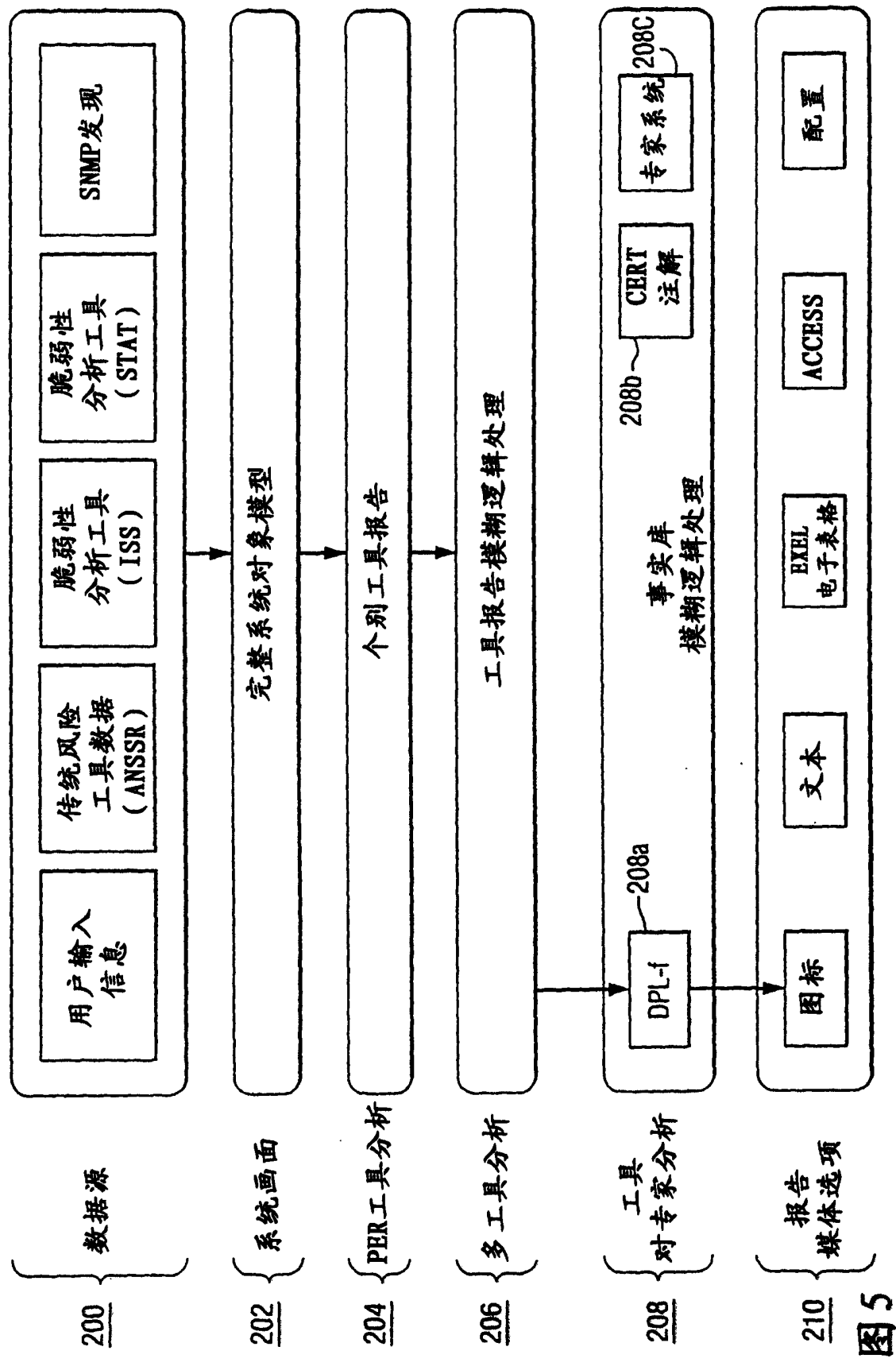


图 4



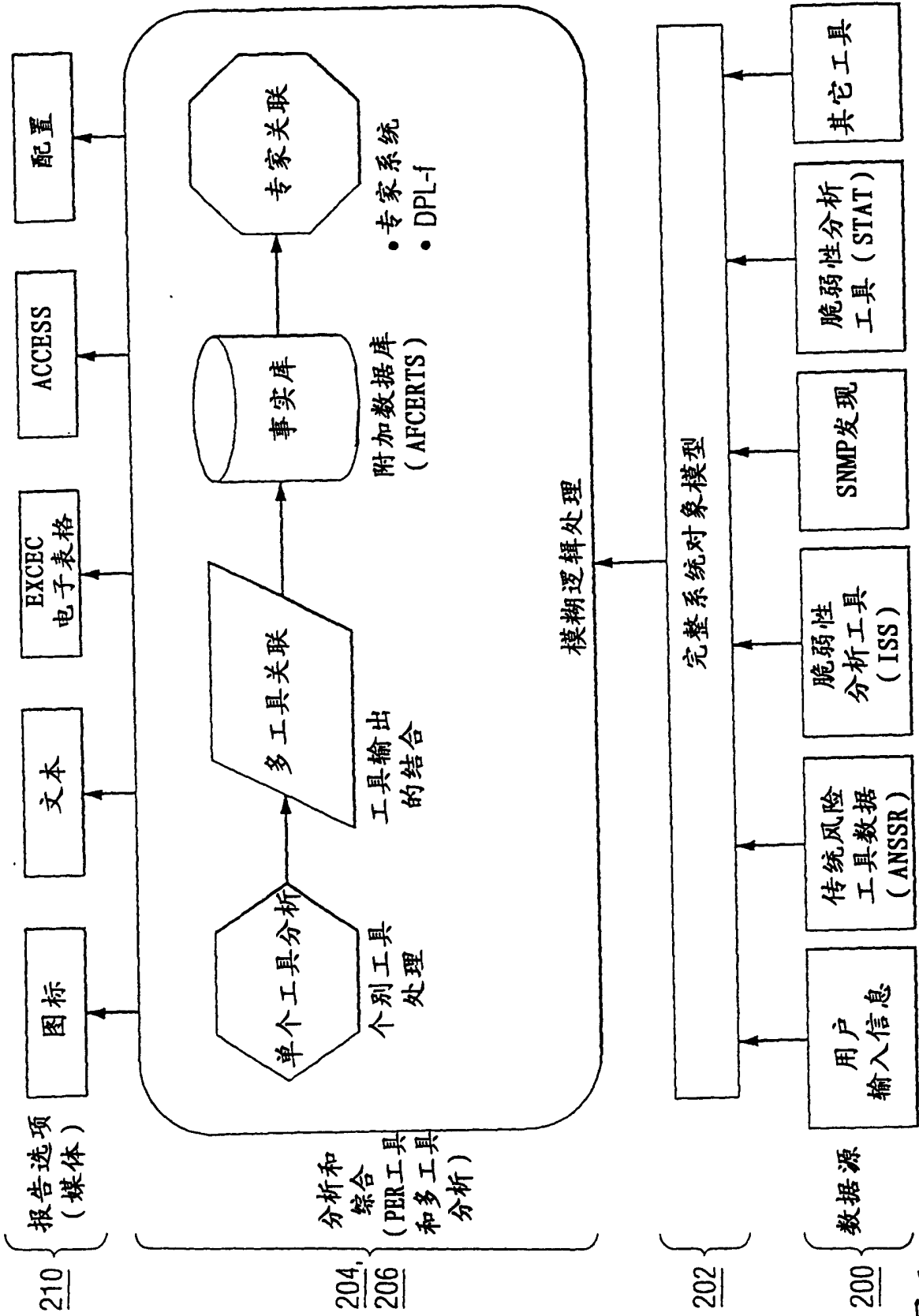
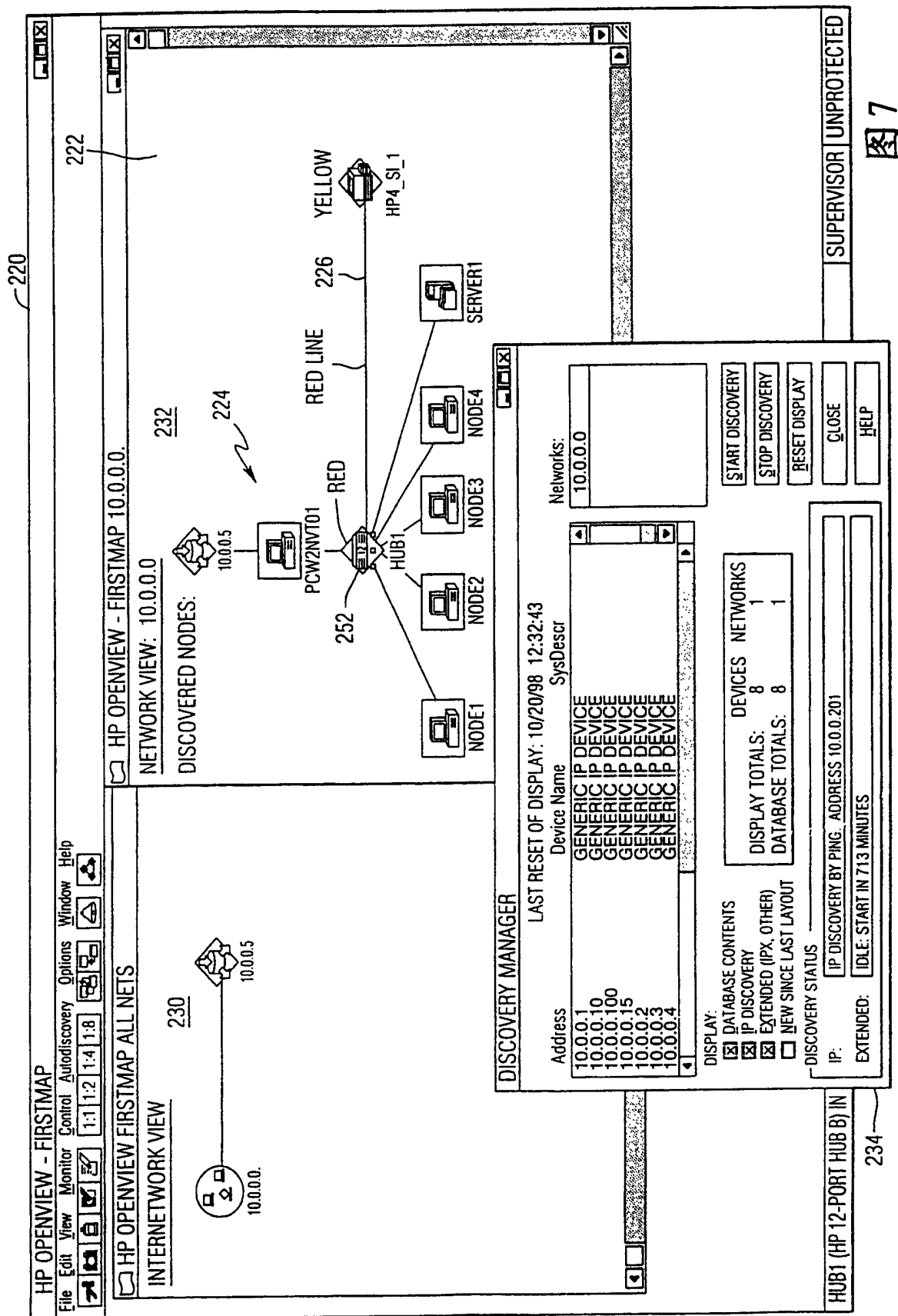


图6



240

SELECT DATA SENSITIVITY

SELECT THE SENSITIVITY FOR THE DATA ON
NODE 1

☐ UNCLASSIFIED

☐ SENSITIVE

☐ CONFIDENTIAL

☐ SECRET

☐ RESTRICTED SECRET

☐ TOP SECRET

OK

RANDOM

DEFAULT

图 8A

250

SELECT NODE CONFIGURATION

SELECT VULNERABILITY PROFILE FOR
NODE 1

RISK SEVERITY	HIGH	MEDIUM	LOW
Network Information	1	2	3
Network Access	4	5	6
Password Access	7	8	9
Root Access	10	11	12
User Access	13	14	15
User Info	16	17	18
Root Access Net	19	20	21
Denial of Service	22	23	24
Data Access	25	26	27
General	28	29	30
Resource Access	31	32	33
System Access	34	35	36
Data Corruption	37	38	39
System Information	40	41	42
Auditing	43	44	45
System Configuration	46	47	48
Remote Execution	49	50	51

OK

DEFAULT

SAVE DEFAULT

VULN TEST

图 8B

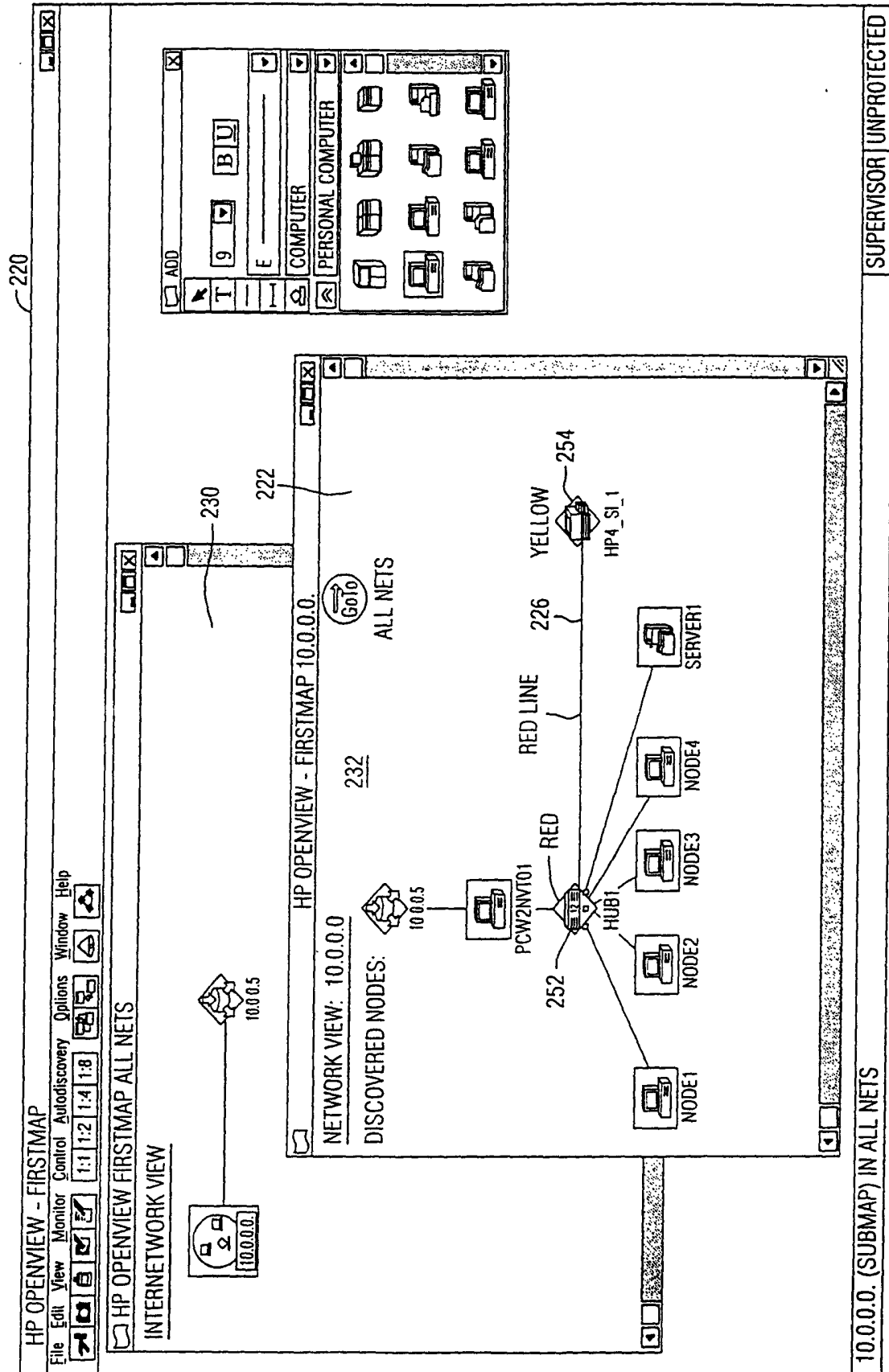


图 9

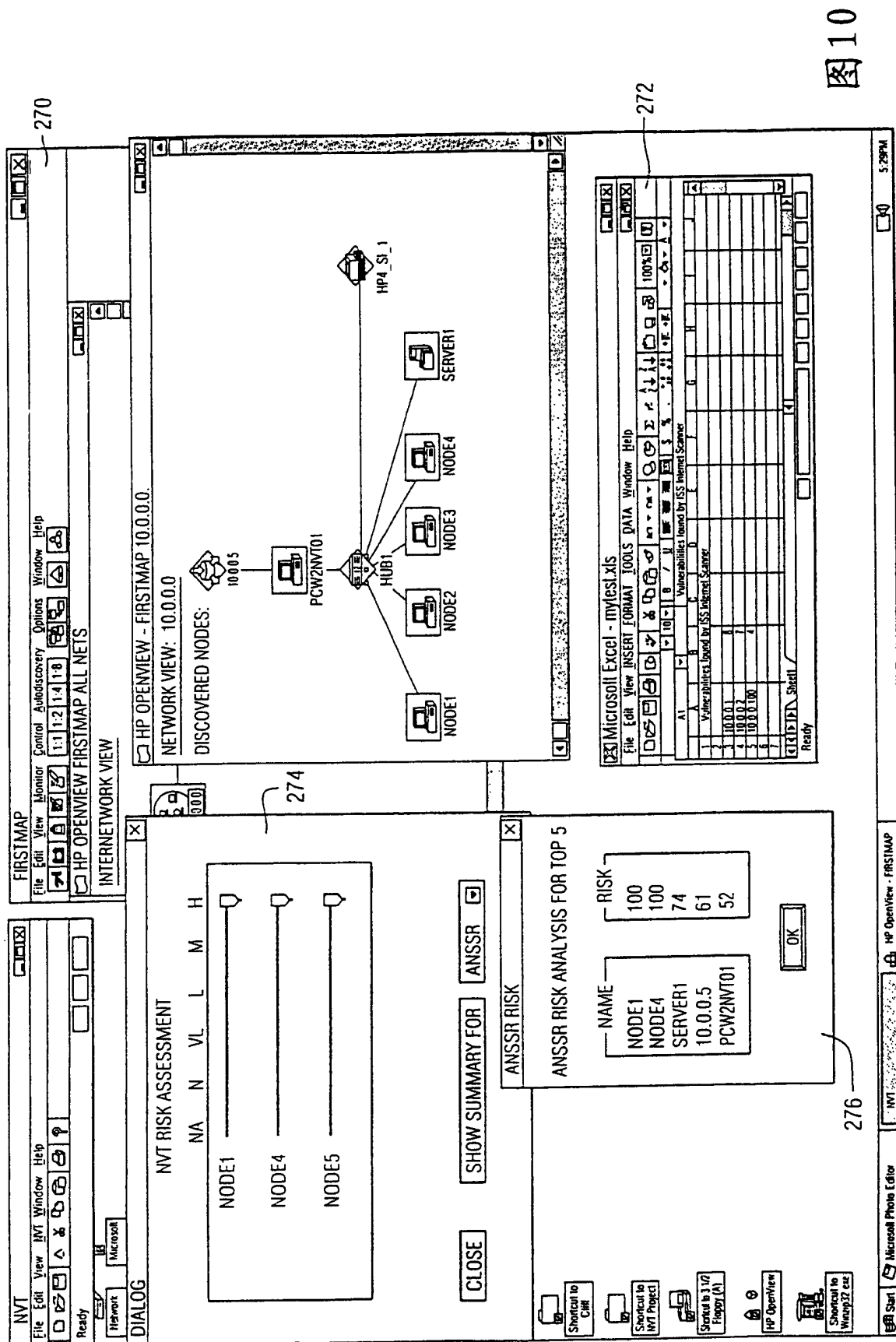


图10

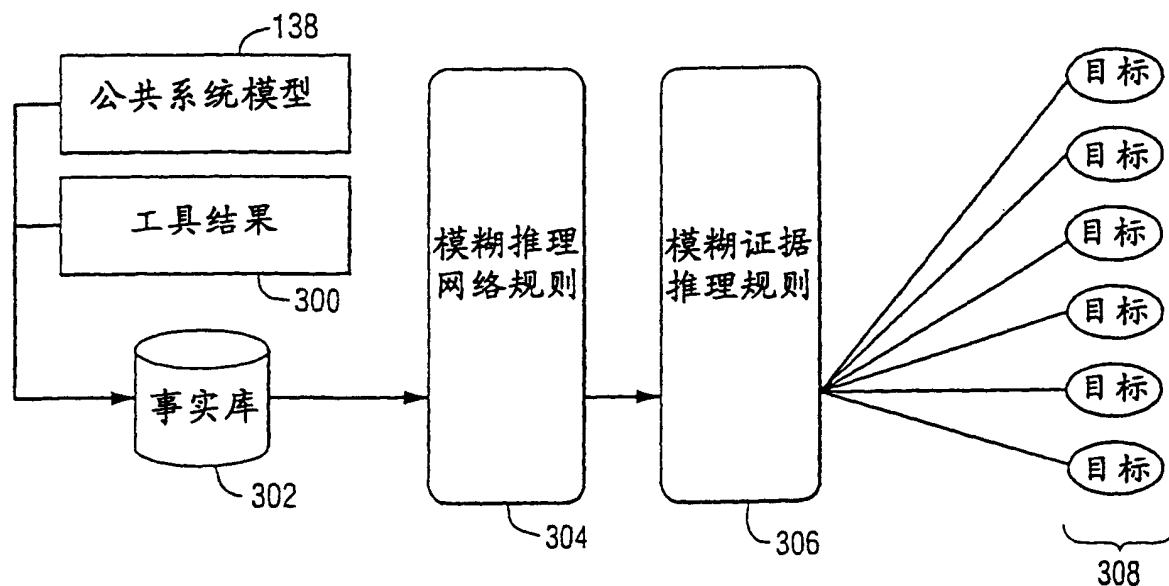


图 11

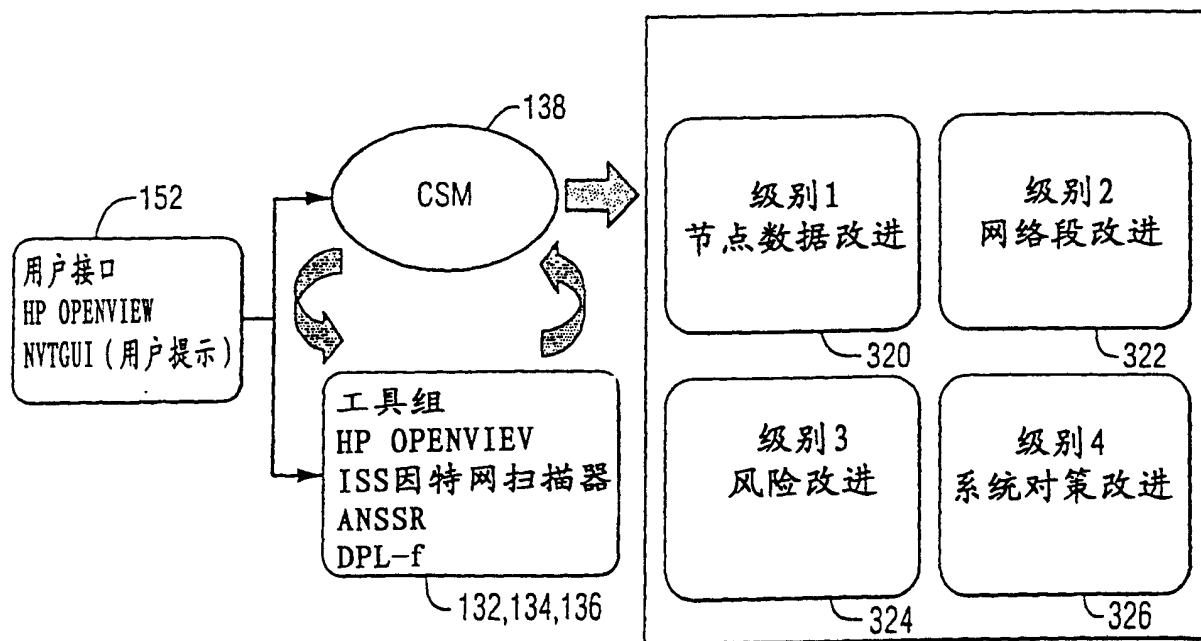


图 12

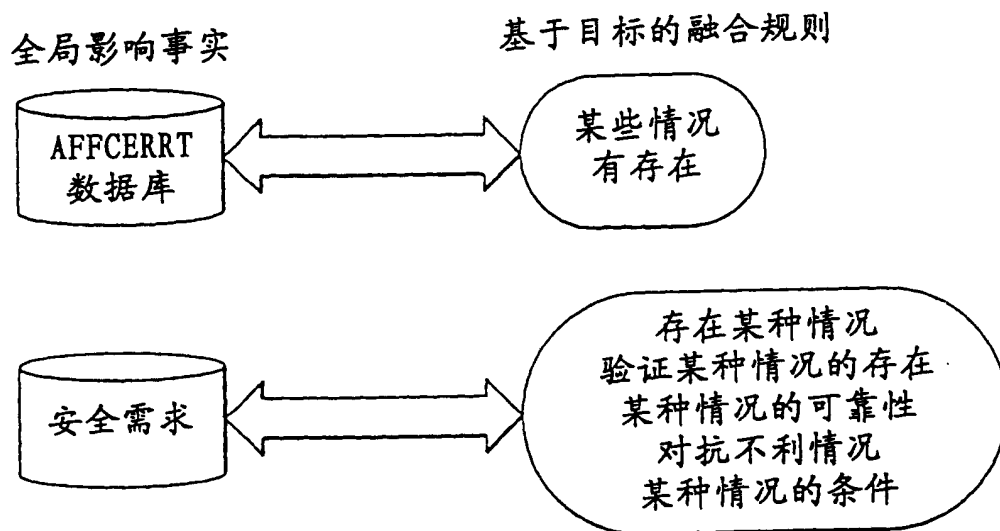


图 13

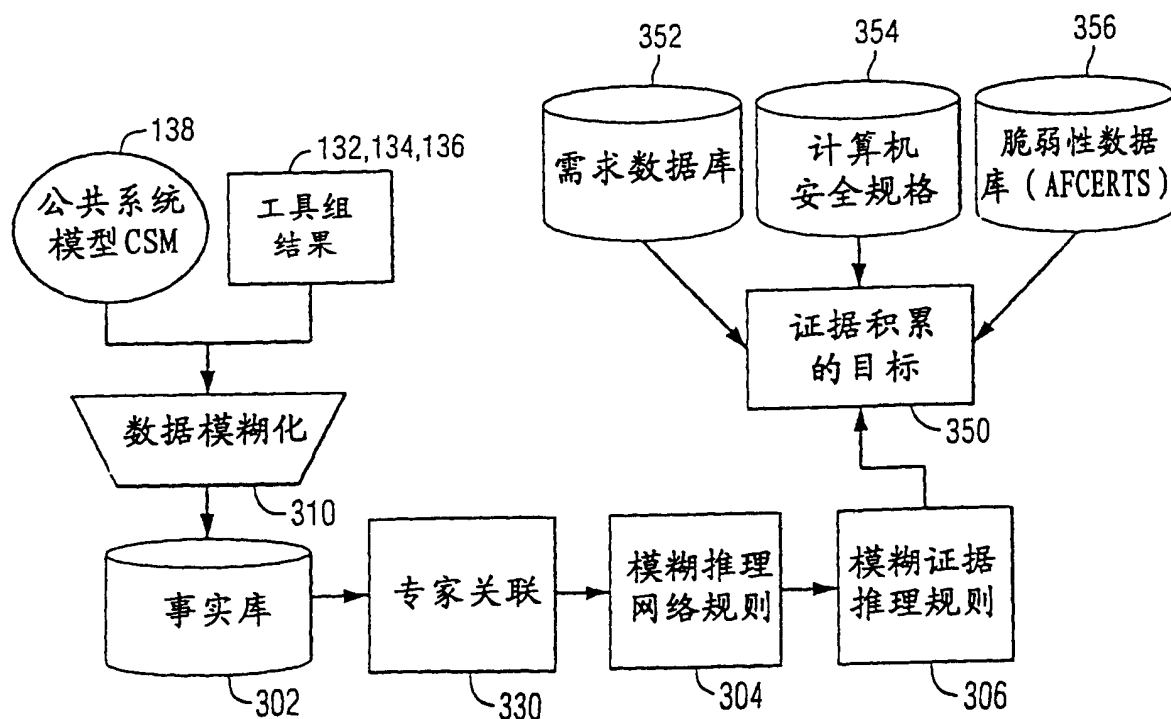


图 14

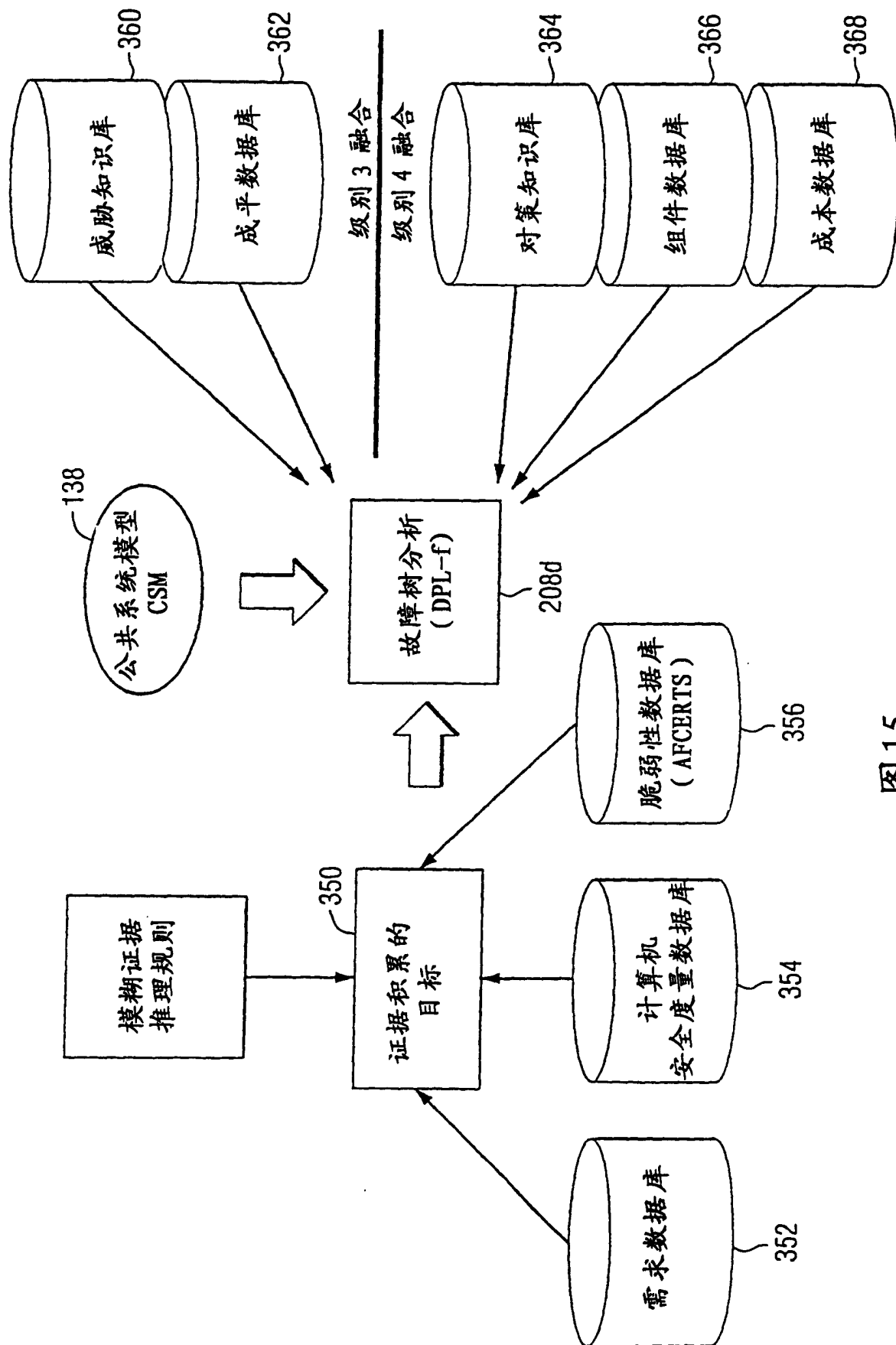


图15

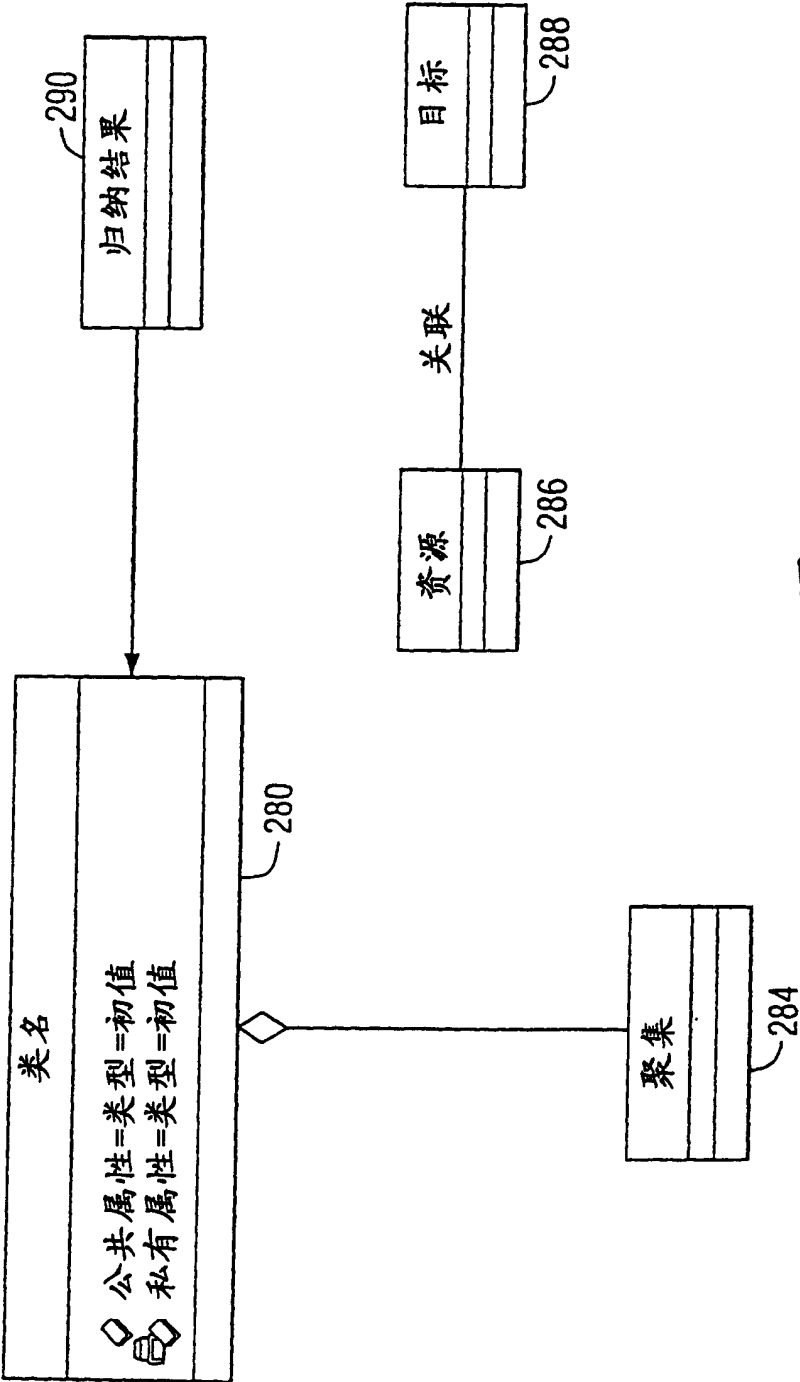
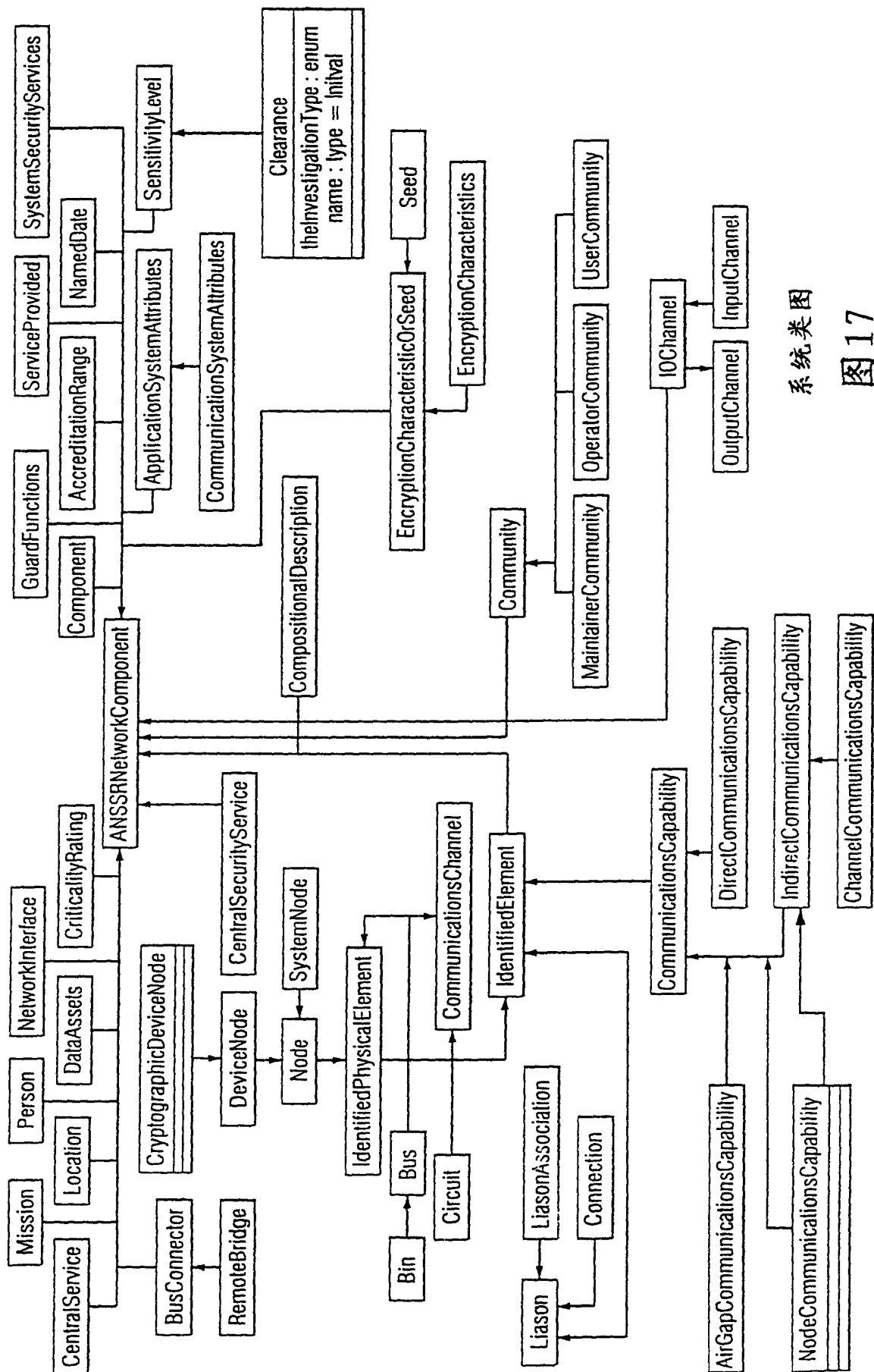


图16



系统类图

图 17