

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
31 October 2002 (31.10.2002)

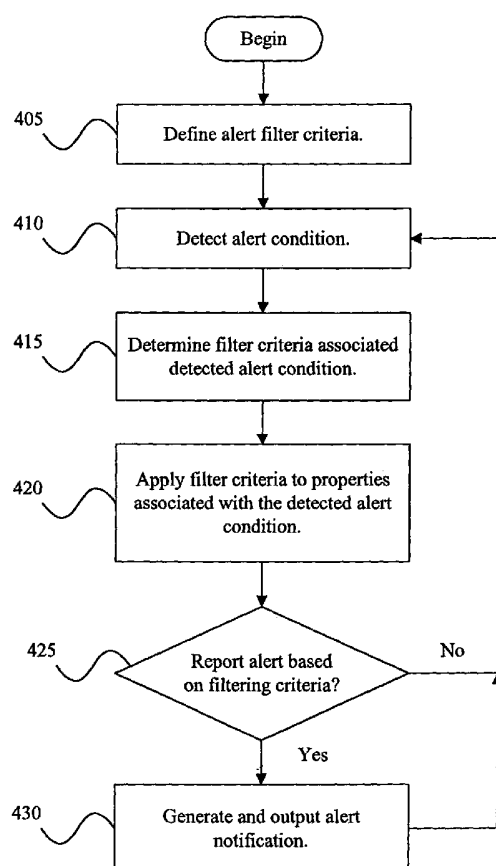
PCT

(10) International Publication Number  
**WO 02/086750 A1**

- (51) International Patent Classification<sup>7</sup>: **G06F 15/173**, G09G 5/00 (72) **Inventor: VINBER, Anders**; 160 Bayview Road, Plan-dome Manor, NY 11030 (US).
- (21) International Application Number: PCT/US02/06443 (74) **Agent: LECH, Robert, R.**; Calfee, Halter & Griswold LLP, 1650 Fifth Third Center, 21 East State Street, Columbus, OH 43215-4243 (US).
- (22) International Filing Date: 4 March 2002 (04.03.2002)
- (25) Filing Language: English (81) **Designated States (national)**: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.
- (26) Publication Language: English
- (30) **Priority Data**:  
60/273,044 2 March 2001 (02.03.2001) US  
09/949,101 7 September 2001 (07.09.2001) US
- (71) **Applicant: COMPUTER ASSOCIATES THINK, INC.** [US/US]; One Computer Associates Plaza, Islandia, NY 11749 (US). (84) **Designated States (regional)**: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) **Title:** SYSTEM AND METHOD FOR FILTERING MESSAGES BASED ON CONTEXT



(57) **Abstract:** A method for reporting alert conditions is disclosed which includes defining alert filter criteria (405), identifying an alert condition (410), analyzing one or more properties of the alert condition based on the alert filter criteria (420), and determining whether to report the alert condition (425). Systems and computer-readable storage media for reporting an alert condition are also disclosed.

WO 02/086750 A1



European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

**Published:**

— *with international search report*

## Method and Apparatus for Filtering Messages Based on Context

### Related Applications

This application is a Continuation-In-Part of U.S. Serial Number 09/949,101  
5 filed September 7, 2001, which is a Continuation of U.S. Patent Number 6,289,380  
issued September 11, 2001, which is a Continuation of U.S. Patent Number 5,958,012  
issued September 28, 1999. This application claims priority to U.S. Provisional  
Application Serial Number 60/273,044 filed March 2, 2001. The present application  
incorporates each related application by reference in its entirety.

10

### Technical Field

The present application generally relates to the field of monitoring and  
managing ongoing processes. More specifically, the present application relates to  
systems and methods for generating alert and diagnostic messages for the attention of  
15 human operators.

### Background

Systems that manage computer or network systems, or other systems with  
embedded computer technology, commonly monitor various system parameters for the  
20 purpose of detecting problems and alerting a human to the problem. Various  
techniques can be employed to monitor ongoing processes. The monitored values can  
be analyzed in various ways, including comparison with thresholds, correlation of  
several values, and correlation of values over time to discover problems,  
unprecedented situations, or other events.

25 Some systems use various techniques to predict events before they occur. One such  
system is described in commonly owned U.S. Patent No. 6,327,550, which is  
incorporated herein in its entirety by reference. In such systems one response to the  
discovery or prediction is to bring the event to the attention of a human operator. For  
example, these management systems can issue a text message alert and different  
30 techniques may be employed for presenting this text message to the operator, such as a  
Windows dialog box, monitoring consoles, event logs, email messages, pager  
messages. The alert can also be provided as an audio message through loudspeakers,

headsets, or a telephone. An example of a system that provides audio alert messaging is described in commonly owned, concurrently filed, co-pending U.S. Utility Application entitled "Method and Apparatus for Generating and Recognizing Speech as a User Interface Element in Systems and Network Management", the entirety of which is incorporated herein by reference. Commonly owned, concurrently filed, co-pending U.S. Utility Application entitled "Method And Apparatus For Generating Context-Descriptive Messages" is also incorporated by reference in its entirety.

In large management systems with many managed components and/or networks and a high level of activity, the management systems may generate a large number of alert messages. Some alert messages may be more important than others, but are typically issued because the alert functionality of such management systems is not open to modification. Other messages may be redundant because several management systems may independently detect the consequences of an event. As a result, current management systems include various techniques for filtering such alert messages based on various rules unrelated to the content of the message.

For example, some conventional management systems designate the severity of a detected or predicted event as the filtering rule. This permits the management system to present only critical messages, or messages about events above a certain level of severity. Other systems correlate alert messages over time or over several objects as a filtering rule. This permits the recognition that a message may indicate a critical problem, even though it may not indicate such criticality by itself, e.g., a minor error may be more critical if it occurs several times in a short time period.

Even after messages have been filtered so only meaningful messages remain, individual users may be interested in different categories of messages. Some management systems include various techniques for filtering alert messages presented to particular individuals, such as messages related to one or more groups of managed components or networks that denote some sort of business process. An example of such a management system is described in commonly owned U.S. Patent No. 5,958,012, which is incorporated herein in its entirety by reference.

### **Summary**

The present disclosure provides management systems and methods with improved alert messaging. The present disclosure also provides alert systems and

methods capable of filtering alert messages generated by management systems to report operator desired messages. According to one embodiment, a method for reporting an alert condition is disclosed which includes defining alert filter criteria, identifying an alert condition and analyzing one or more properties of the alert condition and the alert filter criteria to determine whether or not to report the alert condition. The method further includes reporting the alert condition if the determination is to report the alert condition.

According to another embodiment, a system for reporting an alert condition is disclosed. The system includes a filter criteria maintenance module capable of maintaining filter alert criteria, an alert condition detector capable of identifying one or more alert conditions, an alert condition filter capable of filtering identified alert conditions based on the alert filter criteria, and an alert notification module for reporting the filtered alert conditions.

According to another embodiment, a system for reporting an alert condition is disclosed. The system includes means for maintaining filter alert criteria, means for identifying one or more alert conditions, means for filtering the one or more identified alert conditions based on the alert filter criteria and means for reporting the filtered alert conditions.

According to another alternative embodiment, a computer-readable storage medium is disclosed. The medium is encoded with processing instructions for reporting an alert condition, including instructions for defining alert filter criteria and instructions for identifying an alert condition. The medium also includes computer readable instructions for analyzing one or more properties of the alert condition based on the alert filter criteria and for determining whether to report the alert condition. The medium further includes instructions for selectively reporting the alert condition.

### **Brief Description of the Drawings**

For a more complete understanding of the present methods and systems, reference is now made to the following description taken in conjunction with the accompanying drawings in which like reference numbers indicate like features and wherein:

Figure 1A illustrates an exemplary enterprise system;

Figure 1B illustrates an exemplary management system topology that may be managed in accordance with the disclosed methodology;

Figure 2 is a block diagram illustrating exemplary components for implementing one embodiment of an alert system methodology according to the present disclosure;

Figure 3A is a diagram illustrating exemplary system topology objects used by one or more embodiments of the management system according to the present disclosure ;

Figure 3B is a diagram illustrating exemplary alert filter criteria objects used by one or more embodiments of the management system according to the present disclosure;

Figure 3C is a diagram illustrating exemplary alert condition objects used by one or more embodiments of the management system according to the present disclosure; and

Figure 4 is an exemplary flow diagram of one method for filtering alert conditions in accordance with one embodiment of the present disclosure.

### **Detailed Description**

An exemplary IT enterprise is illustrated in Figure 1A. The IT enterprise includes local area networks 155, 160 and 165. IT enterprise further includes a variety of hardware and software components, such as workstations, printers, scanners, routers, operating systems, applications, and application platforms, for example. Each component of IT enterprise may be monitored and managed in accordance with the present disclosure.

The various components of an exemplary management system 100 topology that can manage an IT enterprise in accordance with the present disclosure are shown in Figure 1B. The management system 100 includes at least one visualization workstation 105, an object repository 110, one or more management applications 115, and one or more management agents 120 associated with each management application 115.

The visualization workstation 105 provides a user access to various applications including a network management application 115. Workstation 105 interacts with an object repository 110 which stores and delivers requests, commands and event notifications. Workstation 105 requests information from object repository 110, sends commands to the object repository, and gets notification of events, such as status changes or object additions from it. The object repository 110 receives request

information from the management application 115, which is fed by the management agents 120 responsible for monitoring and managing certain components or systems in an IT enterprise.

5 The management application 115 maintains object repository 110, in part, to keep track of the objects under consideration. The object repository 110 may be a persistent store to hold information about managed components or systems, such as a database. In an alternative embodiment, the management application 115 and object repository 110 may be integrated into a single unit that can hold information about managed components in volatile memory and perform the tasks of the management  
10 application.

As shown, one architectural aspect of the present system is that in normal operation, the visualization workstation 105 interacts primarily with the object repository 110. This reduces network traffic, improves the performance of graphical rendering at the workstation, and reduces the need for interconnectivity between the  
15 visualization workstation 105 and a multitude of management applications 115, their subsystems and agents 120 existing in the IT enterprises. Of course, embodiments having other configurations of the illustrated components are contemplated, including a stand-alone embodiment in which the components comprise an integrated workstation.

20 In addition to handling requests, commands and notifications, object repository 110 may also handle objects describing the structure and operation of the management system 100. Such objects may describe the momentary state, load, and performance of the components and/or systems. Such objects may be populated using a manual process or an automatic discovery utility.

25 The alert filtering criteria may be, for example, the severity of an event, the relative importance of the object that exhibits the event, the urgency of the notification and the likelihood that the event condition will occur. To illustrate the interplay of severity, importance, urgency and risk, consider two potential problems associated with a personal computer and attached peripherals. The first potential problem might  
30 be an 80% likelihood that there will be a shortage of paper for the printer. The second potential problem might be a 2% likelihood that there will be a hard disk drive failure. The first problem has a high risk and low severity while the second potential problem has a relatively low risk but high severity. Determining the importance and urgency of each potential problem might require additional information regarding the use of the

personal computer. For example, if a major use of a computer is printing, the urgency and importance the first problem might be higher. If the computer is primarily used for data storage, acting as a server for other computers running mission critical applications, the importance of the second problem might be higher, while the urgency  
5 might be moderate.

Referring now to Figure 2, components forming one embodiment of an alert system according to the present disclosure is shown. The alert system **200** may be a distributed system formed by, for example, management application **115** and object repository **110** shown in Figure 1. Alternatively, as noted above, the management  
10 system **115** may incorporate the object repository **110** and the alert system **200** may be an integrated system incorporated into management application **115**. In the embodiment of Figure 2, the alert system **200** includes a filter criteria maintenance module **205**, an alert condition detection module **220**, an alert condition filter module **230**, and an alert notification module **235**. The filter criteria maintenance module **205**  
15 enables an operator to define criteria under which alert notifications may be reported. The alert filter criteria are stored in the object repository **110** as a set of alert filter criteria objects in database **210**. The filter criteria maintenance module **205** may further enable an operator to add, delete, update or otherwise maintain system objects in database **215** that define the topology of IT enterprise **150**. Maintenance of the  
20 system objects in database **215** may include, for example, defining the importance of a system or network component, or defining dependency or containment relationships between and among several system or network components.

According to one embodiment, the alert filter criteria objects in database **210** direct the alert system **200** how to react to an alert message based on both the severity  
25 of an alert condition and on the importance of the affect of the alert condition on system or network component(s). The alert filter criteria objects in database **210** may further direct the system to take the urgency of an alert condition into account, and in the case of a prediction, the alert system **200** may take into account the level of risk.

Because the alert system **200** enables tracking the importance of objects, the severity and urgency of alert conditions and the risk for predicted alert conditions, the  
30 alert system **200** can use any or all of these four metrics to filter and report alert messages or notifications intelligently.

Figure 3A illustrates portions of several exemplary system objects that may be maintained by, for example, filter criteria maintenance module **205**. The illustrated



objects relate to a topology of It enterprise **150**. In this exemplary illustration, object **305** represents a “network server A” which utilizes “router A” and “router B”, represented by objects **307** and **309** respectively, to communicate with other network components. For example, “network server A” utilizes “router B” to communicate with “workstation A” and workstation B”, represented by objects **311** and **313** respectively. Workstation B is running two applications represented by objects **315** and **317**, and “workstation B” has an associated printer “WSB printer” represented by object **319**.

The alert system according to the present disclosure can use the level of importance of each object to facilitate context-based filtering. Instances may occur where the importance of an alert condition is not readily apparent from the object. For example, a database server may not always be mission-critical, and it may depend on whether the database server is being used by an application having an importance level of mission critical. Of course, human operators may know how the database server is being used and can manually enter the appropriate levels of importance for a particular server. Manual entry of importance levels, however, is cumbersome and inefficient, especially in situations where the relationships between different components may be indirect. For example, a database server may be shifted from a moderate level of importance to a mission critical level of importance. If the shift is not detected by the operator, the old lower importance level may inadvertently be retained. Another example of the inefficiency of manual entry of importance level can occur is where the traffic between an application running on a workstation and a database server depends on other network components, e.g., routers. In such situations, the database server, other network components, and the human operator may not be aware of such indirect relationships and consequently may neglect to manually adjust the importance levels.

Thus, according to one embodiment of the present system, if the management system can detect such dependency relationships, the importance rating can be influenced by dependencies.

The objects illustrated in Figure 3A illustrate an example of such inheritance of importance properties based on a dependency relationship. As shown, Application B **317** is a mission critical application so that workstation B **313**, the workstation upon which successful execution of the mission critical application depends, also assumes an importance level of “mission critical”. Further, the router **309** and the network server **305**, upon which the application depends, are also assigned “mission critical”

importance. As a result, the alert system **200** can support the use of dependency relationships to propagate or inherit importance levels.

Figure 3B illustrates several exemplary alert filter criteria objects that may be maintained by filter criteria maintenance module **205**, and used by the alert system **200** to determine whether or not to report an alert condition to an operator. In this exemplary embodiment, each alert filter criteria is assigned a group ID which designates a system component subject to an alert condition. Although the objects of Figure 3B are indexed by group, alternate indexing schemes, such as by operator ID or workstation ID, for example, may also be used.

In the exemplary embodiment of Figure 3B, alert filter criteria object **321** represents a filter rule associated with alerts affecting an accounts receivable business group having a group ID "AR". Alert filter criteria object **321** directs the alert system **200** to report alerts affecting an AR function only if the alert has an importance level of "mission critical". Alert filter criteria object **323** represents a filter rule associated with alerts affecting a human resources business division having a group ID "HR". Alert filter criteria object **323** directs the system to report alerts affecting an HR function only if the alert has an importance level of "medium or higher."

Alert filter criteria object **325** represents a filter rule associated with alerts affecting an accounts payable business division having a group ID "AP". Alert filter criteria object **325** directs the system to report alerts affecting an AP function only if the alert has an importance level of "mission critical" or if the alert has an urgency level of 24 hours or less.

Referring again to Figure 2, the alert condition detection module **220** is used to detect actual or potential alert conditions. Alert condition detection module **220** refers to the system objects in database **215** of object repository **110** among other relevant factors to determine whether an alert condition exists, and generates and stores an alert condition object in database **225**.

In one embodiment, alert condition detection module **220** assigns a severity property to each detected alert condition. This may be accomplished using the principles of the predictive management system described in commonly owned U.S. Patent Number 6,327,550, which is incorporated herein by reference. Risk and urgency properties are also assigned. The urgency property may represent the amount of time remaining before action must be taken or it may represent a rating inversely related to the amount of time remaining. As previously described, module **220** also

assigns an importance property to the alert condition object. The importance property represents a measure of the importance of the object, indicated, for example, along some suitable scale, such as 0–5.

The importance property may be determined in any of a number of ways. For example, the importance property may be manually assigned to each class of objects, so that each object of that class inherits the importance property of the class. Alternatively, classes of objects may be arranged in an inheritance hierarchy, so that a subclass (such as “NT server”) may inherit the importance rating of its parent class (such as “NT system”). In accordance with another example of importance level assignment, individual objects may be manually assigned an importance rating that overrides the rating of the class.

According to another way that the importance property may be assigned, various subsystems, such as for example a job scheduling system, may automatically set the importance properties of individual objects based on some suitable determination, overriding the rating of the class. In yet another example, the importance property may be propagated up a containment hierarchy based on some suitable algorithm. For example, importance may be propagated up based on the highest value among the contained components, so a component that contains several sub-components assumes the highest importance rating of the sub-components it contains.

The importance property may also be propagated along dependency relationships based on some suitable algorithm. For example, the importance property may be propagated along a “depends on” direction of a relationship with a “largest-value” aggregation function, so if an important application server depends on a database server, then the database server gets the same importance property as the application server unless some other propagation gives it a higher rating.

The detected alert condition objects of database **225** are referenced by alert condition filter module **230** and analyzed in accordance with the applicable alert filter criteria from database **210** to determine whether the detected alert condition qualifies to be reported to an operator. If alert condition filter module **230** determines that a detected alert condition merits reporting, the alert notification module **235** is directed to report the alert notification to an appropriate operator.

Figure 3C illustrates several exemplary alert condition objects which may be generated by alert condition detection module **220**. Each illustrated alert condition

object represents an actual or projected alert condition that may be reported to an operator by alert notification module **235** based on the alert filter criteria **210**.

Referring to Figures 3A and 3C, alert condition object **331** is an example of an actual alert condition. Object **331** represents an alert condition in which the used disk space associated with network server A has exceeded a predetermined acceptable threshold. The importance level of the alert is “mission critical” because network server A **305** supports the mission critical application **317** running on workstation B **313**. Alert condition detection module **220** determined the severity to be moderate, due to the fact that there is still available storage space on the disk, and further determined the risk to be “absolute” because the condition exists. Alert detection module **220** also determined that the urgency for this alert is immediate. Due to the relationship of network server A to the other components in the system, the affected groups include AP, AR, HR and IT.

Alert condition object **333** is an example of a potential or projected alert condition. Object **333** represents an alert condition in which there is a potential paper shortage for WSB printer. The importance level of the alert is “mission critical” because WSB printer **319** is used by the mission critical application **317** running on workstation B **313**. Alert condition detection module **220** determined the severity to be high, due to the fact that while there is still available paper, the lack of paper would prevent the proper completion of Application B. Alert condition detection module **220** also determined that the likelihood that the condition will occur is 80% and that the urgency for this alert is “24 hours”. Due to the relationship of the WSB printer to the other components in the system. The group AR the is the only affected group.

As discussed above, the importance level of an object may be propagated along dependency relationships. The alert condition objects of Figure 3C illustrate that in one embodiment, the importance levels, severity, risk and urgency may be propagated among objects may also be propagated along containment relationships. In other words, so a computer or other component that hosts or provides service to an important process is also important, as is the subnetwork within which the computer resides.

Of course, the use of severity and importance properties for filtering messages requires some care, when properties are propagated. Although the importance and severity properties illustrated herein have been qualitative, in an alternative embodiments such properties could be quantitative, e.g. numerical.

In such an embodiment, filter criteria maintenance module **205** may support filter criteria, and alert condition filter module **230** could filter alert condition objects, based on the sum or product of the numerical values representing severity and importance levels. As an example, consider a situation in which sub-network S1 contains computers C1 and C2. In this example, computer C1 is performing an important function and has a “very high” importance level, but a “normal” severity level. Computer C2 is a test system and has a “critical” severity level, but a “low” importance level. If severity and importance are independently propagated, then the subnetwork S1 would have both the “critical” severity and the “very high” importance levels, which might lead the message filtering system to report an alert for sub-network S1. However, if the important computer C1 is functioning properly, and the unimportant test computer C2 exhibits problems, there is no cause for concern regarding sub-network S1 and notification of the alert may not be needed. Therefore, according to an alternative embodiment of the present alert system, a filtering expression, such as, for example “severity + importance”, can be propagated separately so that alerts are reported for those alerts that meet this sum or difference filtering condition.

Referring now to Figure 4, there is illustrated an exemplary flow diagram of methodology for filtering alert conditions in accordance with one embodiment of the present disclosure. At block **405**, alert filter criteria are defined. The filter criteria are utilized to determine whether to report a detected filter condition, and they may include importance, severity, urgency and/or risk properties. The filter criteria may further include one or more identifiers representing a user, a workstation, an interest group or a business process.

At block **410**, an alert condition is detected. The alert condition may be an existing condition that requires operator attention, a warning regarding an existing condition or a predicted/potential condition that may require operator attention. Any technique known to those of skill in the art may be used in the detection of actual or potential alert conditions.

In addition to the detection of an alert condition, block **410** may also include use propagation algorithms to determine certain properties of the alert condition as represented by an alert condition object, such as for example, importance, severity, urgency and/or risk. In addition, associated identifiers such as, for example, an interest group identifier, may also be propagated to the alert condition object. The propagation

may occur, for example, along dependency relationships or along containment relationships.

At block **415**, the filter criteria associated with the detected alert condition are determined. The association between the filter criteria and the detected alert condition  
5 may be based on one or more elements such as, for example, interest group identifier, user identifier or , system component identifier. The association may be based on any factor that would be relevant in reporting the detected alert condition.

At block **420**, the filter criteria is applied to the relevant properties of the detected alert condition. Based on the application of the filter criteria to the detected  
10 alert condition, a determination is made at block **425** whether or not to report the detected alert condition. If the properties of the detected alert condition fall within the alert filtering criteria, an alert notification is generated and output to an appropriate operator at block **430**. Otherwise, the detection and filtering steps are repeated to continually report alert conditions as they arise.

15 Accordingly, it is to be understood that the drawings and description in this disclosure are proffered to facilitate comprehension of the methods and systems, and should not be construed to limit the scope thereof. It should be understood that various changes, substitutions and alterations can be made without departing from the spirit and scope of the disclosed methods systems.

What is claimed is:

1. A method for reporting an alert condition, comprising:  
defining alert filter criteria;  
5 identifying an alert condition;  
analyzing one or more properties of the alert condition based on the alert filter  
criteria;  
determining whether to report the alert condition; and  
selectively reporting the alert condition.  
10
2. The method of claim 1, wherein the one or more properties include importance,  
severity and urgency.
3. The method of claim 1, wherein identifying an alert condition includes  
15 identifying a potential alert condition.
4. The method of claim 1, wherein the one or more properties include a property  
representing a level of risk associated with a potential alert condition.
- 20 5. The method of claim 1, further comprising analyzing a property representing  
an interest group associated with the alert condition.
6. The method of claim 1, further comprising analyzing a property representing a  
business process associated with the alert condition.  
25
7. The method of claim 1, wherein identifying an alert condition includes:  
identifying a first object representing a first system component associated with  
the alert condition;  
identifying a second object representing a second system component having a  
30 dependency relationship to the first system component; and  
propagating a property of the second object to the first object.
8. The method of claim 1, wherein identifying an alert condition includes:

identifying a first object representing a first system component associated with the alert condition;

identifying a second object representing a second system component having a containment relationship to the first system component; and

5 propagating a property of the first object to the second object.

9. A system for reporting an alert condition, comprising:

a filter criteria maintenance module for maintaining filter alert criteria;

an alert condition detector for identifying an alert condition;

10 an alert condition filter for filtering identified alert condition based on the alert filter criteria; and

an alert notification module for selectively reporting the alert condition.

10. The system of claim 9, wherein the alert condition detector assigns importance, severity and urgency properties associated with the alert condition.

11. The system of claim 9, wherein the alert detector identifies a potential alert condition.

20 12. The system of claim 9, wherein the alert condition detector assigns a risk property associated with the potential alert condition.

13. The system of claim 9, wherein the alert condition filter analyzes a property representing an interest group associated with the alert condition.

25

14. The system of claim 9, wherein the alert condition filter analyzes a property representing a business process associated with the alert condition.

15. The system of claim 9, wherein the alert condition filter includes property propagation logic for propagating a property of a first object to a property of a second object based on a dependency relationship between the first and second objects.

30



16. The system of claim 9, wherein the alert condition filter includes property propagation logic for propagating a property of a first object to a property of a second object based on a containment relationship between the first and second objects.

5 17. A system for reporting an alert condition, comprising:

means for maintaining filter alert criteria;

means for identifying an alert condition;

means for filtering identified alert condition based on the alert filter criteria;

and

10 means for selectively reporting the alert condition.

18. A computer-readable storage medium encoded with processing instructions for reporting an alert condition, including:

computer readable instructions for defining alert filter criteria;

15 computer readable instructions for identifying an alert condition;

computer readable instructions for analyzing one or more properties of the alert condition based on the alert filter criteria;

computer readable instructions for determining whether to report the alert condition; and

20 computer readable instructions for selectively reporting the alert condition.

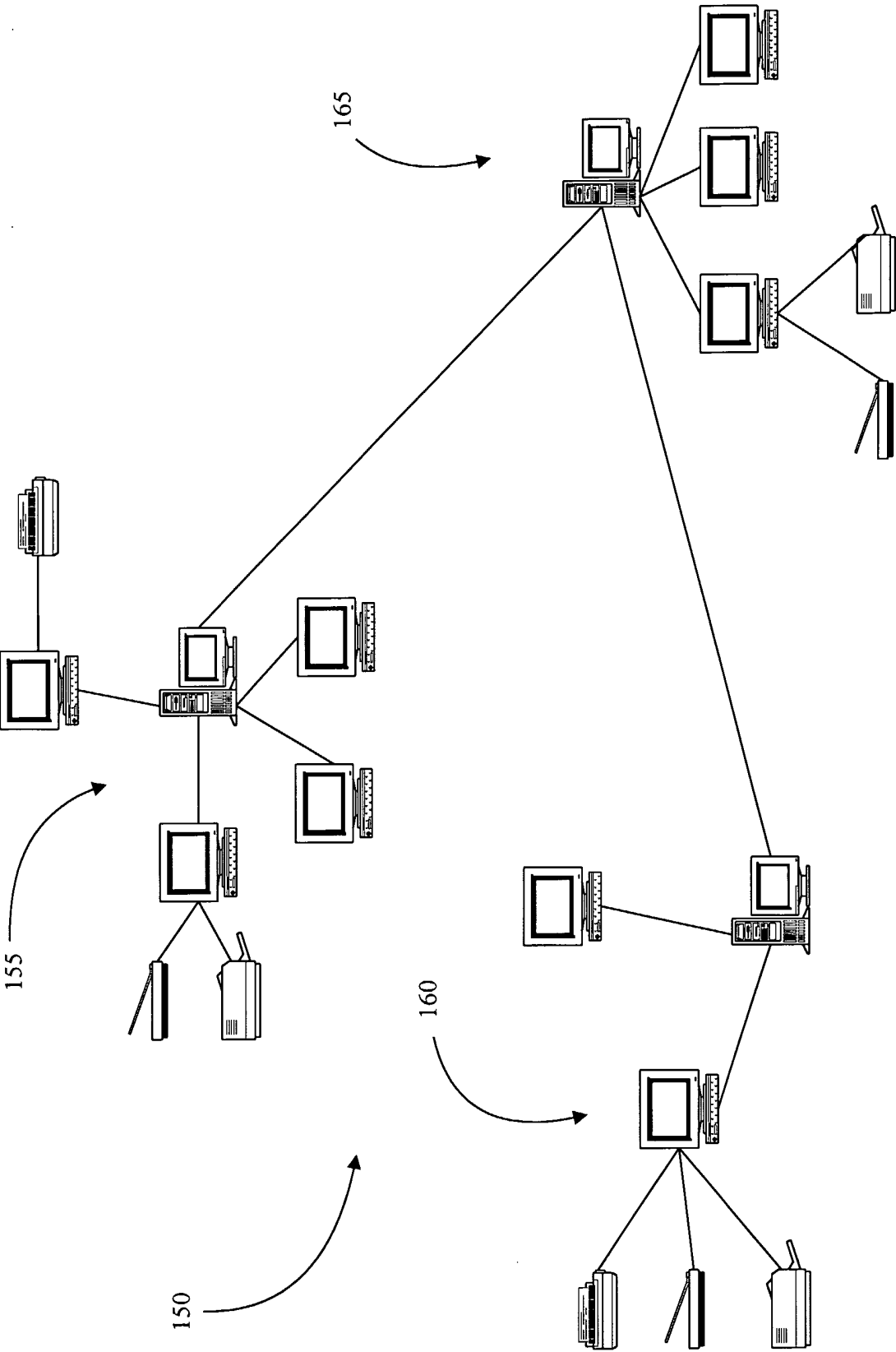


Figure 1A

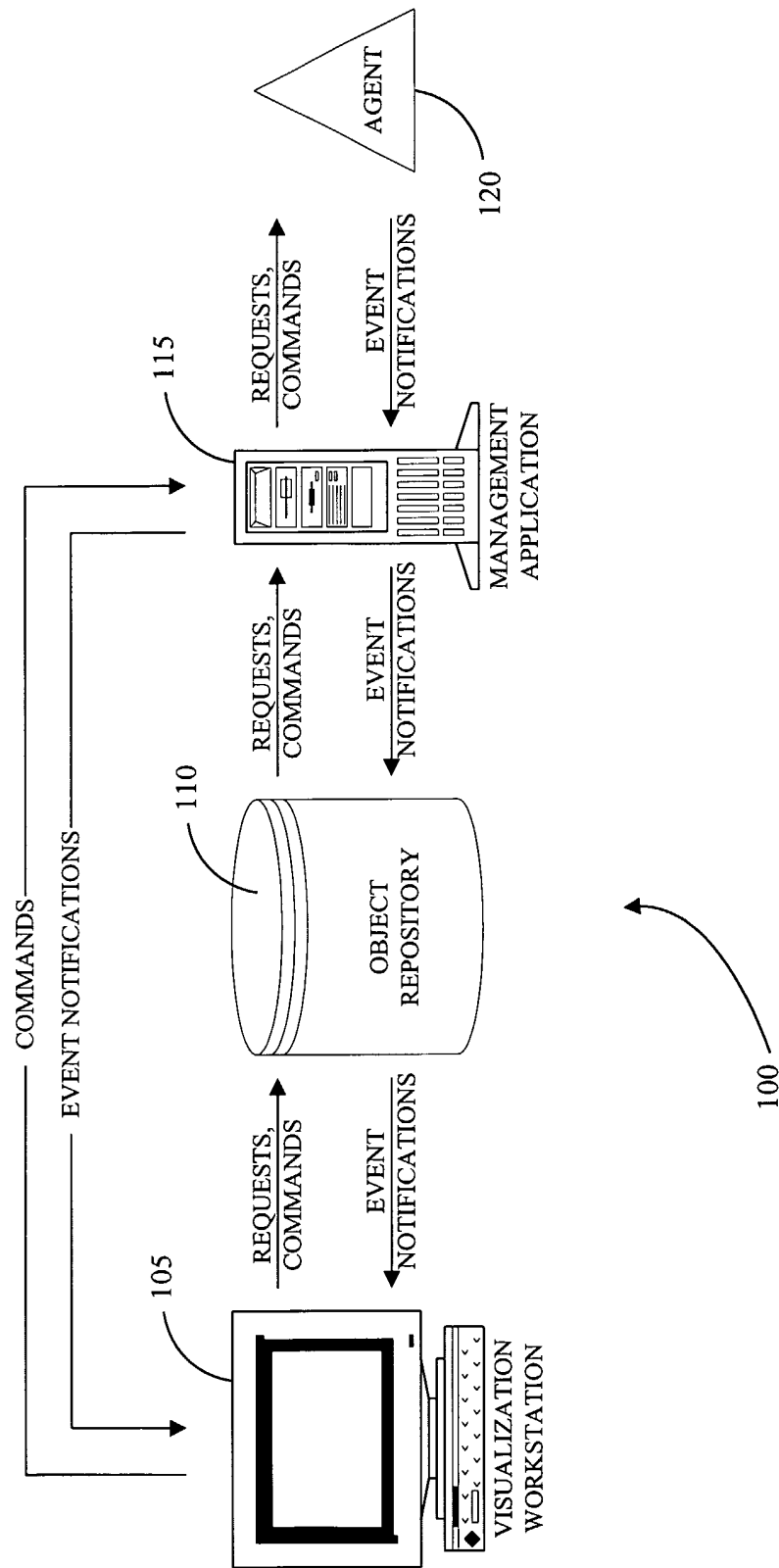


Figure 1B

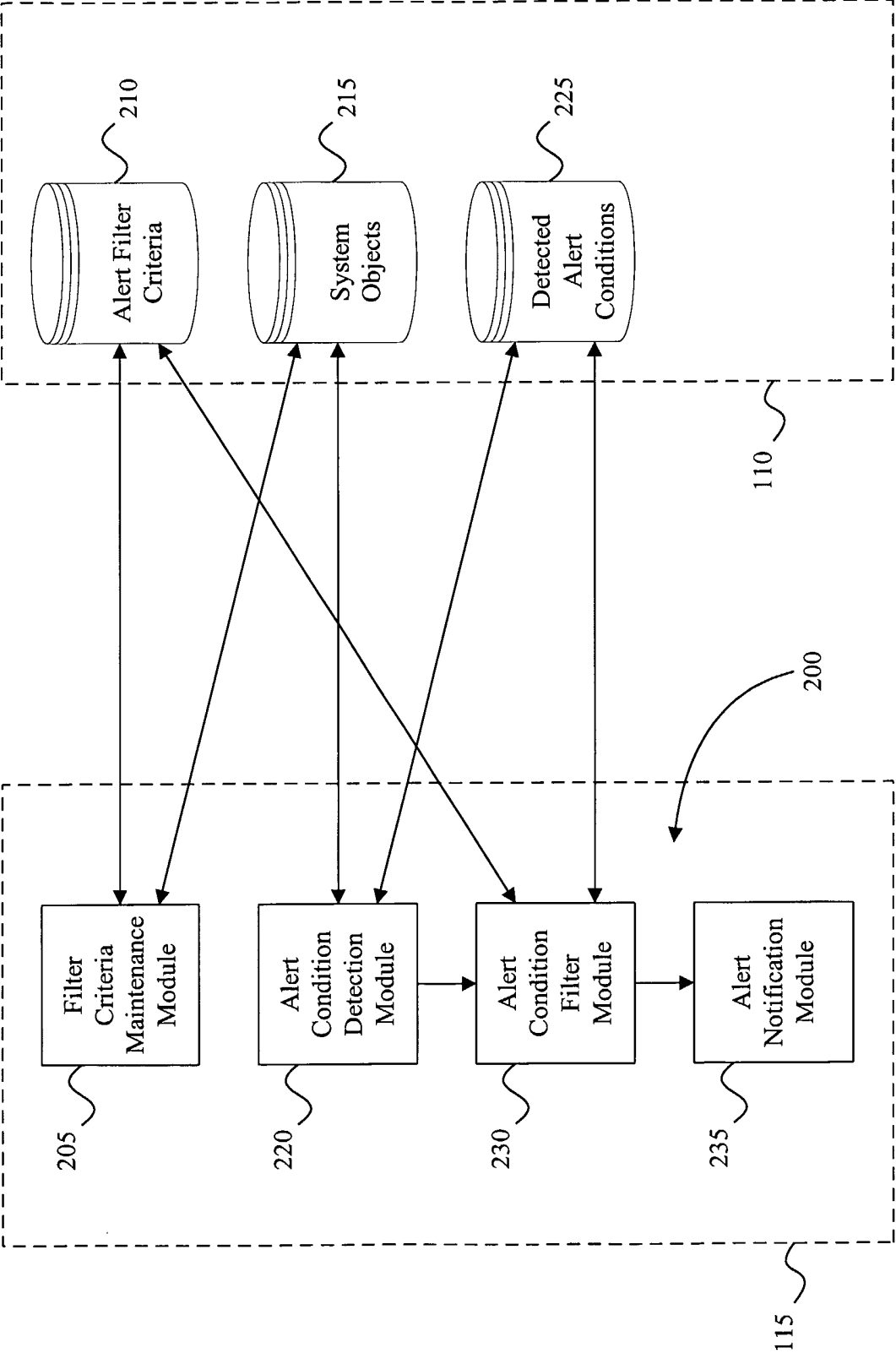


Figure 2

System Objects

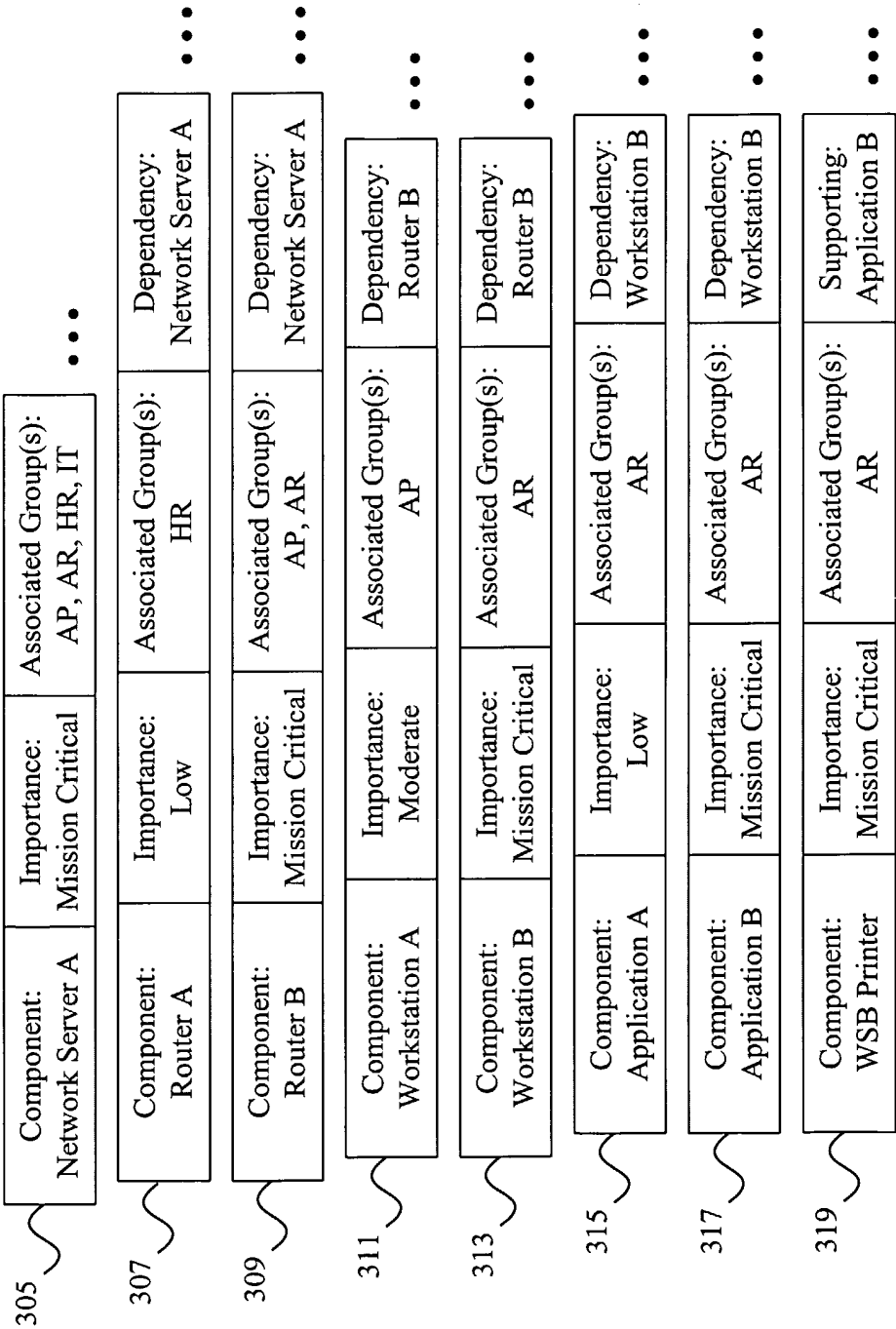


Figure 3A

Alert filter criteria objects

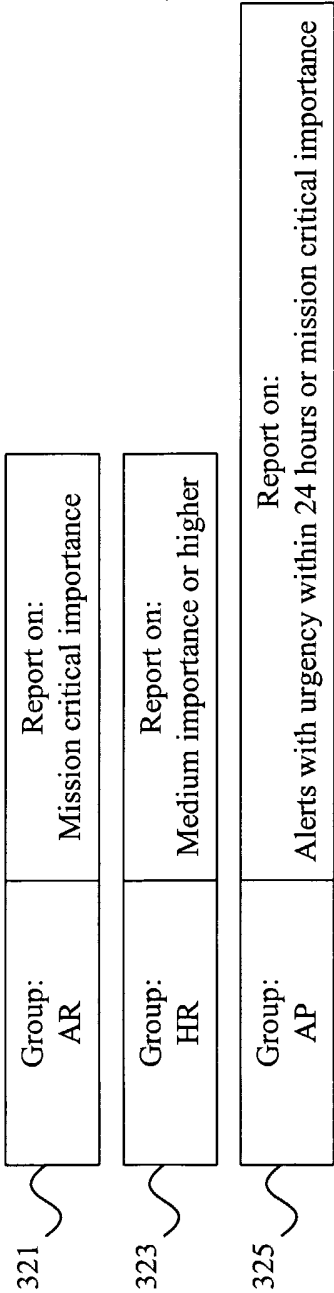
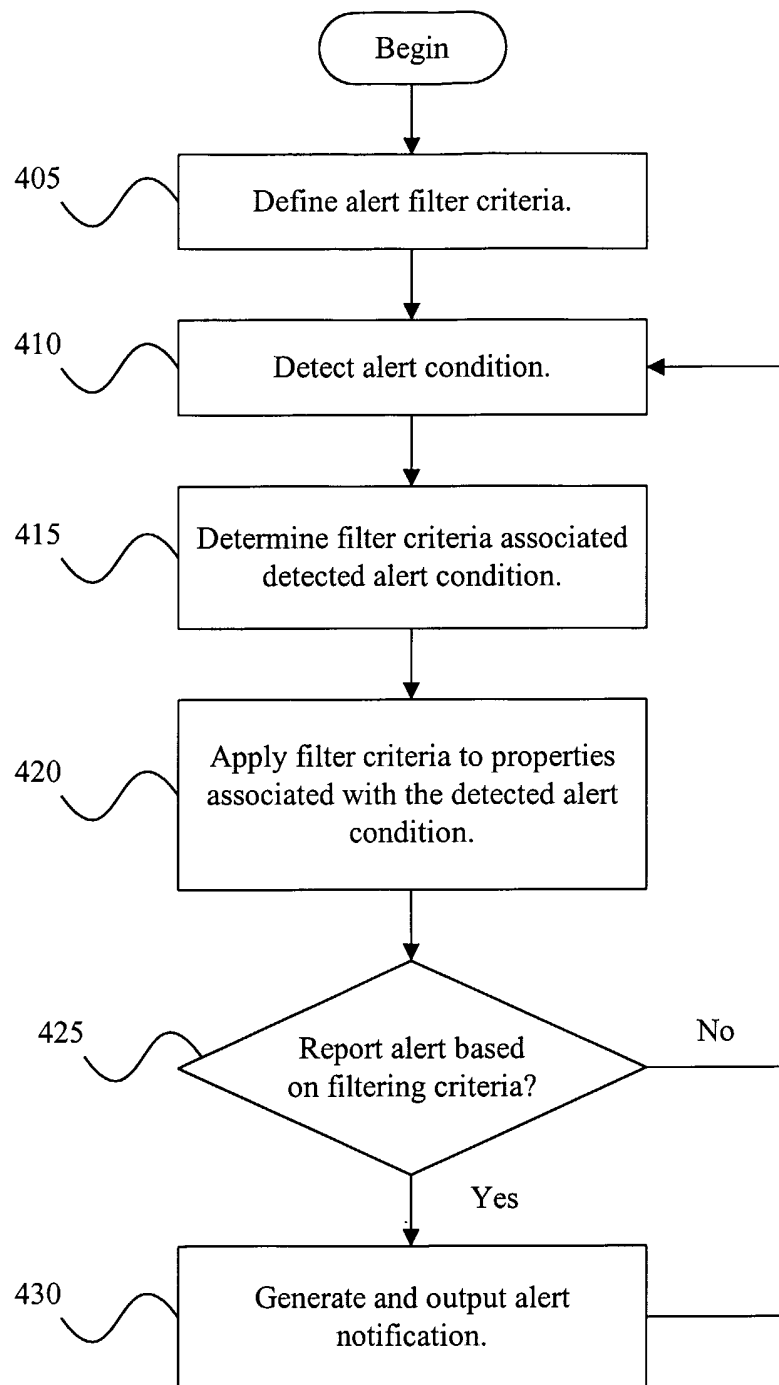


Figure 3B

Alert condition objects

331	Alert: Disk Above Threshold	Component: Network Server A	Importance: Mission Critical	Severity: Moderate	Risk: Absolute	Urgency: Immediate	Group(s): AP, AR, HR, IT
333	Alert: Paper Shortage	Component: WSB Printer	Importance: Mission Critical	Severity: High	Risk: 80%	Urgency: 24 Hours	Group(s): AR
335	Alert: Scheduled Maintenance	Component: Router A	Importance: Low	Severity: Low	Risk: Absolute	Urgency: 1 Week	Group(s): HR
337	Alert: File Not Found	Component: Application A	Importance: Low	Severity: High	Risk: Absolute	Urgency: Immediate	Group(s): AR
339	Alert: Memory shortage	Component: Network Server A	Importance: Mission Critical	Severity: High	Risk: Absolute	Urgency: Immediate	Group(s): AP, AR, HR, IT
341	Alert: Disk full	Component: Workstation A	Importance: Moderate	Severity: High	Risk: Absolute	Urgency: Immediate	Group(s): AP

Figure 3C

**Figure 4**



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/06448

**A. CLASSIFICATION OF SUBJECT MATTER**

IPC(7) : G06F 15/173; G09G 5/00

US CL : 709/224; 345/736

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/223-224; 345/734-737

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4,464,543 A (KLINE et al.) 7 August 1984, col. 8 lines 52-63.	1, 9, 17-18
X	US 5,696,486 A (POLIQUIN et al.) 9 December 1997, col. 4 lines 11-18, col. 7 lines 41-51.	1-2, 9-10, 17-18
----		-----
Y		5-8, 13-16
Y	US 6,167,448 A (HEMPHILL et al.) 26 December 2000, col. 4 lines 58-65.	5-6, 13-14
Y	US 6,052,722 A (TAGHADOSS) 18 April 2000, col. 2 lines 56-61, col. 6 lines 50-61, col. 7 lines 50-65.	7-8, 15-16
A	US 5,958,012 A (BATTAT et al.) 28 September 1999, cols. 15-16.	1-18



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Z" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

03 MAY 2002

Date of mailing of the international search report

31 MAY 2002

Name and mailing address of the ISA/US  
Commissioner of Patents and Trademarks  
Box PCT  
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

ANDREW CALDWELL

Telephone No. (703) 305-3800

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/06443

## B. FIELDS SEARCHED

Electronic data bases consulted (Name of data base and where practicable terms used):

USPAT, USPGPUB

search terms: alert, alerts, alarm, alarms, event, events, trap, traps, notification, notifications, filter