(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 May 2001 (31.05.2001)

PCT

(10) International Publication Number
WO 01/38995 A1

(51) International Patent Classification[7]: G06F 13/00, 17/30, H04N 7/167

(21) International Application Number: PCT/US00/41796

(22) International Filing Date:
2 November 2000 (02.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/163,231 3 November 1999 (03.11.1999) US

(71) Applicant: AVANTCOM NETWORK, INC. [US/US]; 911 Bern Court, Suite 110, San Jose, CA 95112 (US).

(72) Inventor: PATANKAR, Subhash; 892 Meander Drive, Walnut Creek, CA 94598 (US).

(74) Agent: MEIER, Lawrence, H.; Downs Rachlin & Martin, PLLC, 199 Main Street, P.O. Box 190, Burlington, VT 05402-0190 (US).

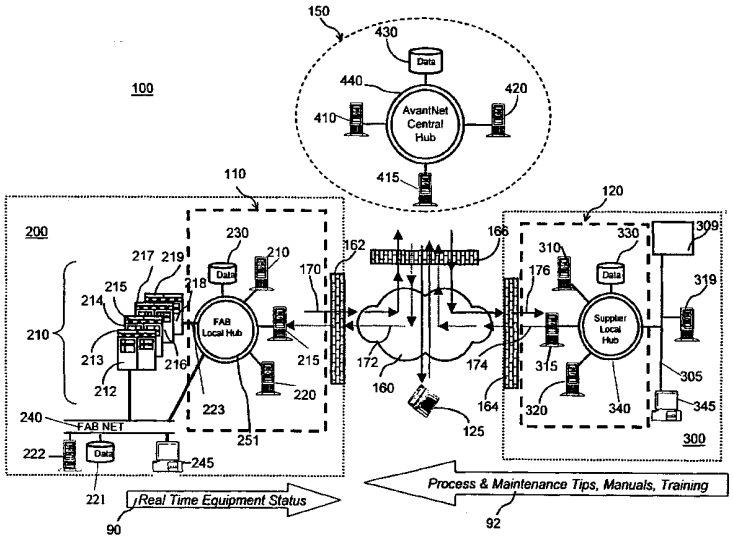
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 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, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

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.

(54) Title: METHOD AND APPARATUS FOR PROPRIETARY DATA COLLECTION AND DISTRIBUTION



(57) Abstract: An industry wide system for collecting and distributing real-time data that includes a central network (150) having a database for receiving real-time data and one or more local networks (110, 120) connected to the central network via an internet network (160). Each local network collects real-time data and transmits the real-time data to the central network database via a secure transmission mode. Access to the central and local network databases is controlled according to prearranged rules that are implemented by an access control program. A user can access the central network database and the real-time data remotely via the internet network. The data stored at any of the network locations may be proprietary. An owner of such proprietary data can share some or all of such proprietary data with the owner of the other local networks according to rules specified by the owner of the proprietary data.

WO 01/38995 A1

METHOD AND APPARATUS FOR PROPRIETARY DATA COLLECTION AND DISTRIBUTION

CROSS REFERENCE TO RELATED CO-PENDING APPLICATIONS

This application claims the benefit of U.S. provisional application Ser. No. 60/163,231 filed on November 3, 1999 and entitled "METHOD AND APPARATUS FOR PROPRIETARY DATA COLLECTION AND DISTRIBUTION" which is commonly assigned and the contents of which are expressly incorporated herein by reference.

FIELD OF INVENTION

The present invention relates to a method and an apparatus providing proprietary data collection and distribution, and more particularly to an industry-wide network that allows collection of proprietary information and secure, real-time, event-driven distribution of the proprietary information to network subscribers.

BACKGROUND OF THE INVENTION

In a high-technology manufacturing environment many aspects of the manufacturing operation are usually tied together in order to control work-in-progress and to monitor quality, throughput, maintenance events and other aspects of the operation. To accomplish this data collection and monitoring, some manufacturers connect all relevant machines to a common signal carrier or bus, which collects real-time data from each machine in a particular format. An example of such a system is a semiconductor fabrication operation that has process equipment connected via a Local Area Network (LAN) to a server. The data collection is accomplished via a messaging software system such as The Information Bus or TIB supplied by TIBCO Software, Inc., of Palo Alto, CA.

Typically a manufacturer selects the type of data to be collected and the format in which it is stored. Data associated with the manufacturing process parameters, quality control and throughput are usually considered proprietary information and are stored at a server located at the manufacturer's site. Access to the server and to the particular proprietary information is usually limited to certain members of the manufacturer's operation. However, frequently, these data need to be analyzed to determine causes for defects or problems in the manufacturing process and to develop improvements of the process. Expert scientist and

specialist from third party organizations are often contracted to conduct this analysis and recommend solutions. In cases where performance of a piece of equipment or consumable material used in the manufacturing process is an issue, suppliers of the specific piece of equipment or material need to be involved. Therefore, there is a need for these outside contracted experts and suppliers to gain controlled access to proprietary data associated with the manufacturing process, in order to work collaboratively with the manufacturer's personnel to solve the problem.

Problems associated with a collaborative working environment involving sharing proprietary data between manufacturer's third party experts and suppliers include incompatibilities between different data formats and complicated management protocols and access control mechanisms. Further, concerns over the security of the shared data, especially transmission out of the manufacturer's facilities, makes manufacturers reluctant to share detailed, real-time data electronically. Therefore, there is a need for an industry-wide network that allows collection of proprietary information in compatible formats and secure, real-time, event-driven distribution of the proprietary information to network subscribers.

SUMMARY OF THE INVENTION

In general, in one aspect, the invention provides an industry wide system for collecting and distributing real-time data. The industry wide system includes a central network having a database for receiving real-time data and a first local network collecting a first set of real-time data according to a first format and transmitting the first set of real-time data to the central network database via a secure transmission mode. Access to the database and real-time data is controlled.

Implementations of the invention may include one or more of the following features. Access to the database may be controlled according to prearranged rules and the rules may be implemented by an access control program. An operator may access the database and the real-time data remotely via an internet network. The real-time data may be proprietary. The secure transmission mode may include encryption of the real-time data and transmission of the encrypted data via an internet network.

The system may also include a second local network collecting a second set of data according to a second format and transmitting the second set of data to the central network database via

a secure transmission mode. First and second operators connected to the first and second local networks, respectively, may have access to the central network database and the first and second set of data. First local network may be located at a manufacturing company and first set of real-time data may be real-time manufacturing process parameters. Second local network may be located at an equipment supplying company and second set of data may be equipment related data.

The system may also include a messaging software for receiving and transmitting real-time data, an encryption software for encrypting and decrypting the transmitted and received real-time data, respectively, a repair report managing software, a business rules managing software, a people profile managing software, a static data entry managing software, a real time monitor software, an equipment logging managing software, an incident managing software, analytical software for analyzing the real-time data, subscribing software for listening, queuing and updating the real-time data in the database and a data replication software for providing security, redundancy, scalability, back-up, recovery, replication and synchronization of data.

In general, in another aspect, the invention features an industry wide system for collecting and distributing real-time data that includes a central network having a database for receiving real-time data and a plurality of local networks collecting and transmitting a plurality of real-time data to the central network database via a secure transmission mode. An operator connected to at least one of the local networks may have access to the central network database and the plurality of data. Access may be controlled according to pre-arranged rules and the rules may be implemented by an access control program.

In general, in another aspect, the invention features a method for collecting and distributing real-time data including providing a central network having a database for receiving real-time data, providing a first local network for collecting a first set of real-time data according to a first format and transmitting the first set of real-time data to the central network database via a secure transmission mode. Access to the database may be controlled according to pre-arranged rules and the rules may be implemented by an access control program.

Among the advantages of this invention may be one or more of the following. The system provides non-invasive business to business communication and collaboration via an internet

network. It offers standard or custom views of shared real-time data and reports to subscribing companies. The system also offers analytical tools and other shared software that allow exchange of proprietary data according to prearranged rules.

The details of one or more embodiments of the invention are set forth in the accompanying drawings and description below. Other features, objects and advantages of the invention will be apparent from the following description of the preferred embodiments, the drawings and from the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic overview diagram of a network system including a manufacturer's local hub, a supplier's local hub and a central hub;

FIG. 2 is a schematic overview diagram of a network system including a manufacturer's local hub, a supplier's local hub, a central hub and a third party local hub;

FIG. 3 is a schematic diagram of a network system with a remote dial-up access;

FIG. 4 is a schematic diagram of a network system including multiple manufacturers' local hubs, multiple suppliers' hubs and a central hub;

FIG. 5 is a diagram depicting various formats describing the "UP" state of a machine;

FIG. 6 is schematic overview diagram of the software modules and databases associated with the local hub and central hub;

FIG. 7 is schematic overview diagram of the shared software programs associated with the central hub.

DETAILED DESCRIPTION OF THE INVENTION

Referring to FIG. 1, network 100 connects local hubs 110 and 120 to a central hub 150. The network 100 includes hardware and software components that allow hubs 110 and 120 to communicate with each other through the central hub 150.

Local hub 110 is installed at a manufacturer's site 200 and serves the purpose of centralizing all the local data, information and communication protocols. In one example, local hub 110 supports data and information associated with a semiconductor fabrication operation 200. The semiconductor fabrication operation 200 includes a manufacturing line 210 that produces integrated circuit devices ("chips"), a resource planning system 222 that plans and coordinates the production operation, a database 221 for storing all the data associated with the semiconductor fabrication operation 200 and a local area network (LAN) 240 that provides connectivity between the manufacturing line 210, the resource planning system 222 and the database 221. The manufacturing line 210 includes a chemical vapor deposition (CVD) chamber 212 for depositing thin films on semiconductor wafers, a photolithography station 214, a chemical mechanical polishing (CMP) apparatus 216 and a quality control and packaging station 218. Control units 213, 215, 217 and 219 for the CVD chamber 212, the photolithography station 214, the CMP apparatus 216 and the quality control and packaging line 218, respectively, are connected to the LAN network 240. LAN network 240 connects to local hub 110 by connecting to local hub network 251. Similarly, the resource planning system 222 and the database 221 connect to the local hub 110 through the LAN network 240 and the local hub network 251. Equipment 212, 214, 216 and 218 connect also directly 223 to the local hub network 251 to communicate information that control units 213, 215, 217 and 219 can not or do not process. Other management and control systems and their databases also connect to the local hub network 251, either directly or through the LAN network 240. Operators, manufacturing managers, engineers, sales and business managers associated with the semiconductor fabrication operation 200 have access to the production operation through their personal computers 245 that are also connected to the local hub 110 via LAN network 240 and the local hub network 251. In other embodiments personal computers 245 are directly connected to the local hub network 251.

Local hub 110 includes a database 230, an application server 220, messaging server 210 and a data replication server 215. Local hub network 251 connects database 230, application server 220, messaging server 210 and data replication server 215. Application server 220 includes a computer server and associated equipment, running an operating system and applications that can be accessed by operators associated with the manufacturing operation 200. In one example, the operating system is a Microsoft™ Windows™ NT™ system. Applications running on the application server 220 include access control software, data acquisition software, analytical software, process control software, equipment diagnostic

software, process diagnostic software, yield diagnostic software, knowledge databases, routing and notification instructions, equipment repair and maintenance management software, instructions and manuals, supply chain planning, coordination and procurement software, call center applications and problem management applications. Database 230 stores real-time data and historical data associated with the manufacturing operation 200 and the equipment used in the manufacturing line. Database 230 is managed by database software, such as Microsoft™ SQL Server™.

Access to the production operation includes listening, retrieving and modifying data and issuing and executing control commands. Accordingly, several access levels are defined by segmenting and grouping the various access functions. Operators, manufacturing managers, engineers, sales and business managers are assigned an appropriate access level as a group and also as individual members of a group. This assignment of access functions to each group and each member of a group within the semiconductor fabrication operation 200 is managed by a local profile manager program 606 and is stored in a local people profile database 605, shown in FIG. 6. Local people profile database 605 holds a table defining and mapping operator profiles to access levels. The local profile manager 606 works cooperatively with a central profile manager program 628 to keep people and profile databases synchronized between the local and central hubs, also shown in FIG. 6.

Access control 705 is part of an overall security system 700 that also includes security 710 and authentication 715, shown in FIG. 7. Each member associated with the semiconductor fabrication operation 200, i.e., operators, manufacturing managers, engineers, sales and business managers is assigned a user identification name and a password which are used to authenticate the operator before any further access to the system is allowed. Each authorized user is also connected to one or more profiles or typical groups of access rights. Each such profile gives access rights to specific types of data about specific equipment or classes of equipment via specific functions embodied in specific applications. Every time a member of the semiconductor fabrication operation logs into the local hub 110 through a personal computer 245, he needs to provide his assigned user identification name and password. After this authentication process he is allowed to execute an operation that may include listening, retrieving, altering data or issuing a command. The requested operation is allowed to be executed based on the authentication information combined with the appropriate retrieved access rights that were assigned to the specific member that is requesting the operation. This

process is invoked every time access is requested. The purpose of this overall security system is to maintain control of the production process, to prevent unauthorized access and to protect the "know how" and intellectual property associated with the semiconductor fabrication operation 200.

Local hub 120 is installed at a supplier's site 300 and serves the purpose of centralizing all the local data, information and communication protocols. In one example, local hub 120 is installed at an equipment supplier company 300 that supplies the above-mentioned CVD chamber 212. Supplier site 300 includes R&D and manufacturing facilities 309 for the CVD chambers, a resource planning system 319 that plans and coordinates the CVD chamber manufacturing and a database 330 for storing all the data associated with the CVD chamber manufacturing. A supplier's local network 305 provides connectivity between the CVD chamber manufacturing line 309 and the resource planning system 319. Local network 305 connects to local hub network 340, thus connecting the CVD chamber manufacturing facilities 309 and the resource planning system 319 to the local hub 120. Database 330 connects directly to the local hub network 340 and thus to local hub 120. Operators, manufacturing managers, engineers, sales and business managers associated with the CVD chamber supplier company 300 have access to the manufacturing operation through their personal computers 345 that are also connected to the local hub 120 via the local hub network 340 and supplier local net 305.

Local hub 120 includes a database 330, an application server 320, messaging server 310 and a data replication server 315. Local hub network 340 connects database 330, application server 320, messaging server 310 and data replication server 315. Application server 320 includes a computer server and associated equipment, running an operating system and applications that can be accessed by operators associated with the supplier company 300. In one example, the operating system is a Microsoft™ Windows™ NT™ system. Applications running on the application server 320 include access control software, data acquisition software, analytical software, process control software, equipment diagnostic software, process diagnostic software, yield diagnostic software, knowledge databases, routing and notification instructions, equipment repair and maintenance management software, instructions and manuals, supply chain planning, coordination and procurement software, call center applications and problem management applications.

Local hub 110 of the semiconductor fabrication operation 200 and local hub 120 of the CVD chamber supplier are connected to a central hub 150 via an internet network 160. Security firewalls 162, 164 and 166 are installed between the local hub 110 and the internet network 160, between the local hub 120 and the internet network 160 and between the central hub 150 and the internet network 160, respectively. In one example, internet network 160 is the "Internet" and firewalls 162, 164 and 166 are computers or other digital appliances that run security and encryption software programs. The purpose of the firewalls 162, 164 and 166 is to control and prevent access to the local hubs 110, 120, and central hub 150 by unauthorized external users. Data transmitted through the firewalls 162, 164 and 166 are encrypted for security purposes. In one example, the firewall security and encryption program is Firewall-1 provided by CheckPoint of Redwood City, CA.

Central hub 150 is located at the network provider's site, i.e., AvantNet, and includes a central database 430, a messaging server 410, an application server 420, a data replication server and a LAN network 440 connecting the central database 430 and servers 410, 415 and 420. A firewall 166 is installed between the central hub 150 and the internet network 160. Application server 420 includes a computer server and associated equipment, running an operating system and applications that can be accessed and shared between the local hubs 110 and 120 and other authorized and authenticated users 125 accessing the central hub via the Internet. In one example, the operating system is a Microsoft™ Windows™ NT™ system. Applications running on the application server 420 include access control software, data acquisition software, analytical software, process control software, equipment diagnostic software, process diagnostic software, yield diagnostic software, knowledge databases, routing and notification instructions, equipment repair and maintenance management software, instructions and manuals, supply chain planning, coordination and procurement software, call center applications and problem management applications. Applications running on application server 420 run also on the local hub applications servers 220 and 320. In this way, two layers of application providers are possible, that is an application is hosted at the local hub and the central hub servers. Applications stored at the local hub servers offer a privacy advantage to the manufacturer that owns the local hub, whereas applications stored at the central hub have the advantage of allowing sharing by multiple users while each user's input and output data remain secure at the respective local hubs. In other embodiments, the above mentioned applications are stored only at the central hub applications server 420 and are accessed and shared by the subscribing local hubs 110, 120.

The central database 430 host data from the local hubs 110 and 120 that can be accessed by both the semiconductor fabrication operation 200 and the equipment supplier company 300 based on a contractual arrangement. In some cases a third party 125 is also allowed to access the data stored in the central database 430 based again on contractual arrangements between the third party, the semiconductor fabrication operation 200 and the equipment supplier company 300. The database 430 is managed by database software, such as Microsoft™ SQL Server™. Third party data are also stored at the central database and can be accessed by both the semiconductor fabrication operation 200 and the equipment supplier company 300 based on a contractual arrangement. Real time equipment status data flows from the manufacturer site 200 to the supplier site 300 via the central hub 150, shown schematically by arrow 90. Equipment process and maintenance tips, manuals and training material flow from the supplier site 300 to the manufacturer site 200 via the central hub 150, shown schematically by arrow 92.

Data travels along paths 170 and 172 from the local hub 110 to the central hub 150 and back, respectively, and along paths 174 and 176 from the local hub 120 to the central hub 150 and back, respectively. The data flow includes passive listening and retrieving of data and active altering of data and issuing of commands. Both the passive and active flow of data is managed by a messaging middleware application 411, shown in FIG. 7, that is installed on various servers running applications that need to communicate with each other. In one example, the messaging middleware application 411 is The Information Bus (TIB) supplied by TIBCO Software, Inc., of Palo Alto, CA. In some embodiments, the data transfer process is automated. In one example, the data is a user's manual for a piece of equipment, which is stored in the central database 430 and can be accessed by all manufacturer's that use the specific equipment in their operations and have either a local hub connected to the central hub or have remote dial access to the central hub. Upgrades of the manual are automatically fed to the central database 430 from the equipment supplier 300 and can be accessed by all manufacturers 200 without delay.

A data replication software 416 manages replication and synchronization of data between the local hubs 110, 120 and the central hub 150. The data replication software 416 is installed in the data replication servers 415, 215 and 315 of the central hub server 150 and the local hubs 110 and 120, respectively. Connectivity and administration of the overall network and hub

operations are provided by an internet service provider. In one example the internet service provider is EXODUS, Inc located in Santa Clara, California.

Referring to FIG. 2, a third local hub 130 is installed at a consulting practice 500 where a group of expert scientist and specialists practice. Among the expert scientists and specialists are CVD specialist and semiconductor fabrication experts. These CVD experts have special knowledge that allows them to analyze data from both the semiconductor fabrication operation 200 and the equipment manufacturing 300. In one example, the data from the semiconductor fabrication operation 200 are quality control data for the produced integrated circuit devices and the data from the equipment manufacturing 300 are the specifications of the CVD chamber 212. Based on the analysis of process parameters, quality control data and the CVD chamber 212 specification data, the CVD experts can develop correlations between semiconductor process parameters and integrated circuit device properties and make recommendations regarding appropriate adjustments to equipment design or processing methods. The third local hub 130 includes a server 550 that host applications used for the data analysis, a database 510 that stores results from previous analyses and a LAN network 540 connecting the server 550 and the database 510. In one example, the data analysis software is multi-variant yield management application proprietary to the consulting practice 500. The expert scientists and specialists can access the LAN network 540 via personal computers 520 which are also connected to the local LAN network 540. A firewall 168 is installed between the third local hub 130 and the internet network 160.

Referring to FIG. 3, authorized third parties 140 access data stored in the central hub 150 via remote dial-up to the internet network 160. Third parties 140 include sales representatives, distributors, suppliers for either the integrated circuit devices or the CVD equipment and the consulting service practices. Security, access control and authentication are provided by the access control software 700 installed in the central hub 150 application server 420. Operators, manufacturing managers, engineers, sales and business managers associated with each of the local hubs 110, 120 and 130 have also remote dial-up access to both the central hub 150 and the local hubs via the internet network 160. Data transmitted from the central hub 150 to a user via the internet network 160 are encrypted for security purposes. One example of such encryption is the use of a Virtual Private Network (VPN-1) supplied by CheckPoint, Redwood City, CA. The VPN-1 is installed on the third party computer 140.

Referring to FIG. 4, network 100 includes local hubs 110a-110l associated with Manufacturer1-Manufacturer4 and local hubs 120a-120g associated with Supplier1-Supplier 50. Local hubs110a-110l and local hubs 120a-120g are connected to a central hub 150. Manufacturer1 has three local hubs 110a, 110b and 110c associated with three fabrication facilities Fab1, Fab2 and Fab3, respectively. Fab1, Fab, 2 and Fab3 may be facilities located in the same location or different locations spread out throughout the world. In this latter case, central hub 150 provides a way for Manufacturer1 to have a comprehensive view of all its own facilities. Each equipment supplier Supplier1-Supplier 50 has access to data from multiple manufacturers and each manufacturer Manufacturer1-Manufacturer4 has access to data from multiple suppliers. In this way a single distributed network serves as a data collection and dissemination tool for multiple manufacturers and suppliers, while taking into consideration security concerns. User access profiles are developed for each manufacturer and each supplier and each authorized employee or agent of each manufacturer and each supplier and are stored in the central hub database. The network provides connectivity, shared data structures and real-time data and historical data collection and dissemination. The network 100 also provides analytical tools and third party applications that can be accessed by all subscribers, i.e., suppliers, manufacturers and third party members. Authorized expert scientists, specialists and other authorized third parties have also access to data stored in the central database and provide analysis and solutions to problems associated with the manufacturing operation and the equipment.

Referring to FIG. 5, sensor 211 monitors the operation of a CVD chamber 212. CVD chamber 212 is located in a manufacturer's site Fab1 associated with a local hub 110a, which belongs to an industry-wide network 100, shown in FIG. 4. Network 100 includes multiple manufacturers and suppliers, as described in FIG. 4. When the CVD chamber 212 is in a normal operating mode sensor 211 sends out a signal indicating that the reactor is "UP". This information is collected by both the manufacturer's local hub 110a and the central hub 150 and has a format 560. Other manufacturers and suppliers having similar CVD chamber or reactors 212 also collect in their corresponding local hubs and the central hub 150 the same information. However, the format for the signal indicating normal operation is not universal and can take the forms 562, 564 and 566. In other cases, normal operation of the CVD chamber 212 is indicated by the term "Productive", "Normal" and "aa1" and can take formats 570-574, 580 and 582, respectively. The system of local hubs 110, 120, 130 together with central hub 150 and the applications running on these hubs serve the purpose of mapping

data and formats between manufacturers, suppliers and all other network subscribers so that there is one to one correlation. Interface programs 750 provide the mapping of data and formats between local hubs 110, 120, 130 and central hub 150, shown in FIG. 7. For example, equipment and model identifications, equipment-specific and/or model specific states are mapped between manufacturers standards, supplier's standards and industry specific standards. Similarly identifications of people, manufacturer groups, supplier groups and third party groups are mapped and shared to eliminate redundant data entry into the system.

Referring to FIG. 6, local hub 110 hosts a number of software programs 771, including a repair report manager 602, a business rule manager 604, a local profile manager 606, a static data entry and maintenance 608, analytical tools 610, an equipment log manager 612, a real time monitor 614 and a Fab subscriber 616. Local hub 110 also includes databases or segments of a database 230 that include data associated with the above mentioned software programs. These databases or segments of database 230 contain among others local repair reports 601 generated by the repair report manager 602, local security rules 603 generated by the business rules manager 604, people profiles 605 generated by the local profile manager 606, local business rules 607 generated by the static data entry and maintenance manager, specific machine details 609 generated by the analytical tools 610, historical data 611 generated by the equipment log manager 612, real time status 613 generated by the real time monitor 614 and local equipment log 615 generated by the Fab subscriber 616.

Central hub 150, hosts a number of software programs 770 which can be accessed and shared by each subscribing company including manufacturers, suppliers and other third party members of the network 100. These software programs 770 include an incident knowledge manager 622, a repair report manager 624, a business rule manager 626, a central profile manager 628, a static entry data and maintenance 630, analytical tools 632, an equipment log manager 634, a real time monitor 636, and a central subscriber 634. Central database 430 includes separate database segments 780a, 780b, 780c for each subscribing local hub 110, 120, 130, respectively. In other embodiments, database segments 780a, 780b, 780c are separate databases. Database segments 780a, 780b, 780c contain data associated with the above mentioned software groups for each subscribing company. These data include diagnostic and repair knowledge 621 generated by the knowledge manager 622, central repair reports 623 generated by the repair report managermanager 624, subscribing company

security rules 625 generated by the business rules manager 626, people profiles 627 generated by the central profile manager 628, subscribing company business rules 629 generated by the static data entry and maintenance manager 630, general machine model details 631 generated by the analytical tools 632, historical data 633 generated by the equipment log manager 634, real time status 635 generated by the real time monitor 636 and central equipment log 637 generated by the central subscriber 638.

Repair report managers 602 and 624 manage the mechanism for entering the details of scheduled and unscheduled equipment repairs. They are available via both the local hub and the central hub so that entries can be made by fab technicians and operators who may only have access to the local hub 110 and also by equipment supplier technicians and operators who may only have access to the central hub 150. Central hub and local hub repair report managers share a common database 623. Local repair reports database 601 has only those entries pertaining to the equipment associated with the local hub 110. Central repair report database 623 is segregated by equipment supplier and includes entries for all equipment associated with a specific equipment supplier. Repair report managers 602 and 624 provide a structured format with prompts to capture symptoms, diagnosis and probable cause, repair and results. Repair report managers 602 and 624 also generate repair reports that include equipment identification, operator identification at time of failure and at completion of repair, time stamps marking time to response, time to repair and billable time and input about the symptoms, diagnosis, repair actions, results, replaced parts and applied upgrades. Repair report managers 602 and 624 also maintain records on consumables, processes, metrology, yield analysis, Failure Reporting Analysis & Corrective Action System (FRACAS) and repair knowledge base.

Incident knowledge manager 622 is a knowledge engine designed to improve the diagnosis process. It assists repair technicians in determining probable causes and suggests adjustments or repairs for observed symptoms based on historical data.

Local profile manager 606 creates and updates data stored in the local people profile database 605. Local people profile database 605 holds information about who is authorized to use which functionality within which application to view or manipulate which data about which equipment, who has local access and to what, who needs to be alerted internally or externally in case of a problem and who needs to be notified at which escalation level.

Central profile manager 628 creates and updates data stored in the central people profile database 627. Central people profile database 627 holds information about individual person set-up, individual to equipment supplier relation, individual to equipment relation, who has central access and to what, company specific alerting and escalation profiles and individual to profile assignment. The central profile manager 628 and the central profile database 627 have similar functionality and data as the local profile manager 606 and local profile database 605. The central profile manager 628 has the additional function of coordinating with the local profile manager 606 in order to disseminate, replicate and synchronize profile changes made to any local database 605 at any local hub. In one example, changes in access rights and profiles caused by employee turnover at equipment supplier site 120 are made available to manufacturer site 110 in real time. This is particularly useful if the concerned employee had access rights to local hub 110 because of his or her employment with supplier 300.

Local business rules manager 604 creates and updates data stored in the local business rules database 607 and local security rules database 603. Local business rules database 607 holds information about alerting rules, escalation rules, shift hours and shift end procedures, arbitration rules that are unique to that local hub. Local security database 603 holds information about the local hub security rules. In one example, local security database holds the local security rules about inbound and outbound messages between that local hub and all other local and central hubs. In this example such rules include rules about who is allowed to originate messages across the local hub firewall, in which direction, containing what data, addressed to which recipient, at which network address. The local business rules manager 604 also manages and enforces the security rules and business rules at that local hub. In one example, the business rules manager employs the services of a subsidiary application or module or sub module to manage specific rules at the site so as to take advantage of specialized capabilities of such subsidiary applications. In this example an access control application or module manages the access control rules while another subsidiary application manages the arbitration rules. In this example the use of specialized subsidiary applications or modules or sub modules extends to multiple layers of specialization. In this example the specialized sub function of operator authentication by use of digital certificates or digital keys is delegated to a module specializing in this capability. In another example the maintenance and management of arbitration rules governing the correction and revision of previously recorded equipment history is delegated to a specialized module while the maintenance and

management of remote diagnostics rules is managed by another set of subsidiary applications or modules or sub modules. In this example the rules governing the supply chain or procurement processes is managed by yet another set of subsidiary applications or modules or sub modules. In this example a single business process makes the use of specialized sub modules from many different primary applications.

Central business rules manager 626, the central business rules database 629 and central security rules database 625 have similar functionality and responsibilities as the local business rules manager 604 , the local business rules database 607 and local security rules database 603. The central business rules manager 626, the central business rules database 629 and central security rules database 625 have the additional function and responsibilities of coordinating with the local business rules manager 604 in order to disseminate, replicate and synchronize business rule changes and usage at any local hub. Referring to FIGS. 1 and 6, in one example, an operator connected to local hub 120 requests to revise the stored historical data of a CVD chamber that is connected to local hub 110. The request is relayed to an appropriate expert at the manufacturer 200 through collaboration and discharge of appropriate responsibilities by the local business rules manager 604 at local hub 120, the central business rules manager 626 at central hub 150 and the local business rules manager 604 at local hub 110. In another example, an authorized expert at supplier company 300 changes the remote diagnostic procedures in the local business rules database 607 of local hub 120. The changes in the remote diagnostic procedures are then replicated by the central business rules manager 626 in the central business rules database 628 through a collaboration between the local business rules manager 603 at local hub 120 and the central business rules manager 626. Further the central business rules manager 626 collaborates with the local business rules manager 603 at local hub 110 to replicate the changes in the remote diagnostic procedures from the central business rules database 628 to the local business rules database 607 at local hub 110. In another example, an authorized expert at manufacturer 200 initiates a Request For Proposal (RFP). The request is replicated from the local business rules database 607 at manufacturer local hub 110 to the central business rules database 628 through collaboration between the local business rules manager 603 at local hub 110 and the central business rules manager 626. Further the central business rules manager 626 collaborates with the local business rules managers 603 located at all local hubs that are connected to the central hub 150 to automatically replicate any changes from the central business rules

database 628 to the local business rules databases 607, based upon qualification rules that are stored in the local business rules databases 607.

Local static data entry and maintenance 608 creates and updates information in the specific equipment details database 609. Specific equipment details database 609 holds information about specific manufacturer's designation for the equipment, equipment supplier's designation for the equipment, equipment serial number, model, equipment manufacturing company, equipment profile parameters, equipment state model, operator and technician profiles, warranty, contact information and service contract code and coverage. Equipment database 609 also holds the equipment state format translation table.

Central static data entry and maintenance 630 creates and updates information in the general model details database 631. General model details database 631 holds information about equipment supplier's designation for the supplier's equipment models, possible model configurations and their associated specifications, subsystem and sub assembly details, drawings, training and manuals.

At the end of each manufacturing shift, local equipment log manager 612 summarizes the local equipment usage and creates shift totals for each piece of equipment including data required for calculating availability and reliability reports and metrics such as Mean Time Between Failures (MTBF) and Mean Time To Repair (MTTR). It also writes these shift totals to a summary report, causes posting of new availability, reliability and overall equipment effectiveness reports, tracks open and incomplete repair reports and generates alerts and escalations for tardy repair reports. This information is stored in appropriate local databases such as the local equipment log database 615.

Central equipment log manager 634 receives updated information from all the local equipment log managers and updates information in the central equipment log database 637. The central equipment log database 637 holds data similar to the data held by the local equipment log database 615. However, the local equipment log database 615 holds data about all the equipment connected to that local hub regardless of the equipment supplier, whereas the central hub has a separate equipment log database 637 for each equipment supplier that supplies equipment connected to any local hub. Such a supplier specific database is also replicated and stored at the supplier local hub. Similarly, the central hub 150 has a separate

equipment log database 637 for each manufacturer that is connected to the central hub. A key responsibility of the central equipment log manager 634 is to receive updates from all local hubs and to post the new data to each appropriate subscriber's equipment log database.

Fab subscriber 616 manages real-time data acquisition and dynamic transfer within the local hub 110. Subscriber 616 listens to messages on the local LAN 240. In one example the subscriber 616 uses TIB to listen to the appropriate authorized messages, queues up the messages so that none is lost until all appropriate databases are updated, sends a message to an "alert" engine when a machine goes from any "up" state to any unscheduled "down" state and updates the local databases.

Central subscriber 638 listens to messages from the data replication engine on the central TIB, queues up the messages so that none are lost until all appropriate databases are updated, and updates the central databases.

Local real time monitor 614 queries the local real time status table 613 and other related databases and displays current status of a specific equipment to all authorized operators. The data are stored in the manufacturer's real time status database 613. Central real time monitor 636 displays current status for a specific machine based upon real time status database 635 to all authorized personnel .

Analytical tools 610 and 632, stored in local hub 110 and central hub 150, respectively include software packages used in analyzing production data, such as statistical analysis programs.

Referring to FIG. 7, central hub 150 includes the following software modules that were generally described in the Business Rules Manager 604, 626 description. Security and access control 700, interfaces 750, arbitration 720 and messaging middleware application 411. These software modules are also hosted in local hubs 110 and 120 (not shown). Security and access control 700 includes access control 705, authentication 715 and security 710. Security 710 provides encryption and firewall management. In one example, the firewall security and encryption program is Firewall-1 provided by CheckPoint of Redwood City, CA, and the authentication program 715 is SiteMinder, supplied by Netegrity, Waltham, MA. Arbitration 720 includes a group of software programs used in managing the

business rules applicable at each of central hub 150 and local hubs 110 and 120. Applications 770 include the software programs described in FIG. 6. Interfaces 750 include a group of software programs that provide application to application or machine to application connectivity between machines and application used by manufacturers, suppliers and all other network subscribers so that there is only one way in which each machine or applications needs to communicate to any other application. Passive and active flow of data is managed by a messaging middleware application 411 that is installed in the messaging server 410. In one example, the messaging middleware application 411 is The Information Bus (TIB) supplied by TIBCO Software, Inc., of Palo Alto, CA.

The many features and advantages of the present invention are apparent from the detailed specification, and, thus, it is intended by the appended claims to cover all such features and advantages of the described apparatus that follow the true spirit and scope of the invention. Furthermore, since numerous modifications and changes will readily occur to those of skill in the art, it is not desired to limit the invention to the exact construction and operation described herein. Accordingly, other embodiments are within the scope of the following claims.

What is claimed is:

1. An industry wide system for collecting and distributing real-time data in a secure and differentiated manner comprising:
   a) a central network having a database for receiving real-time data; and
   b) a first local network collecting a first set of real-time data according to a first format and transmitting said first set of real-time data to said central network database via a secure transmission mode; and
   wherein access to said database and real-time data is controlled.

2. The system of claim 1 wherein said access to said database is controlled by an access control program.

3. The system of claim 1 wherein said access to said database is controlled according to prearranged rules, wherein said rules are implemented by an access control program.

4. The system of claim 1 wherein an operator accesses said database and said real-time data remotely.

5. The system of claim 1 wherein an operator accesses said database and said real-time data remotely via an internet network.

6. The system of claim wherein said real-time data are proprietary.

7. The system of claim 1 wherein said secure transmission mode comprises:
   a) encryption of said real-time data; and
   b) transmission of said encrypted data via an internet network.

8. The system of claim 1 further comprising:
   a) a second local network collecting a second set of data according to a second format and transmitting said data to said central network database via a secure transmission mode.

9. The system of claim 8 wherein a first and second operators connected to said first and second local networks, respectively, have access to said central network database and said first and second set of data.

10. The system of claim 1 wherein said first local network is located at a manufacturing company.

11. The system of claim 10 wherein said real-time data comprise real-time manufacturing process parameters.

12. The system of claim 8 wherein said second local network is located at an equipment supplying company.

13. The system of claim 12 wherein said second set of data comprises equipment related data.

14. An industry wide system for collecting and distributing real-time data comprising:

a) a central network having a database for receiving real-time data and wherein access to said database and real-time data is controlled;

b) a first local network collecting and transmitting a first set of real-time data to said central network database via a secure transmission mode;

c) a second local network transmitting a second set of data to said central network database via said secure transmission mode; and

wherein a first and second operators connected to said first and second local networks, respectively, have access to said central network database and said first and second set of data and wherein said access is controlled according to pre-arranged rules and said rules are implemented by an access control program.

15. An industry wide system for collecting and distributing real-time data comprising:

a) a central network having a database for receiving real-time data and wherein access to said database and real-time data is controlled;

b) a plurality of local networks collecting and transmitting a plurality of real-time data to said central network database via a secure transmission mode; and

wherein an operator connected to at least one of said local networks has access to said central network database and said plurality of data and wherein said access is controlled according to pre-arranged rules and said rules are implemented by an access control program.

16. The system of claim 1 further comprising a messaging software for receiving and transmitting real-time data.

17. The system of claim 1 further comprising an encryption software for encrypting and decrypting said transmitted and received real-time data, respectively.

18. The system of claim 1 further comprising a repair report managing software.

19. The system of claim 1 further comprising a business rules managing software, said business rules software comprising specialized subsidiary applications for security, access control and arbitration .

20. The system of claim 1 further comprising a people profile managing software.

21. The system of claim 1 further comprising a static data entry managing software.

22. The system of claim 1 further comprising a real time monitor software.

23. The system of claim 1 further comprising an equipment logging managing software.

24. The system of claim 1 further comprising an incident managing software.

25. The system of claim 1 further comprising analytical software for analyzing said real-time data.

26. The system of claim 1 further comprising subscribing software for listening, queuing and updating said real-time data in said database.

27. The system of claim 1 further comprising a network and a data replication software for providing security, redundancy, scalability, back-up, recovery, replication and synchronization of data.

28. A method for collecting and distributing real-time data comprising:
a) providing a central network having a database for receiving real-time data and a controlled access to said database and said real-time data;
b) providing a first local network for collecting a first set of real-time data according to a first format; and
c) transmitting said first set of real-time data to said central network database via a secure transmission mode.

29. The method of claim 28 wherein said access to said database is controlled by an access control program.

30. The method of claim 28 wherein said access to said database is controlled according to prearranged rules, wherein said rules are implemented by an access control program.

31. The method of claim 28 further comprising accessing said database and said real-time data remotely.

32. The method of claim 28 further comprising accessing said database and said real-time data remotely via an internet network.

33. The method of claim 28 wherein said real-time data are proprietary.

34. The method of claim 28 wherein said secure transmission mode comprises:
a) encrypting said real-time data; and
b) transmitting said encrypted data via an internet network.

35. The method of claim 28 further comprising:
a) providing a second local network for collecting a second set of data according to a second format; and

b) transmitting said second set of data to said central network database via a secure transmission mode.

36. The method of claim 35 further comprising accessing said central network database and said first and second set of data by first and second operators connected to said first and second local networks, respectively.

37. The method of claim 28 wherein said first local network is located at a manufacturing company.

38. The method of claim 37 wherein said real-time data comprise real-time manufacturing process parameters.

39. The method of claim 35 wherein said second local network is located at an equipment supplying company.

40. The method of claim 35 wherein said second set of data comprises equipment related data.

41. A method for collecting and distributing real-time data comprising:

a) providing a central network having a database for receiving real-time data and wherein access to said database and real-time data is controlled;

b) providing a first local network for collecting a first set of real-time data;

c) transmitting said first real-time data to said central network database via a secure transmission mode;

d) providing a second local network for collecting a second set of real-time data;

e) transmitting said second set of data to said central network database via said secure transmission mode; and

wherein first and second operators connected to said first and second local networks, respectively, have access to said central network database and said first and second set of data and wherein said access is controlled according to pre-arranged rules and said rules are implemented by an access control program.

42. A method for collecting and distributing real-time data comprising:

a) providing a central network having a database for receiving real-time data and wherein access to said database and real-time data is controlled;

b) providing a plurality of local networks collecting and transmitting a plurality of real-time data to said central network database via a secure transmission mode; and

wherein operators connected to at least one of said local networks have access to said central network database and said plurality of data, wherein said access is controlled according to pre-arranged rules and said rules are implemented by an access control program.

43. The method of claim 28 further comprising a messaging software for receiving and transmitting real-time data.

44. The method of claim 28 further comprising an encryption software for encrypting and decrypting said transmitted and received real-time data, respectively.

45. The method of claim 28 further comprising a repair report managing software.

46. The method of claim 28 further comprising a business rules managing software.

47. The method of claim 28 further comprising a people profile managing software.

48. The method of claim 28 further comprising a static data entry managing software.

49. The method of claim 28 further comprising a real time monitor software.

50. The method of claim 28 further comprising an equipment logging managing software.

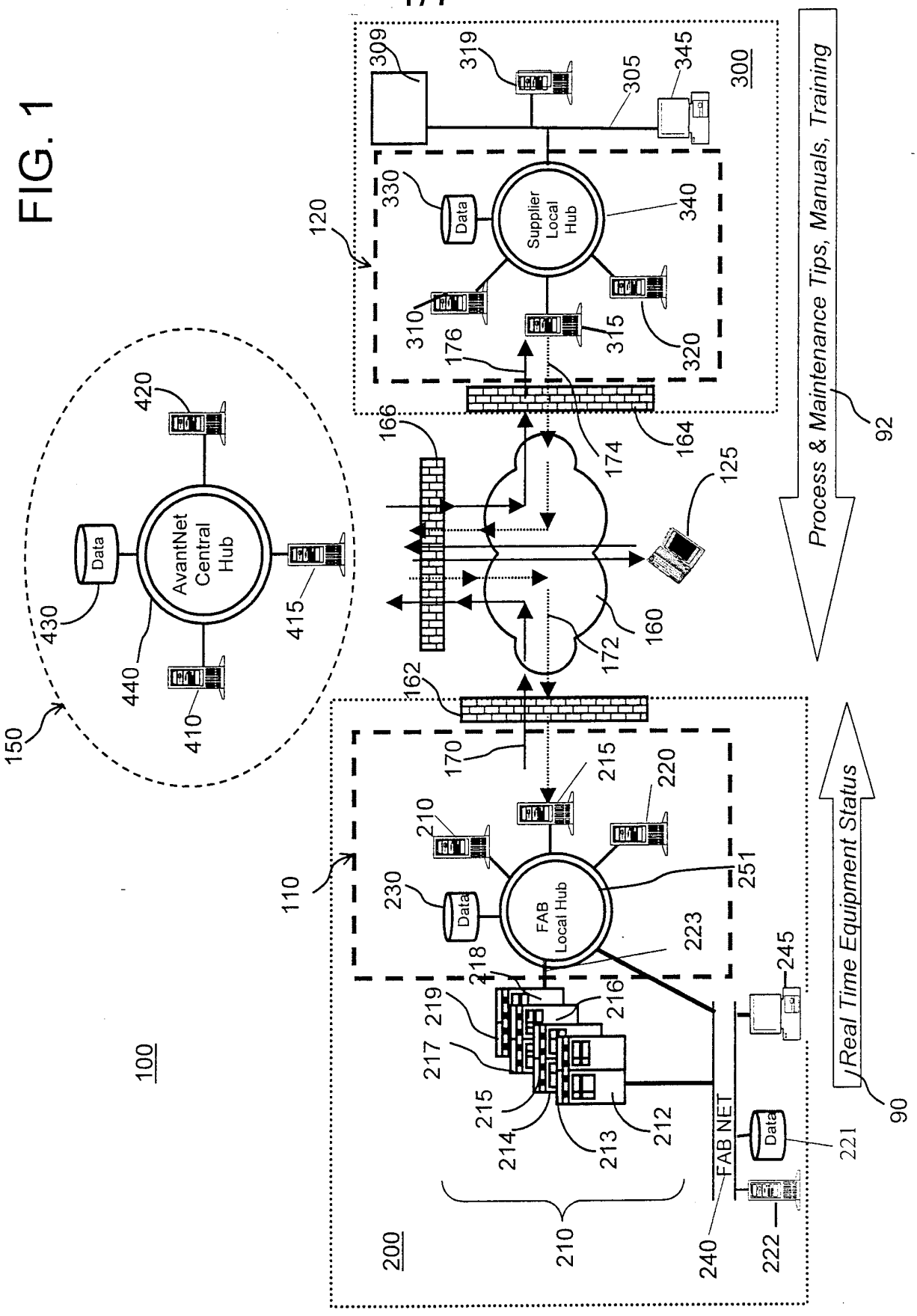
51. The method of claim 28 further comprising an incident managing software.

52. The method of claim 28 further comprising analytical software for analyzing said real-time data.

53. The method of claim 28 further comprising subscribing software for listening, queuing and updating said real-time data in said database.

54. The method of claim 28 further comprising a data replication software for providing security, redundancy, scalability, back-up, recovery, replication and synchronization of data.

FIG. 1


100
150
AvantNet Central Hub
Data
420
430
440
410
415
120
300
309
319
305
345
330
Data
Supplier Local Hub
340
310
315
320
176
166
174
164
125
160
172
162
170
110
200
FAB Local Hub
Data
210
215
220
230
251
223
218
245
216
219
217
215
214
213
212
210
FAB NET
240
221
Data
222
Process & Maintenance Tips, Manuals, Training
92
Real Time Equipment Status
90

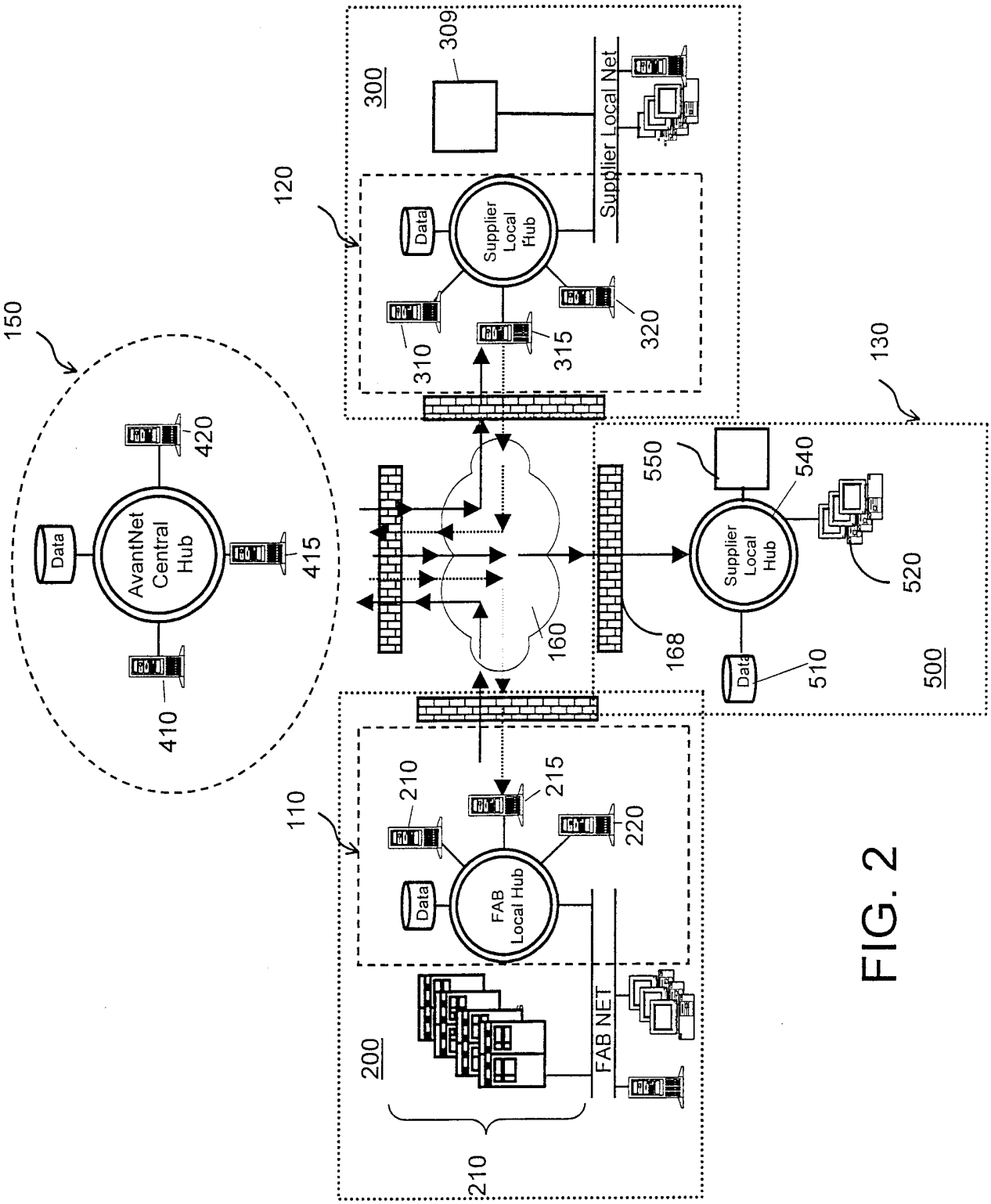

150
AvantNet Central Hub
Data
420
415
410
120
300
309
Supplier Local Net
Supplier Local Hub
Data
310
315
320
130
550
540
Supplier Local Hub
520
Data
510
500
160
168
110
210
215
220
FAB Local Hub
Data
200
FAB NET
210

FIG. 2

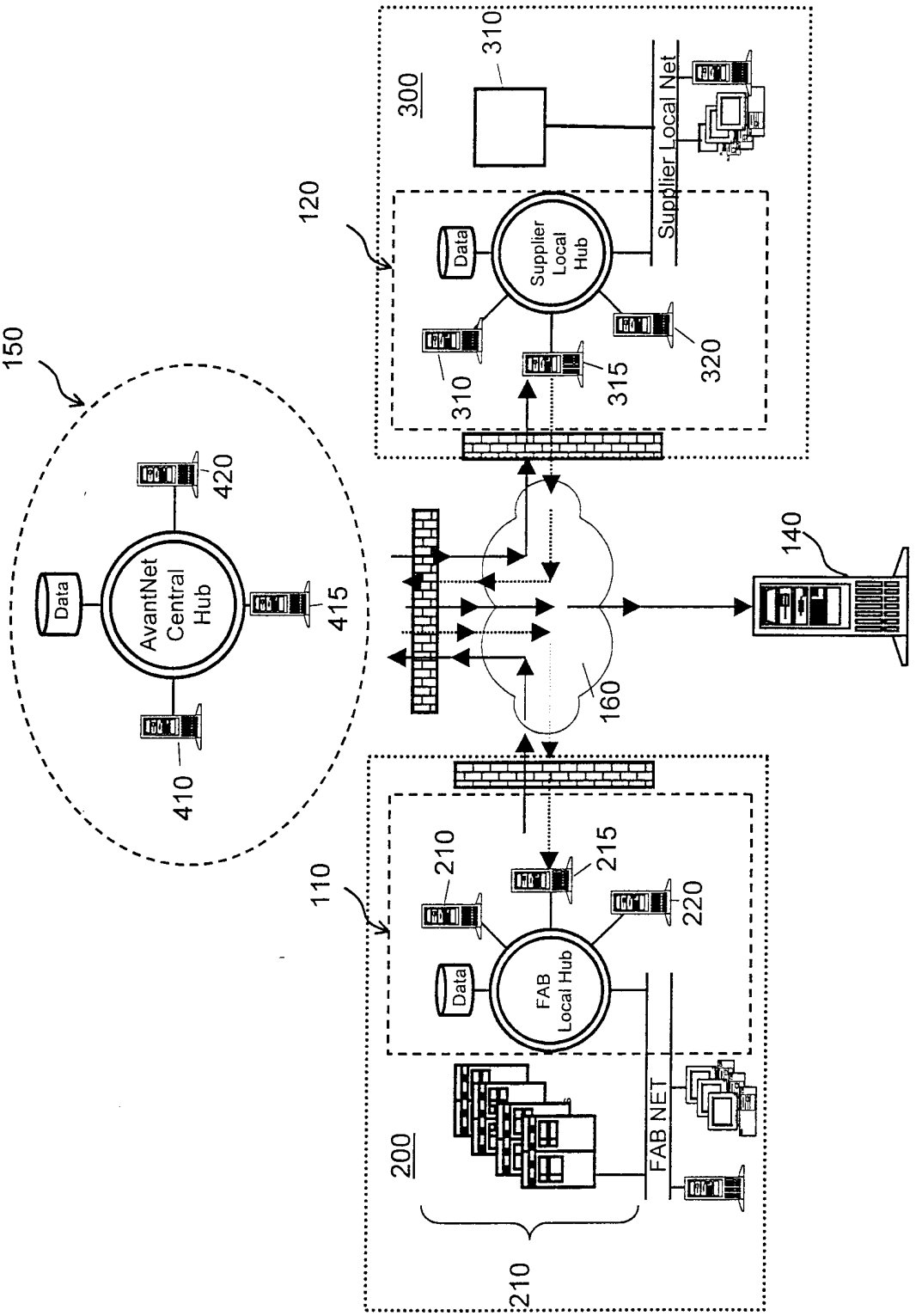

150
AvantNet Central Hub
Data
420
415
410
120
300
310
Supplier Local Net
Supplier Local Hub
Data
310
315
320
140
160
110
210
215
220
FAB Local Hub
Data
200
FAB NET
210

FIG. 3

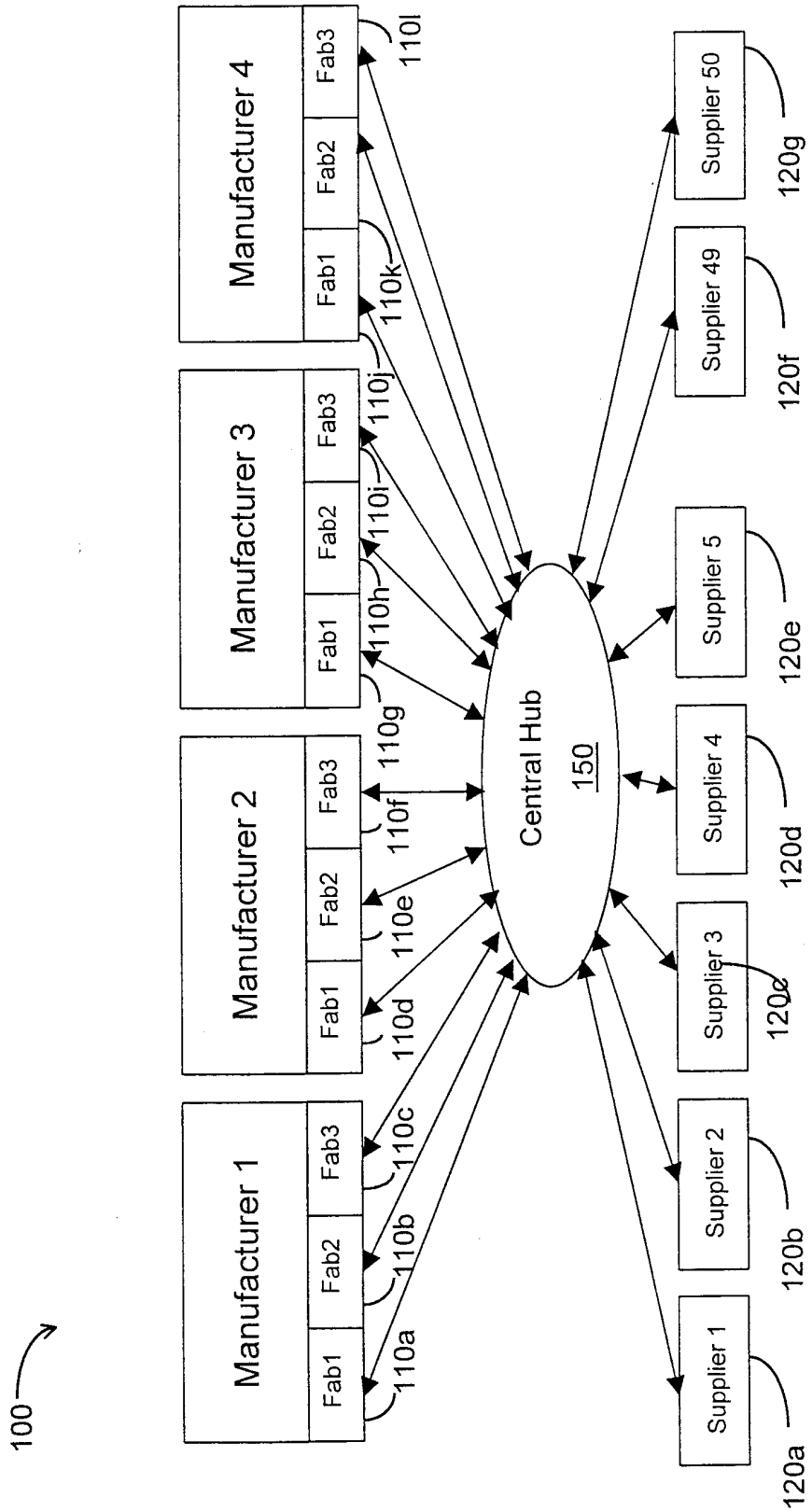

100
Manufacturer 1
Fab1
Fab2
Fab3
110a
110b
110c
Manufacturer 2
Fab1
Fab2
Fab3
110d
110e
110f
Manufacturer 3
Fab1
Fab2
Fab3
110g
110h
110i
Manufacturer 4
Fab1
Fab2
Fab3
110j
110k
110l
Central Hub
150
Supplier 1
120a
Supplier 2
120b
Supplier 3
120c
Supplier 4
120d
Supplier 5
120e
Supplier 49
120f
Supplier 50
120g

FIG. 4

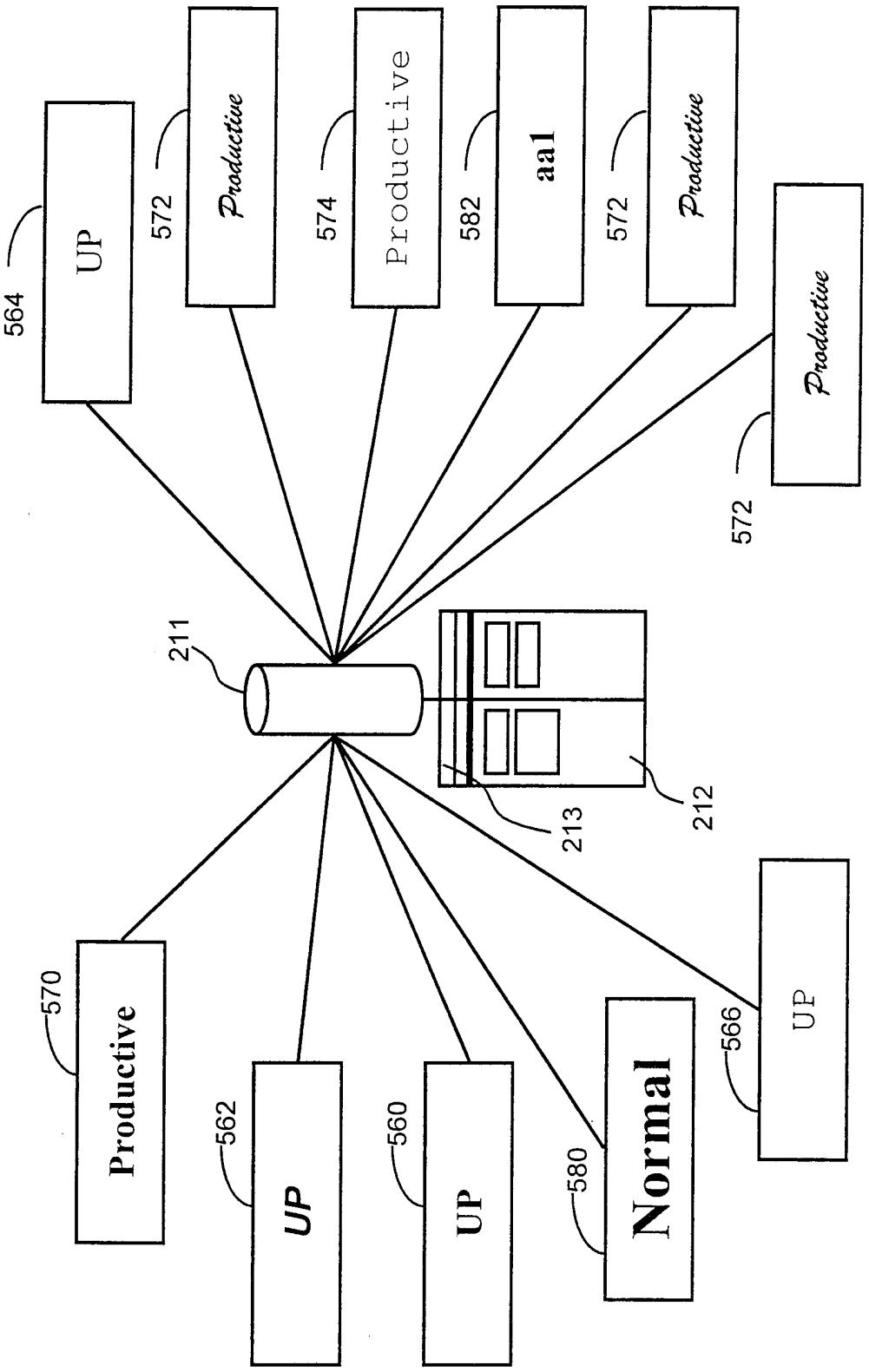

564
UP
572
Productive
574
Productive
582
aa1
572
Productive
572
Productive
211
213
212
570
Productive
562
UP
560
UP
580
Normal
566
UP

FIG. 5

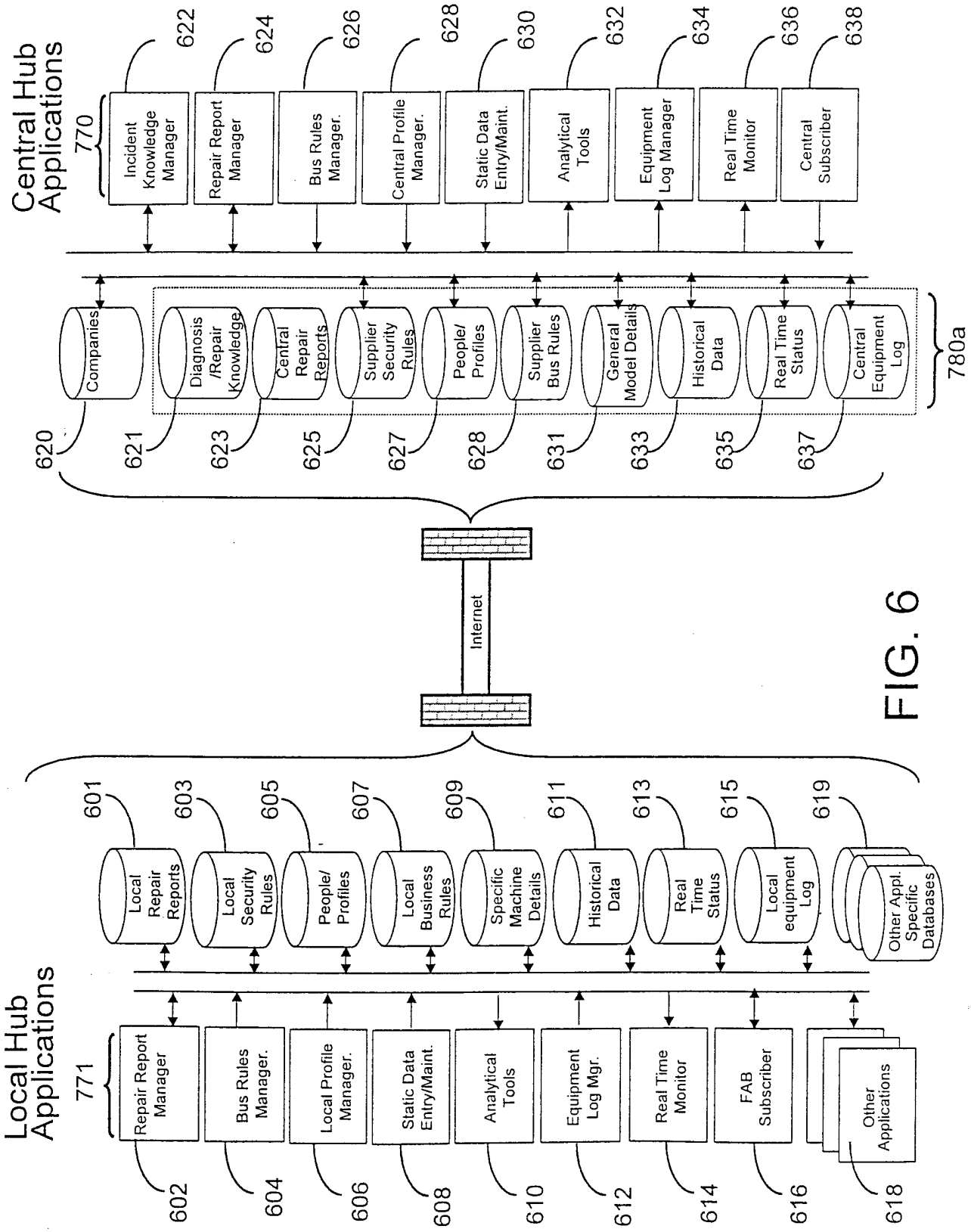

Central Hub Applications
770
Incident Knowledge Manager
Repair Report Manager
Bus Rules Manager.
Central Profile Manager.
Static Data Entry/Maint.
Analytical Tools
Equipment Log Manager
Real Time Monitor
Central Subscriber
622
624
626
628
630
632
634
636
638
Companies
Diagnosis /Repair Knowledge
Central Repair Reports
Supplier Security Rules
People/ Profiles
Supplier Bus Rules
General Model Details
Historical Data
Real Time Status
Central Equipment Log
780a
620
621
623
625
627
628
631
633
635
637
Internet
Local Hub Applications
771
Repair Report Manager
Bus Rules Manager.
Local Profile Manager.
Static Data Entry/Maint.
Analytical Tools
Equipment Log Mgr.
Real Time Monitor
FAB Subscriber
Other Applications
602
604
606
608
610
612
614
616
618
Local Repair Reports
Local Security Rules
People/ Profiles
Local Business Rules
Specific Machine Details
Historical Data
Real Time Status
Local equipment Log
Other Appl. Specific Databases
601
603
605
607
609
611
613
615
619

FIG. 6

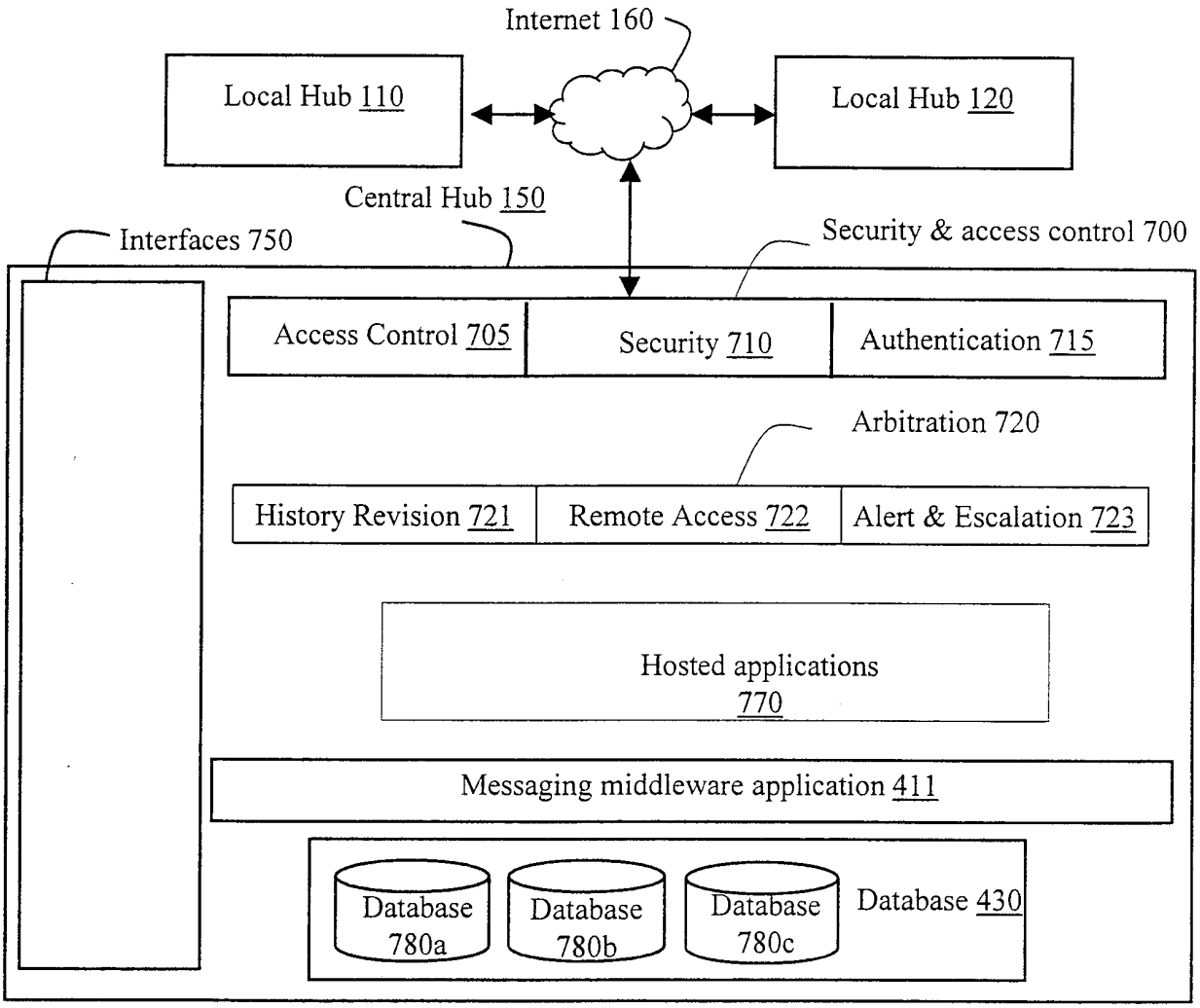

Internet 160
Local Hub 110
Local Hub 120
Central Hub 150
Interfaces 750
Security & access control 700
Access Control 705
Security 710
Authentication 715
Arbitration 720
History Revision 721
Remote Access 722
Alert & Escalation 723
Hosted applications 770
Messaging middleware application 411
Database 780a
Database 780b
Database 780c
Database 430

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/41796

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 13/00, 17/30; H04N 7/167
US CL :709/200; 707/4, 9, 10, 104; 380/5

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. : 709/200; 707/4, 9, 10, 104; 380/5

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

NONE

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

WEST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,742,762 A (SCHOLL et al.) 21 April 1998, the entire paper is relevant	1-41
Y	US 5,899,990 A (MARITZEN et al.) 04 May 1999, the entire paper is relevant	1-41
Y	US 5,819,271 A (MAHONEY et al.) 06 October 1998, the entire paper is relevant	1*41
Y	US 5,778,368 A (HOGAN et al.) 07 July 1998, the entire paper is relevant	1-41
Y	US 5,734,719 A (TSEVDOS et al.) 31 March 1998, the entire paper is relevant	1-41

[X] 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)	"&"	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
07 APRIL 2001

Date of mailing of the international search report
27 APR 2001

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
THOMAS BLACK
Peggy Harod

Telephone No. (703) 305-9707

Form PCT/ISA/210 (second sheet) (July 1998) ★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/41796

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,864,871 A (KITAIN et al.) 26 January 1999, the entire paper is relevant	1-41
Y	WO 98/44694 A1 (BECKETT ET AL.) 08 October 1998, the entire paper is relevant	1-41