US005867714A

United States Patent [19]

Todd et al.

[11] Patent Number: 5,867,714

[45] Date of Patent: Feb. 2, 1999

[54] **SYSTEM AND METHOD FOR DISTRIBUTING CONFIGURATION-DEPENDENT SOFTWARE REVISIONS TO A COMPUTER SYSTEM**

[75] Inventors: **David K. Todd**, Atlanta, Ga.; **Michael R. Terrell**, Spencerport, N.Y.

[73] Assignee: **NCR Corporation**, Dayton, Ohio

[21] Appl. No.: **740,584**

[22] Filed: **Oct. 31, 1996**

[51] **Int. Cl.**[6] **G06F 9/445**

[52] **U.S. Cl.** **395/712**; 395/500; 395/651; 395/653; 707/10; 707/104; 707/201; 707/203

[58] **Field of Search** 395/712, 500, 395/651, 653, 200.5, 200.51–200.54, 200.47–200.49, 182.01, 182.05, 183.01, 183.03, 183.07, 183.13, 183.14, 183.2, 184.01, 828, 830; 707/1, 10, 104, 200, 201, 203; 364/550, 551.01, 944.61, 946.1, 949.4, 191, 192, 131, 132, 138, 147, 184; 702/119, 112, 123, 183–186, 188

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,019,963	5/1991	Alderson et al.	707/201
5,155,847	10/1992	Kirouac et al.	395/200.51
5,247,683	9/1993	Holmes et al.	395/200.51
5,287,505	2/1994	Calvert et al.	707/10
5,579,529	11/1996	Terrell et al.	395/828
5,619,716	4/1997	Nonaka et al.	395/712
5,664,093	9/1997	Barnett et al.	395/183.07

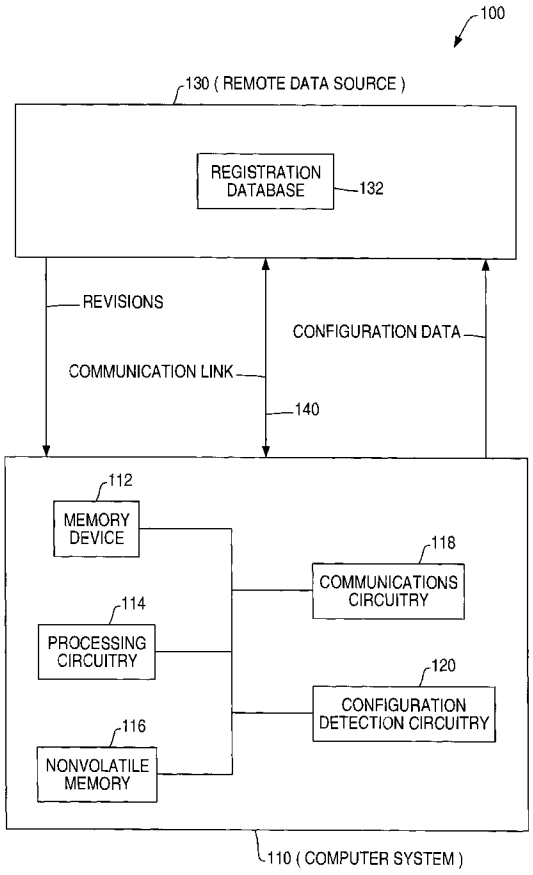
Primary Examiner—Hal Dodge Wachsman

Attorney, Agent, or Firm—William A. Munck

[57] **ABSTRACT**

There is disclosed a system for detecting and avoiding faults stemming from conflicts in hardware and/or software configurations in a computer system. The system comprises communications circuitry that, from time to time, automatically transmits at least part of the current hardware and software configuration data of the computer system to a remote data source capable of identifying inherent conflicts in the hardware and software configuration. The remote data source then transmits to the computer system software revisions that are capable of resolving the inherent conflicts. After the communications circuitry receives the software revisions, processing circuitry in the computer system modifies the current software configuration according to the received software revisions.

20 Claims, 3 Drawing Sheets

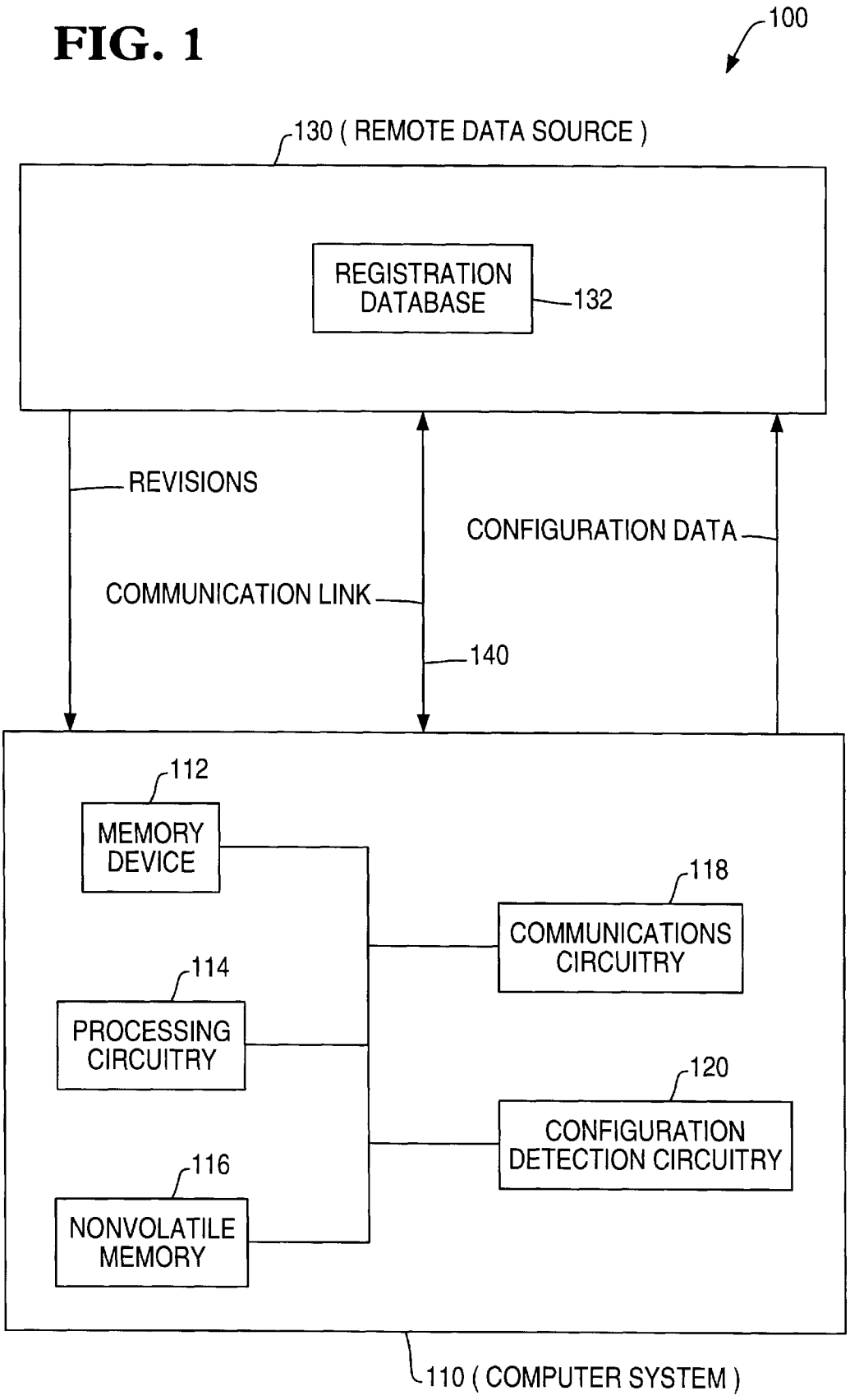


MICROSOFT CORP.
EXHIBIT 1006

DOCKET ALARM

Find authenticated court documents without watermarks at docketalarm.com.

FIG. 1



DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

FIG. 2A

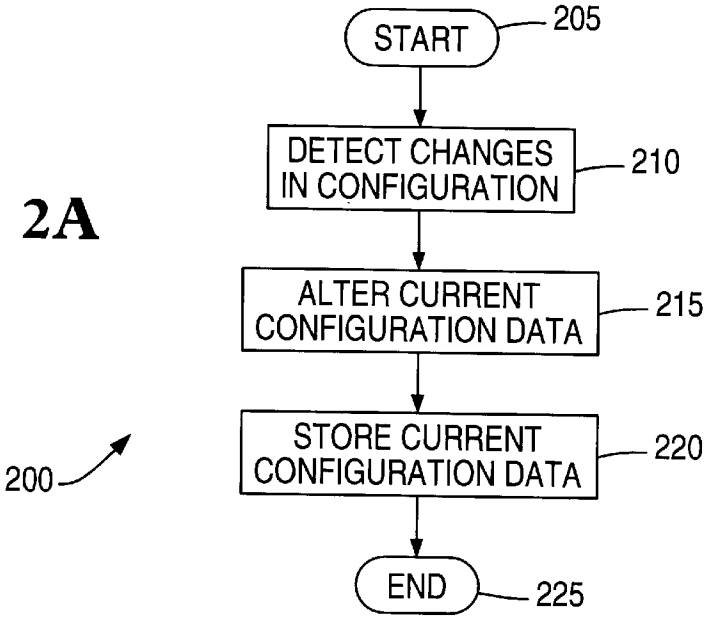
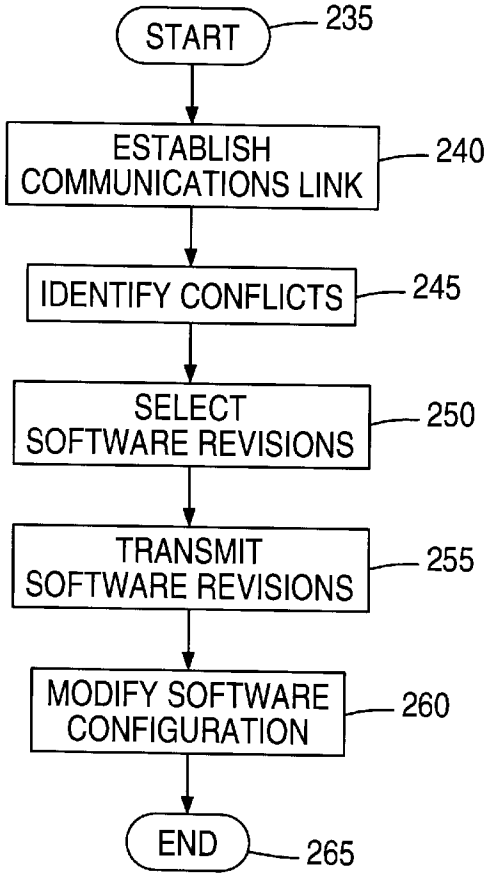
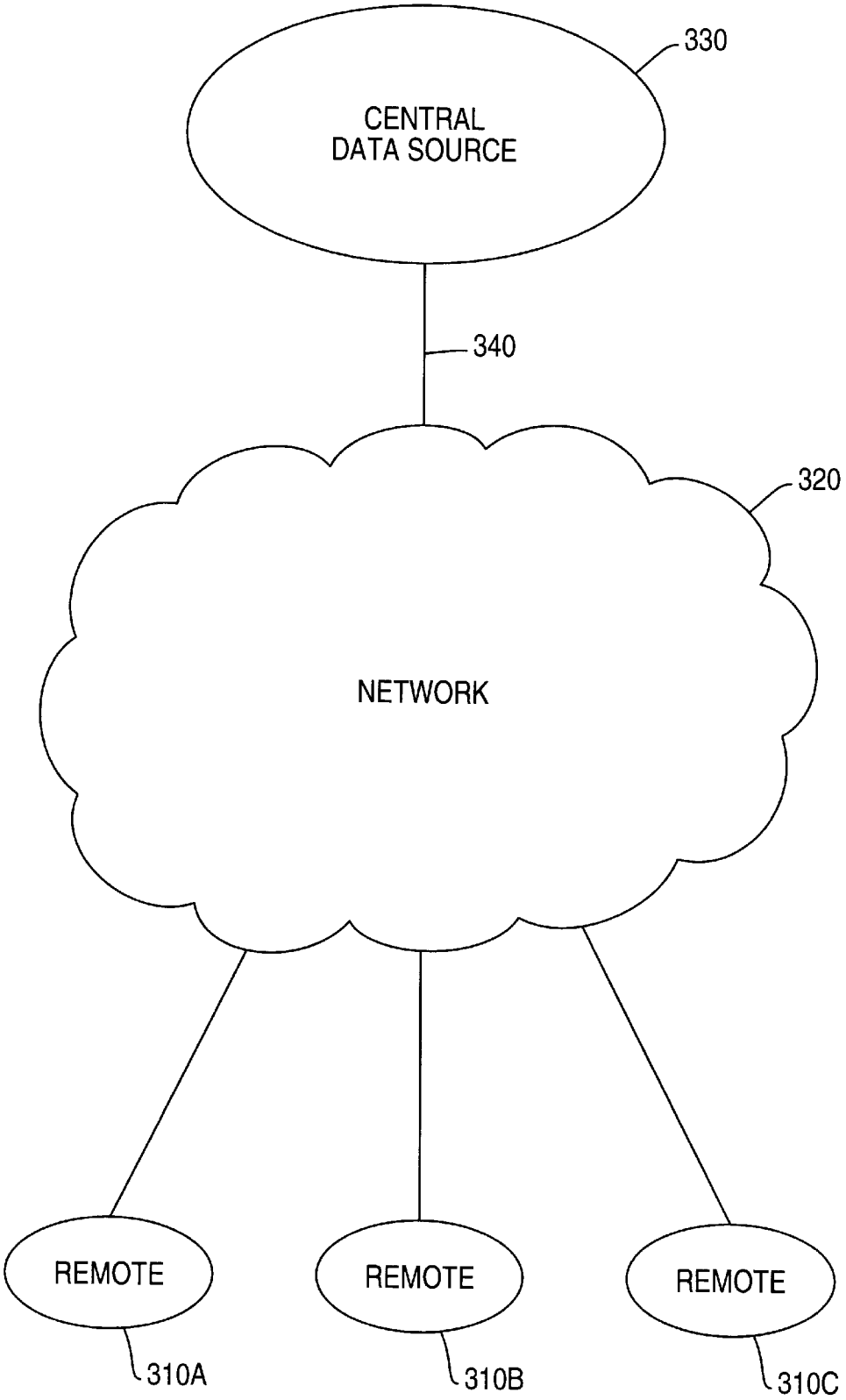


FIG. 2B



DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

FIG. 3



DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

SYSTEM AND METHOD FOR DISTRIBUTING CONFIGURATION-DEPENDENT SOFTWARE REVISIONS TO A COMPUTER SYSTEM

TECHNICAL FIELD OF THE INVENTION

The present invention is directed, in general, to a computing apparatus and, more specifically, to a computer system capable of distributing or receiving software revisions that are a function of a specific system hardware and software configuration.

BACKGROUND OF THE INVENTION

Immeasurable gains in technology offered in personal computers ("PCs") have allowed PCs to assume roles performed only by mainframe or minicomputers in the past. Many companies and individual users rely solely on commercially-available PCs, such as those provided by NCR, to meet their information processing needs. Thus, it is vital that their PCs perform reliably. If, however, a PC experiences a fault, it is equally vital that the PC communicate existence of the fault to inform the user of a need to repair the fault so the PC can return to active service. For computer systems in general, it is most helpful for the computer system itself to provide an indication of the specific location and nature of the fault to help the user more quickly isolate and more economically repair the fault. To that end, today's PCs are typically equipped with some form of internal diagnostics, the purpose of which is to detect and subsequently isolate specific hardware and software component failures and faults brought about by interactions among the PC's hardware and software components (so-called "conflicts" leading to so-called "configuration faults").

For years, PCs have been provided with diagnostic routines that test and report on the operational status or functionality of hardware and software components within the computer, allowing a user to repair or replace hardware or software components that are not functioning to the desired degree or to resolve certain conflicts manually.

As PC systems become more and more complex and as users come more and more to rely on the services of remote, skilled technicians to maintain and repair their PCs, it is growing less desirable to force the user to diagnose PC faults alone. The general direction in the development of diagnostic software systems to this point has been to isolate the user somewhat from the intricate and technically complex operations of diagnostic routines by: (1) providing more user-friendly diagnostic programs to the user, with interfaces written in clear text and presented in an aesthetically pleasing manner and (2) providing remote diagnostic capability so the remote technician may query the PC directly and determine faults without the user's substantial participation. However, the user is still forced to undergo a fault and contact a remote technician for help.

Unlike outright hardware or software failures, conflicts arise quite frequently and are entirely predictable. Quite often, technicians see the same conflicts over and over again. Users having similar hardware and software configurations tend to experience the same conflicts, some earlier than the rest. Therefore, the user may not have had to experience the conflict in the first place.

The solution to such configuration problems usually involves manually correcting the computer's configuration by revising (usually updating) portions (such as libraries and hardware drivers) of the computer's operating system. The

remote technician or the user may effect these revisions. Unfortunately, the above-described solutions to the diagnostic problem still require the user to suffer a fault and contact a technician, even if it is an avoidable fault due to a conflict.

In the past, the answer has seemed to lie merely in automating the diagnostic process. For example, U.S. Pat. No. 5,287,505, issued on Feb. 15, 1994, to Calvert, et al., and entitled "On-line Problem Management of Remote Data Processing Systems, Using Local Problem Determination Procedures and a Centralized Database" is directed to automated problem analysis and resolution of a customer data-processing system in which a central service data-processor system communicates with the customer system. Included is a database for converting machine, software and symptom data into instructions, hardware and software module lists, and service call schedules. The customer system detects data concerning its own configuration and problem symptoms for communication to the service system. The service system itself orders repair modules, and electronically communicates software fixes to the customer system.

Unfortunately, Calvert, et al., is expressly directed to repair of a fault once it has occurred and does not provide a means by which to anticipate and avoid faults, particularly configuration faults arising out of hardware/software conflicts.

In the past, some effort has been given to automating the process of software revision to avoid prospective, purely software-based faults. For example, U.S. Pat. No. 5,155,847, issued on Oct. 13, 1992, to Kirouac, et al., and entitled "Method and Apparatus for Updating Software at Remote Locations" is directed to a method and system for updating the software used in remote computer systems from a central computer system. The method includes storing, in the central computer system, copies of the software executable used in each remote computer system. When the copies of the software in the central computer system are upgraded, for example, to correct the software, to add new facilities, to change user interfaces, to make cosmetic changes, to improve performance, etc., each change made to the software is monitored and stored. The remote computer systems are permitted access to the central computer system via communications links and the software in the remote computer systems and the corresponding software in the central computer system are compared. All of the changes that have been made to the software in the central computer system which have not been made to the corresponding software at the remote computer system accessing the central computer are detected. The detected changes are then transmitted to the remote computer system and applied to the software therein in order to upgrade the software in the remote computer system. The upgraded software in the remote computer system is examined to ensure that the software has been changed correctly. The method allows the software at the remote computer systems to be upgraded even while the software at the remote site is being used. The system and method also allow the software used in the remote computer systems to be upgraded when the remote computer systems use different versions of the software and allow the software to be upgraded in a variety of hardware environments and operating systems.

Unfortunately, Kirouac, et al., is directed only at revising application-level software. Kirouac, et al. is not directed to analyzing the complete hardware and software configuration of a computer system in an effort to identify hardware/software conflicts and potential configuration faults. Further, Kirouac, et al., is not directed to revising components of the computer's operating system.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.