PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00	A1	(11) International Publication Number: WO 97/15878
		(43) International Publication Date: 1 May 1997 (01.05.97)

(21) International Application Number: PCT/US96/15343

(22) International Filing Date: 25 September 1996 (25.09.96)

(30) Priority Data:
08/547,211 24 October 1995 (24.10.95) US

(71) Applicant: YBM TECHNOLOGIES, INC. [US/US]; 110 Terry Drive, Newton, PA 18940 (US).

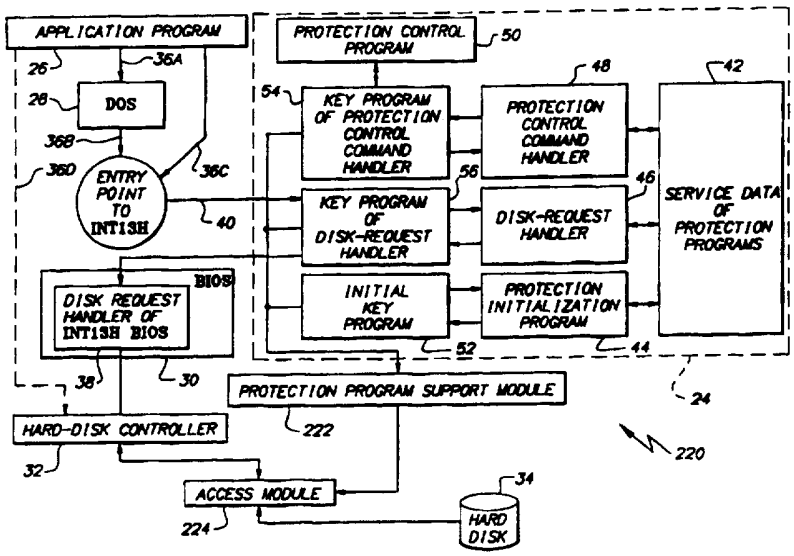
(72) Inventors: FISHERMAN, Igor; Suite 14B, 9945 Norwalk Road, Philadelphia, PA 19115 (US). KOUZNETSOV, Oleg, V.; Apartment 36A, 301 Heights Lane, Feasterville, PA 19053 (US). PAVLISHIN, Sergey, P.; Apartment 29A, 301 Heights Lane, Feasterville, PA 19053 (US). SHATILOV, Alexander, N.; Apartment 12F, 301 Heights Lane, Feasterville, PA 19053 (US).

(74) Agent: SLOMOWITZ, Scott, M.; Caesar, Rivise, Bernstein, Cohen & Pokotilow, Ltd., Seven Penn Center, 12th floor, 1635 Market Street, Philadelphia, PA 19103-2212 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: PERSONAL COMPUTER HARD DISK PROTECTION SYSTEM



(57) Abstract

The personal computer hard disk protection system (220) is designed to protect data stored on computer hard disks (34) of computers utilizing non-ISA buses while permitting multiple user operation. The personal computer hard disk protection system (220) prevents unauthorized access to the hard disk (34) by software applications, and permits safe servicing of requests which use the BIOS. The basis for the personal computer hard disk protection system (220) functions is the dynamic transformation of the file system to the configuration of the current user. The system (220) is based on a hardware device called the protection-program support module (222) and a set of protection programs (24), most of which is stored in the protection-program support module (222). The protection program support module (222) is an external board and is connected to the computer system bus (58, 60, 62), and to the base IDE connection level, the latter of which is controlled by the protection program support module (222) for either permitting or denying access to the hard disk (34).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

PERSONAL COMPUTER HARD DISK PROTECTION SYSTEM

SPECIFICATION

FIELD OF THE INVENTION

The invention pertains to apparatus for protecting data stored on a computer from inadvertent or intentional distortion. In particular, this invention concerns a hard disk protection system that protects data stored on a personal computer system that is accessible to a plurality of users.

BACKGROUND OF THE INVENTION

The most general and progressive approach to shared information processing using personal computers is to join the computers into a local area network (LAN). LAN's facilitate data gathering and allow more efficient use of personal computer memory. However, these networks also provide favorable conditions for the rapid spread of programs known as computer viruses, and thus increase the risk of massive distortion of the information on the personal computer hard disks. LAN's are particularly vulnerable to computer viruses which distort information for the purpose of causing economic loss to the information owners. Because of the enormous losses caused by existing viruses and the continual introduction of new viruses, personal computers have to be equipped with protection subsystems which prevent the deliberate distortion of information. However, despite the wide variety of available file-protection subsystems, computer crime statistics indicate that computer viruses are as dangerous as ever and are still capable of causing enormous losses to personal computer users. Users of personal computers connected in LAN's have a much higher risk than users of isolated computers. Therefore, there is still an urgent need to improve the methods and means of protecting computer files, especially for LAN-linked computers.

An analysis of current methods and means of protecting computer files shows that the most reliable protection is provided by subsystems which use dedicated hardware to support the protection programs. One particularly effective way of protecting computer files is to use specialized processors acting as a connecting link between the central processor and

the file storage device. A typical example of a highly reliable protection subsystem is the computer file protection subsystem developed and patented by Empirical Research System, Inc. (Computer File Protection System: International Publication No. WO 90/13084, C06F 12/14. Application submitted 4/19/89, published 11/1/90). This subsystem can be accessed by the operating system for modifications only during installation. The hardware for this subsystem includes programmable external memory and a programmable external control device. The programmable control device is based on a digital microprocessor and is installed as an intermediate link between the central processor and the file storage device. The programmable control device monitors the control logic signals, the address signals, and the data signals formed by the central processor. An auxiliary memory stores file-access criteria established by the supervisor. The control device checks for file access authorization and prevents access attempts that do not meet the established criteria. The control device also reads the signatures of all the protected files and compares the signatures of the loaded files with the reference signatures. To store the file signatures, the controller creates a protected memory region that is inaccessible to the operating system. In the event of any deviation from the established protection criteria, the protection subsystem prohibits the use of the computer.

An obvious disadvantage of the above-described subsystem is that any user can view the disk directories. This circumstance permits complete viewing of the disk directories, and encourages unsanctioned activity by users wishing to study and distort the data of other users. Another obvious disadvantage of the above-described subsystem is that the hardware serving as the intermediate link between the central processor and the file storage device must be located on a board which connects to the file storage device or on the boards of other devices. As a result, this protection subsystem requires additional hardware and does not provide the most efficient use of the existing hardware.

OBJECTS OF THE INVENTION

Accordingly, it is the general object of this invention to provide apparatus which address the aforementioned needs.

It is another object of this invention to eliminate the need to monitor requests at the operating system level and at the modular device driver level of the personal computer.

It is yet another object of this invention to require less complicated hardware.

It is still yet another object of this invention to provide a personal computer hard disk protection system that can be implemented with personal computers that utilize non-ISA (Industrial Standard Architecture) buses.

It is still yet another object of this invention to provide a personal computer hard disk security system that can intercept all input/output calls at the base IDE (Integrated Drive Electronics) connection level.

SUMMARY OF THE INVENTION

These and other objects of the instant invention are achieved by providing a hard disk protection system for protecting data stored on a hard disk of a personal computer having a non-ISA bus and having a base IDE connection level. Moreover, this personal computer is available to a plurality of users. The hard disk has logical disk structure including an operating system having logical drives. The system comprises protection programs that interpret the logical drives as a fixed set of zones on the hard disk for a particular user and wherein each of the fixed set of zones have respective access rules. The system also includes a hardware module responsive to the protection programs, that either allows or denies access to the hard disk at the base IDE connection level based on the access rules. The hardware module has a first memory that is inaccessible to the central processing unit and a second memory that is accessible to the central processing unit.

DESCRIPTION OF THE DRAWINGS

Other objects and many of the attendant advantages of this invention will be readily appreciated as the same becomes

better understood by reference to the following detailed description when considered in connection with the accompanying drawings wherein the structure and functional organization of the data protection and sharing system are illustrated in the following drawings:

Fig. 1 is a structural block diagram of the hard disk protection system installed in a computer;

Fig. 2 is a structural block diagram of the protection program support module and the access module;

Fig. 3 is a functional block diagram of the program discriminator;

Fig. 4 is a functional block diagram of the programmable controller;

Fig. 5 is an electrical connection interface of the access module, PPSM and the hard disk;

Figs. 6A and 6B together constitute a wiring diagram of the access module;

Fig. 7 is an electrical connection interface of the access module, PPSM and two hard disks;

Fig. 8 is a diagram of a first ribbon cable for use with one access module;

Fig. 9 is a diagram of a second ribbon cable for use with two access modules;

Fig. 10 is an electrical connection interface to a plurality of hard drives using first and second ribbon cables; and

Fig. 11 is an electrical connection interface to a plurality of hard drives using second ribbon cables only.

DESCRIPTION OF THE INVENTION

Referring now in detail to the various figures of the drawing wherein like reference characters refer to like parts, there is shown at 220 in Fig. 1, a personal computer hard disk protection system (HDPS) that comprises a hardware module 222, known as the protection-program support module (PPSM), a access module 224 and protection software 24. At this juncture, it is necessary to point out that the protection software 24 is subject matter of U.S. Application Serial No. 08/336,450,

assigned to the same assignee as this invention and whose disclosure is also incorporated by reference herein. The only difference between the HDPS 220 and the HDPS 20 of U.S. Application Serial No. 08/336,450 is the introduction of the access module 224. Hence, in the interest of brevity, there will be no further discussion of the protection programs 24 other than to relate their operation with the PPSM 222 and the access module 224.

Furthermore, the hardware of the PPSM 222 is based on the PPSM 120B as set forth in U.S. Application Serial No. 08/269,591, also assigned to the same assignee as this invention and whose disclosure is also incorporated by reference herein.

The HDPS 220, by utilizing the access module 224, resolves the problem of hard drive controllers 32 being on a separate bus, different from the buses that the PPSM 222 is coupled to. For example, in some personal computer systems, the hard disk controllers may be located on a PCI (Peripheral Component Interconnect) bus, VESA (Video Electronics Standards Association) bus, a processor's local bus (which does not connect directly to the peripheral bus but rather ties the processor to memory, cache or occasionally to some peripherals that are not on the peripheral bus) or other non-ISA bus. In those situations, the PPSM 22 of U.S. Application Serial No. 08/336,450 and the PPSM 120B of U.S. Application Serial No. 08/269,591, both being located on the ISA bus, cannot intercept hard disk input/output calls from other buses. On the other hand, as will be discussed in detail later, the PPSM 222 via the access module 224 can intercept these non-ISA bus hard disk input/output calls at the base IDE connection level.

Moreover, various manufacturers may implement their own Superset of the ISA standards. Since it is impossible to determine what the effect of such unknown implementations are, the PPSM 22/PPSM 120B, by themselves, may not prevent unauthorized input/output calls to the hard disk 34. On the other hand, the PPSM 222 via the access module 224 can intercept these ISA bus hard disk input/output calls at the base IDE connection level.

As shown in Fig. 1, a conventional personal computer system basically comprises application software 26, an operating system 28 (e.g., DOS or WINDOWS, etc., hereinafter "OS") and a basic input/output system (BIOS) 30. Typically, access to the hard disk controller 32 (and, thereby, the hard disk 34 itself) from the application program 26 is via the entry point 34 to the standard BIOS handler known as INT 13H BIOS, as shown by paths 36A-36C. In some cases, access from the application program 26 to the hard disk controller 32 is direct, as shown by path 36D.

However, with the HDPS 220 coupled to the personal computer system, as will be discussed in detail later, the HDPS 220 prevents direct access to the hard-disk controller 34 by the application program 26 (as indicated by the hatched access path line 36D) and ensures security for disk access using the BIOS disk-request handler 38. In order to verify and ensure the security of disk requests using INT 13H BIOS, the HDPS 220 uses a link 40 with the BIOS input. This link 40 is established by modifying the interrupt vector table to replace the address of the original handler of INT 13H BIOS with the address of the key program of the disk-request handler.

The protection software 24 comprises a set of protection programs which create service data 42 for use in the HDPS 220 processes. These service data 42 of the protection programs are a separate information component. The set of protection programs includes a protection initialization program 44, a disk-request handler 46, a control-command handler 48, a protection control program 50, and a set of key programs, which includes the initial key program 52, the command-handler key program 54, and the request-handler key program 56.

The set of protection programs is stored on the hard disk 34 and in the PPSM 222. In particular, the protection control program 50 is stored as an ordinary file on the hard disk 34. The other protection programs are stored in the PPSM 222.

The PPSM 222 provides hidden storage of the protection programs and establishes a logical relationship between the ability to access the hard disk 34 and the execution phase of

the protection programs. As shown in Fig. 2, the PPSM 222 comprises an external board connected to the peripheral bus (i.e., the address bus 58, data bus 60 and control bus 62 which depict an ISA bus) of the personal computer, and has two operating modes: active and passive. In the active mode, the PPSM 222 activates the access module 224 to deny access to the hard disk 34. In the passive mode, the PPSM 222 does not activate the access module 224, thereby permitting access to the hard disk 34. In order to obtain free access to the hard disk 34, the CPU 64 must switch the PPSM 222 to the passive mode, and to do this, the CPU 64 must use one of the key programs. The reason for the use of the key programs is that the PPSM 222 determines the type of program which is attempting to change the status, and the PPSM 222 allows a change in its status only if flags are present indicating that the key program is active. After the PPSM 222 is switched to the passive mode, the key program transfers control to the protection programs stored in the PPSM 222.

The PPSM 222 comprises a first memory 66, a second memory 68, a programmable controller 70, and a program discriminator 72. The first memory 66 stores the protection programs and can be made inaccessible to the CPU 64. The second memory 68, which is always accessible to the CPU 64, stores the set of key programs which are used to change the status of the PPSM 222. The programmable controller 70 prevents access to the hard disk 34 and forbids access to the first memory 66. The CPU 64 can program the mode of the programmable controller 70 only when a signal is present indicating that one of the key programs is active. The program discriminator 72 determines the type of program acting on the programmable controller 70 and establishes a logical relationship between the ability to switch the PPSM 222 mode and the type of program acting on the programmable controller 70. If flags are present indicating that one of the key programs is active, the program discriminator 72 allows the entry of information into the programmable controller 70. Otherwise, the program discriminator 72 does not permit the

entry of information in the programmable controller 70. The PPSM 222 also includes an address decoder 74 and an AND gate 76.

The module memories 66 and 68 should occupy the address space for the external-device ROM. The programmable controller 70 should be set for the address of the control register of the hard disk controller 32. With regard to hard disk controllers 32 which have an IDE (Integrated Drive Electronics) interface, the programmable controller 32 should be set to the hexadecimal address 177 or 1F7.

The operation of the PPSM 222 will now be discussed.

The program discriminator 72 (Fig. 3) comprises an AND gate 166, a control-port decoder 168, an inverter 170, and two D-type flip-flops 172 and 174. The programmable controller 70 (Fig. 4) comprises a port decoder 176, a mode register 178, and a buffer 180.

The PPSM 222 is reset by the RESET signal (Figs. 3 and 4) from the system reset line. In particular, the RESET signal is transmitted to the input of the inverter 170 (Fig. 3), the output of which is connected to the S-input of the D-type flip-flop 172 of the program discriminator 72; the RESET signal is also transmitted to the R-input of the mode register 178 (Fig. 4) of the programmable controller 70. The RESET signal to the inverter 170 sets the flip-flop 172, which in turn generates a low level logic signal from the inverted output $\overline{Q}$ of the flip-flop 172. This low level logic signal from the inverted output $\overline{Q}$ sets the S-input of the D-type flip-flop 174 which in turn generates a high level logic signal from direct output Q of the flip-flop 174. This high-level logic signal at the direct output Q of the flip-flop 174 of the program discriminator 72 is transmitted through line 154 to the programmable controller 70, thereby permitting installation of data input into the mode register 178 of the programmable controller 70.

As shown in Fig. 4, the system-RESET signal feeds into the R-input of the mode register 178 which resets the register 178, thereby causing the Q0 output of the mode register 178 to send a low-level logic signal to the A1 of the port decoder 176. At the Q1 output (memory access control output 156 of the

programmable controller 70) of the mode register 178 there is also a low-level logic signal, which is sent through line 160 to the second input 158 of the AND gate 76. The low-level logic signal on line 160 enables the second input 158 of the AND gate 76, thereby permitting the transmission of select signals for the first memory 66 as requested by the address decoder 74 via line 140. The output 144 of AND gate 76 is thereby connected to the select input 146 of the first memory 66; i.e., the first memory 66 becomes accessible to the CPU 64.

With the above-described combination of signals at the port-decoder 176 inputs, a high-level logic signal is present at the second output (D1) of the decoder 176 and is sent to the input of the control input 182 of buffer 180. This high-level signal at the control input 182 causes the output 162 of the buffer 180 to convert to a high impedance state which does not affect the command from the hard disk controller 32 to the hard disk 34.

Thus, the initial state of the PPSM 222 is the passive mode, and the first memory 66 is read-accessible. In this regard, it should be noted that the RESET signal causes the CPU 64 to determine the personal-computer configuration and transfer control to programs resident in the external-device ROM. Since the first memory 66 of the PPSM 222 occupies the region of address space reserved for the external-device ROM, the protection programs 24 receive control before the OS 28 is loaded. As a result, the protection programs 24 can switch the PPSM 222 into the required mode before the personal computer is in the ready state. In particular, the protection programs 24 can switch the PPSM 222 into the active mode after the OS 28 is loaded. In addition, the protection programs 24 can prevent access to the first memory 66 and can be hidden from the applications software 22 and the OS 28.

In order to change the mode of the PPSM 222, the CPU 64 must enter the code for the desired mode into the mode register 178 of the programmable controller 70. The protection programs 24 change the mode of the PPSM 222 using a corresponding version of the key program stored in the second

memory 68. During the extraction of key program codes, the second output of the address decoder 74 produces a low-level logic signal, which is sent through line 152 to the select input 148 of the second memory 126. This signal also is transmitted to the control input 150 of the program discriminator 72. The other inputs of the program discriminator 72, which are connected to the system control lines 54, receive signals specifying the type of bus cycle.

In particular, the $\overline{\text{MEMRD}}$ input (Fig. 3) of the AND gate 76 receives pulsed signals which specify the read-memory bus cycles. If the $\overline{\text{REFR}}$ (refresh) input and AEN (address enable) input to the AND gate 76 do not comprise signals used for memory restoration and direct access to memory, then the output of the AND gate 76 will produce pulsed signals which travel to the C-input of the flip-flop 172 and which latch the state of line 152. If there is a low-level logic signal at the D-input (i.e., at control input 150 of program discriminator 72) of the flip-flop 172, then each signal arriving at the C-input of the flip-flop 172 will produce at the inverse output $\overline{Q}$ of the flip-flop 172 a high-level signal which enables the operation of the flip-flop 174. If in that case, an active signal ($\overline{\text{IOW}}$) arrives at the control port decoder 168 from the system output line and if the address at the other inputs of the decoder 168 is the address of the control port, then the output of the control-port decoder 168 will be a pulsed signal indicating key program activity. This signal causes the direct output Q of the flip-flop 174 to have a low-level signal which is sent through line 154 to the first control input (pin V of the mode register 178 (Fig. 4) of the programmable controller 70, and this input acts as the permit mode register 178 setup input.

If an active signal (i.e., a low-level signal is present on line 154) is present at the first control input of the programmable controller 70, the state of the mode register 178 can be changed if another active signal (i.e., low-level signal $\overline{\text{IOW}}$) is present at the port decoder 176 from the system output line and if the other inputs to the decoder 176 have the address which is the address of the control port. If this

combination of signals is present at the permit mode register 178 setup input and at the port decoder 176 inputs, then the first output D0 of the port decoder 176 will produce a pulsed signal which sets the given information code at the outputs of the mode register 178.

If the code preventing access to the first memory 66 is entered into the mode register 178 then the Q1 output (i.e., memory access control output 156) of the mode register 178 will produce a high-level signal, which is sent through line 160 to the second input 158 of the AND gate 76. When that high-level signal is present, the AND gate 76 blocks the transmission of the select signals for the first memory 66 from the address decoder 74, as discussed earlier. As a result, the first memory 66 becomes inaccessible to the CPU 64.

If the active mode code is entered into the mode register 178, then the first output Q0 (Fig. 3) of the mode register 178 produces a "disable hard disk" signal DISHD. The DISHD is the command signal transmitted from the PPSM 222 to the access module 224 for denying access to the hard disk 34 when the PPSM 222 is in an active mode. In particular, the DISHD is sent to a buffer 190 whose output line 192 is connected to PPSM connector 194 and 195. The buffer 190 is always enabled through a control line 196 coupled to ground. Hence, wherever the switching of the PPSM 22 as set forth in A.S.N. 08/336,450 from the passive mode to the active mode occurs, instead of the PPSM 222 transmitting a $\overline{I}/\overline{O}$ $\overline{CH}$ $\overline{RDY}$ signal that prevents the completion of the bus cycle (and, therefore, any further use of the personal computer), the PPSM 222 prevents the selection of a hard drive 34 via the transmission of the DISHD signal to the access module 224. Similarly, wherever the switching of the PPSM 22 as set forth in A.S.N. 08/336,450 from the active mode to the passive mode occurs, instead of the PPSM 222 terminating the $\overline{I}/\overline{O}$ $\overline{CH}$ $\overline{RDY}$ signal, the PPSM 222 permits the selection of a hard drive 34 by terminating the DISHD signal.

In addition, the DISHD signal is sent to the first input A1 of the port decoder 176. The signal causes the port

decoder 176 to verify the bus cycles for CPU 64 access to output devices.

(It should be pointed out at this juncture that the PPSM 222 can be easily modified to operate in accordance with the PPSM of A.S.N. 08/336,450 (i.e., PPSM 22) and 08/269,591 (i.e., PPSM 120B) since the hardware which generates a low-level signal on the system ready line $\overline{I/O}$ $\overline{CH}$ $\overline{RDY}$ on the system bus availability line (and, therefore, prevents the completion of the current bus cycle and any further use of the personal computer) remains on the circuit card of the PPSM 222. However, the output of that hardware is physically disconnected from the system ready line. In particular, as shown in Fig. 4, the output line 164 of the buffer 180 has a coupling 198 for receiving a jumper wire (not shown). Without this jumper wire installed, the PPSM 222 cannot affect the system ready line.)

The interconnection of the access module 224, the hard disk 34, and the PPSM 222 is shown in Fig. 5. In a typical personal computer configuration, the hard disk controller 32 is interfaced directly to the hard disk 34 via a standard IDE cable 300. In particular, the IDE cable 300 has a connector 302 that couples directly to a connector 304 on the hard disk 34 itself.

On the other hand, with the HDPS 220 installed in the PC, the standard IDE cable connector 302 is coupled to a first connector 306 on the access module 224 and the access module 224 is directly plugged into the hard disk connector 304 via a second connector 308 on the access module 224. By this connection, the access module 224 is inserted in series between the hard disk controller 32 and the hard disk 34.

The PPSM 222 is coupled to the access module 224 via a ribbon cable 310 (Figs. 5 and 8). One end of the ribbon cable 310 having a connector 312 is coupled to the PPSM connector 195 while the other end of the cable 310 having a connector 314 is coupled to a third connector 316 (Fig. 6B) on the access module 224.

With the access module 224, the hard disk 34, and the PPSM 222 coupled together as shown in Fig. 5, the access module 224 wiring diagram of Figs. 6A and 6B can now be discussed.

As can be seen in Figs. 6A and 6B, the access module 224 passes all of the signals from the standard IDE cable 300 to the hard disk 34. However, the Select Hard Disk Controller (HDC) Data and Control I/O Ports Signal and the Select HDC Control I/O Port Signal are each diverted through respective buffers 318A and 318B (e.g., 74LS125A Buffer). In particular, the Select Hard Disk Controller (HDC) Data and Control I/O Ports Signal is fed to the buffer 318A as input signal $\overline{SCS0}$, while the Select HDC Control I/O Port Signal is fed to the buffer 318B as input signal $\overline{SCS1}$. The respective buffer output signals are indicated by $\overline{HCS0}$ and $\overline{HCS1}$. The buffers 318A and the 318B are controlled by a single signal on control line 320. With the ribbon cable 310 coupled to the access module 224 via the connectors 314/316, the DISHD/$\overline{DISHD}$ signal is fed to control line 320 from the PPSM 222. Therefore, the state of the DISHD signal controls whether the input select signals $\overline{SCS0}$ and $\overline{SCS1}$ are permitted to pass through the buffers 318A/318B (indicated as $\overline{HCS0}$ and $\overline{HCS1}$, respectively) and thereby select a hard disk 34 or, are denied passage through these buffers, thereby preventing the selection of a hard disk 34.

It should be understood that the access module 224 is not intended to be limited to the use of buffers only; any type of switching mechanism that can be activated/de-activated by the DISHD/$\overline{DISHD}$ signal is intended by the applicants.

Where there are two hard disks (34A and 34B) in the personal computer, the HDPS 220 can protect both hard disks 34A/34B via the use of two ribbon cables 310A and 310B in conjunction with a respective access modules 224A and 224B coupled to hard disks 34A and 34B, respectively. In particular, as shown in Fig. 7, one ribbon cable 310A is connected between the PPSM connector 195 and the access module 224A, while another ribbon cable 310B is coupled between the PPSM connector 194 and a second access module 224B. The second access module 224B is coupled in a similar fashion between the second hard disk 34B and its corresponding standard IDE cable 300B.

Where three hard disks (34A, 34B and 34C having respective access modules 224A, 224B and 224C coupled thereto)

are available in a personal computer, a variation of the ribbon cable 310 is used, as shown in Fig. 9 at 410. In particular, as shown in Fig. 9, the ribbon cable 410 comprises a connector 412 (identical to the connector 312) at one end, a connector 414 (identical to the connector 314) at the other end of the cable 410; in addition, the cable 410 includes a central connector 416 that is identical to the connector 414. This ribbon cable 410 allows a single ribbon cable to couple two access modules 224A and 224B to one PPSM 222, as shown in Fig. 10. The third hard disk 34C is coupled to the PPSM 222 via a ribbon cable 310.

Fig. 11 depicts the connections made when four hard disks (34A, 34B, 34C and 34D having respective access modules 224A, 224B, 224C and 224D coupled thereto) are available and the HDPS 220 is installed. In that situation, two ribbon cables 410 are used to couple pairs of hard drives to the PPSM 222.

Without further elaboration, the foregoing will so fully illustrate our invention that others may, by applying current or future knowledge, readily adopt the same for use under various conditions of service.

CLAIMS

1. A hard disk protection system (220) for protecting data stored on a hard disk (34) of a personal computer having a non-ISA bus and having a base IDE connection level and wherein the personal computer is available to a plurality of users, the hard disk (34) having logical disk structure including an operating system (28) having logical drives, characterised in that said system (220) comprises:

protection programs (24) that interpret the logical drives as a fixed set of zones on the hard disk (34) for a particular user and wherein each of said fixed set of zones have respective access rules, and

a hardware module (222), responsive to said protection programs (24), that either allows or denies access to the hard disk (34) at the base IDE connection level based on said access rules, said hardware module (222) having a first memory (66) that is inaccessible to the central processing unit (64) and a second memory that is accessible to the central processing unit (64).

2. The system of Claim 1 wherein said protection programs (24) comprise:

a protection initialization program (44) which uses an initial key program (52) for transferring control;

a disk request handler program (46) which uses a disk request handler key program (56) for transferring control;

a protection control program (50); and

a protection control command handler (48) which uses a protection control command handler key program (54) for transferring control and for communicating with said protection control program (50).

3. The system (220) of Claim 2 wherein said protection initialization program (44) comprises:

means for verifying a user name and a user password;

means for generating service data (42) for each user for determining said fixed set of zones;

means for allocating disk space on the hard disk (34) for establishing said fixed set of zones for each logical drive; and

means for changing the address of the INT 13H BIOS handler in the interrupt vector table.

4. The system (220) of Claim 3 wherein said service data (42) comprises a first set of data and a second set of data, said first set of data being stored in one of said fixed set of zones on the hard disk (34) and said second set of data being stored in said first memory (66).

5. The system (220) of Claim 4 wherein said first set of data comprises a list of directory and file descriptors, a map of access rights, a disk space partitioning table, a cluster affiliation table, a main file allocation table and a list of disk control and address parameters.

6. The system (220) of Claim 5 wherein said second set of data comprises a list of user names and passwords.

7. The system (220) of Claim 5 wherein a first one of said fixed zones occupies the disk space from the sector containing the description of the logical drive partition to the loading sector of the disk, inclusive, said first zone being monitored and controlled by said disk request handler program for permitting access for reading only of information on the hard disk.

8. The system (220) of Claim 5 wherein a second one of said fixed zones occupies the disk space from the first sector of the first copy of the logical-drive file allocation table to the first sector of the root directory of the disk, said second zone being monitored and controlled by said disk request handler program (46) for permitting access for reading of, and for making permitted changes to, information on the hard disk (34).

9. The system (220) of Claim 5 wherein a third one of said fixed zones occupies the disk space from the first to the last sector of the disk root directory, inclusive, said third zone being monitored and controlled by said disk request handler program (46) for permitting access for reading of, and for making permitted changes to, information on the hard disk (34).

10. The system (220) of Claim 5 wherein a fourth one of said fixed zones occupies the disk space at the end of the logical drive, said zone having a beginning location, said fourth zone being monitored and controlled by said disk request handler program (46) for permitting access for reading of, and for making permitted changes to, information on the hard disk (34).

11. The system (220) of Claim 5 wherein a fifth one of said fixed set of zones comprises a size that occupies the disk space from the first sector of the first cluster of the disk to the beginning location of said zone that occupies the disk space at the end of the logical drive, said fifth zone being monitored and controlled by said disk request handler program (46) for prohibiting any access for reading or writing, said size being determined by said list of directory and file descriptors, said access map, said cluster table and said main file allocation table.

12. The system (220) of Claim 2 wherein each of said key programs (52, 54, 56) can switch said hardware (222) module into either a passive mode or an active mode, said passive mode permitting said protection programs (24) to be read without affecting access to the hard disk (34) by the central processing unit (64), said active mode hiding said protection programs from the central processing unit and denying access to the hard disk (34), each of said key programs (52, 54, 56) being stored in said second memory (68) and having a corresponding memory address.

13. The system (220) of Claim 2 wherein said initial key program (52) receives control from the BIOS ROM Scan procedure.

14. The system (220) of Claim 5 wherein said disk request handler program (46) uses said disk space partitioning table to interpret any hard disk request involving reading or altering of information on the hard disk (34) in one of said fixed set of zones.

15. The system (220) of Claim 14 wherein said disk request handler program (46) utilizes said map of access rights and said cluster affiliation table for responding to the hard disk request for a particular one of said fixed set of zones.

16. The system (220) of Claim 3 wherein said means for changing the address of the INT 13H BIOS handler in the interrupt vector table replaces the address of the original handler of INT 13H BIOS in the interrupt vector table with said corresponding address of said disk request handler key program (56) before the operating system (28) is loaded.

17. The system (220) of Claim 2 wherein said protection control command handler key program (54) transfers control from said protection control program (50) to said protection command request handler program (48).

18. The system (220) of Claim 5 wherein said protection control command handler program (48) comprises:

means for monitoring the access privilege of a calling program;

means for registering new users;

means for deleting a user from said system;

means for changing the status of a file;

means for changing the file attribute;

means for changing a user password; and

means for changing a user name.

19. The system (220) of Claim 18 wherein said protection control program (50) is the only program that can access said control-command handler program (48) and thereby provide an interface between the user and said system (220) in the execution of said means for registering new users, said means for deleting a user from said system, said means for changing the status of a file, said means for changing the file

attribute, said means for changing a user password or said means for changing a user name.

20. The system (220) of Claim 2 wherein said protection control program (50) is stored on the hard disk (34) as an ordinary file.

21. The system (220) of Claim 2 wherein said protection initialization program (44), said disk request handler program (46) and said protection control command handler program (48) are stored in said first memory (66).

22. The system (220) of Claim 11 wherein said first set of data is stored in said fifth zone.

23. The system (220) of Claim 22 wherein said means for allocating disk space allocates disk space in said fifth zone, said allocation means creating a region of disk space at the end of each logical drive, said allocation means transferring any user files or user directories in said region to clusters which are accessible to the user.

24. The system (220) of Claim 3 wherein said protection initialization program (44) further comprises means for converting the values of the deStartCluster fields from real cluster values to virtual cluster values in constructing said file allocation table and thereby forming a virtual continuous disk space, said virtual continuous disk space being formed by eliminating clusters that do not belong to the current user.

25. The system (220) of Claim 22 wherein said protection initialization program (44) further comprises means for transferring said map of access rights and said disk space partitioning table to said first memory (66) from said fifth zone whenever the previous user is identical to the current user.

26. The system (220) of Claim 22 wherein said protection initialization program (44) further comprises means for converting the values of deStartCluster fields from virtual cluster numbers to real cluster numbers whenever the current user is different from the previous user.

27. The system (220) of Claim 5 wherein said access map is constructed based on the deAttributes of the files of the directories belonging to the current user, and wherein:

the clusters belonging to files with ATTR_READONLY=0 and unoccupied clusters receive an access right of ACCESS_FIELD= (1,1);

the clusters belonging to files with ATTR_READONLY =1 receive an access right of ACCESS_FIELD=(1,0);

the clusters belonging to directories receive an access right of ACCESS_FIELD=(0,1); and

the clusters which are not accessible to the current user receive an access right of ACCESS_FIELD=(0,0).

28. The system (220) of Claim 27 wherein said main file allocation table, said disk space partitioning table and said cluster affiliation table are constructed based on said access map.

29. The system (220) of Claim 15 wherein said disk request handler program (46) further comprises means for converting said virtual cluster number into a real cluster number for determining the sector address pertaining to the request.

30. The system (220) of Claim 1 wherein said hardware module (222) includes an access module (224) that is coupled to the hard disk (34) at the IDE connection level for permitting or denying access to the hard disk (34) when commanded by said hardware module (222).

31. The system (220) of Claim 30 wherein the base IDE connection level includes a Select Hard Disk Controller (HDC) Data and Control I/O Ports Signal and a Select HDC Control I/O Port Signal, said access module (224) controlling the passage of the Select Hard Disk Controller (HDC) Data and Control I/O Ports Signal and the Select HDC Control I/O Port Signal.

32. The system (220) of Claim 31 wherein said access module (224) is coupled to said hardware module (222) through a first cable (310) having a first end and a second end, said first cable (310) having a first connector (312) at said first end coupled to said hardware module (222) and having a second

connector (314) at said second end coupled to said access module (224).

33. The system (220) of Claim 30 wherein the personal computer comprises a plurality of hard disks (34A, 34B, 34C) and wherein the hardware module (222) comprises a plurality of access modules (224A, 224B, 224C), said plurality of access modules (224A, 224B, 224C) being coupled to a respective one of the plurality of hard disks (34A, 34B, 34C).

34. The system (220) of Claim 33 wherein a first (224A) and a second access module (224B) are coupled to said hardware module (222) through a second cable (410) having a first end, a second end and a middle portion, said second cable (410) having a first connector (412) at said first end coupled to said hardware module (222), said second cable (410) having a second connector at said second end coupled to said second access module (224B), and said second cable (410) having a third connector (416) disposed at said middle portion coupled to said first access module (224A).

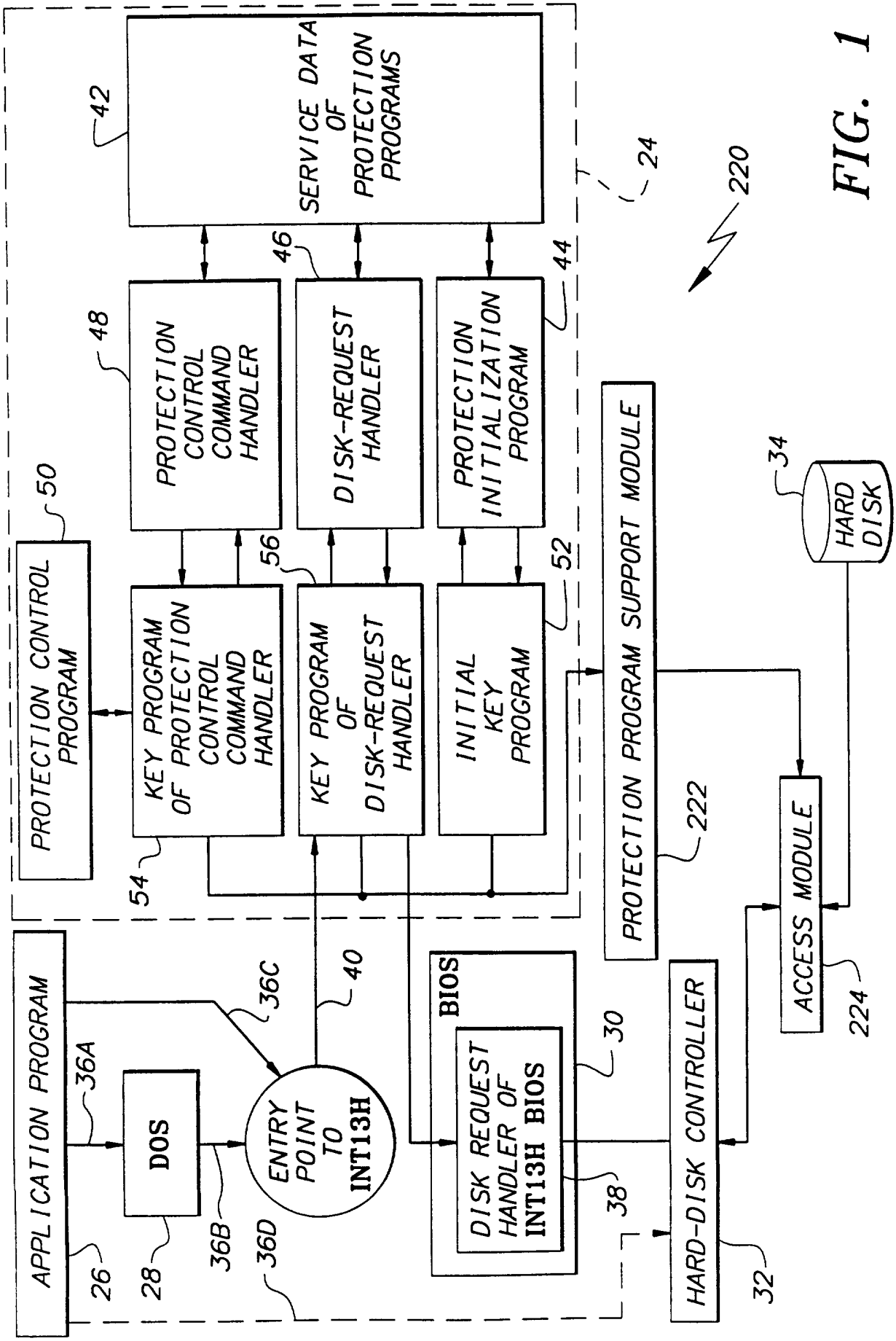

SERVICE DATA OF PROTECTION PROGRAMS
42
24
220
PROTECTION CONTROL COMMAND HANDLER
48
DISK-REQUEST HANDLER
46
PROTECTION INITIALIZATION PROGRAM
44
PROTECTION CONTROL PROGRAM
50
KEY PROGRAM OF PROTECTION CONTROL COMMAND HANDLER
56
KEY PROGRAM OF DISK-REQUEST HANDLER
INITIAL KEY PROGRAM
52
54
HARD DISK
34
PROTECTION PROGRAM SUPPORT MODULE
222
ACCESS MODULE
224
APPLICATION PROGRAM
26
36A
DOS
28
36B
36C
ENTRY POINT TO INT13H
40
36D
BIOS
DISK REQUEST HANDLER OF INT13H BIOS
30
38
HARD-DISK CONTROLLER
32

FIG. 1

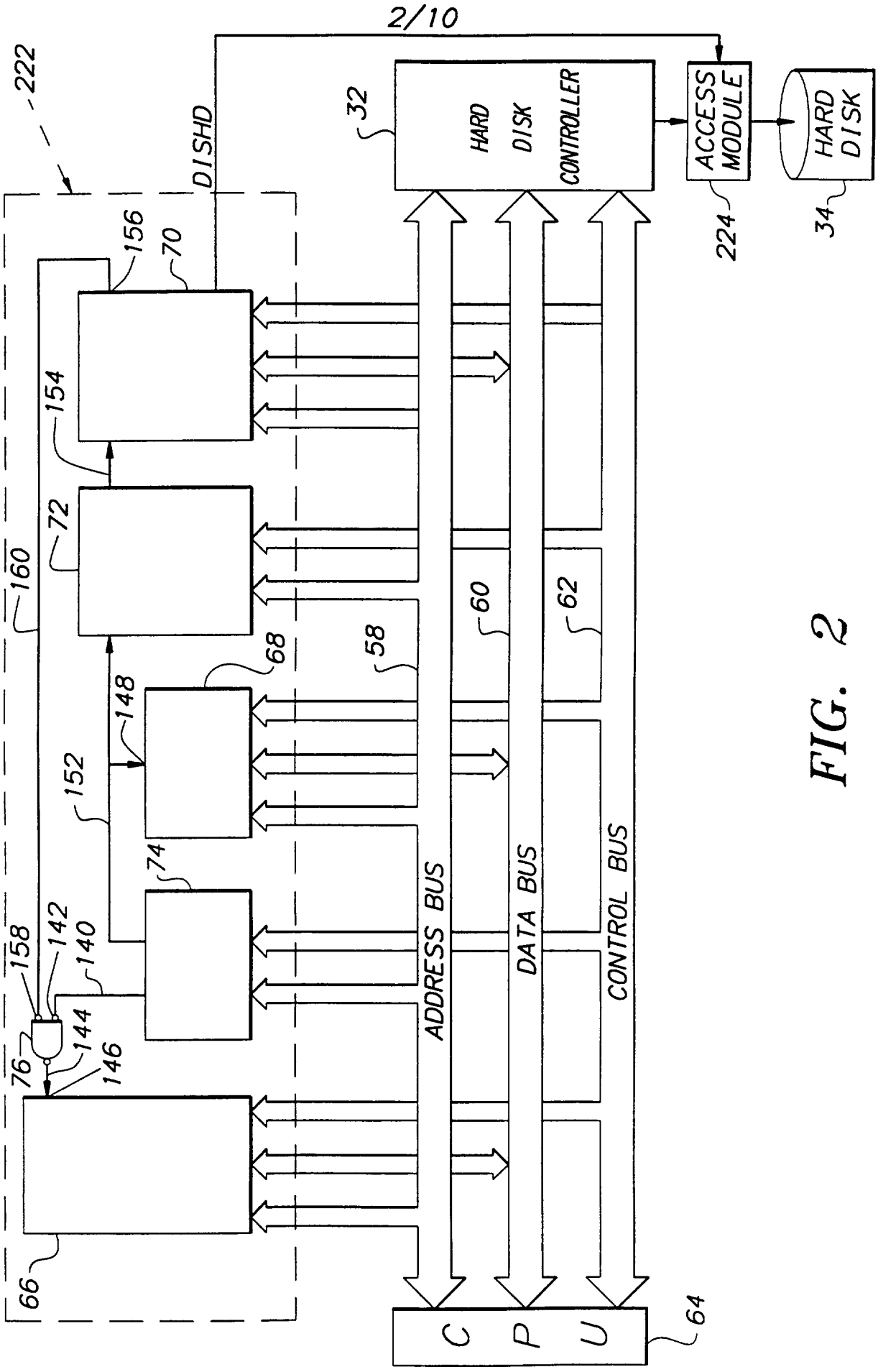

2/10
222
DISHD
32
HARD DISK CONTROLLER
ACCESS MODULE
HARD DISK
224
34
156
70
154
72
160
68
58
60
62
148
152
74
158
142
140
144
146
76
66
ADDRESS BUS
DATA BUS
CONTROL BUS
C P U
64

FIG. 2

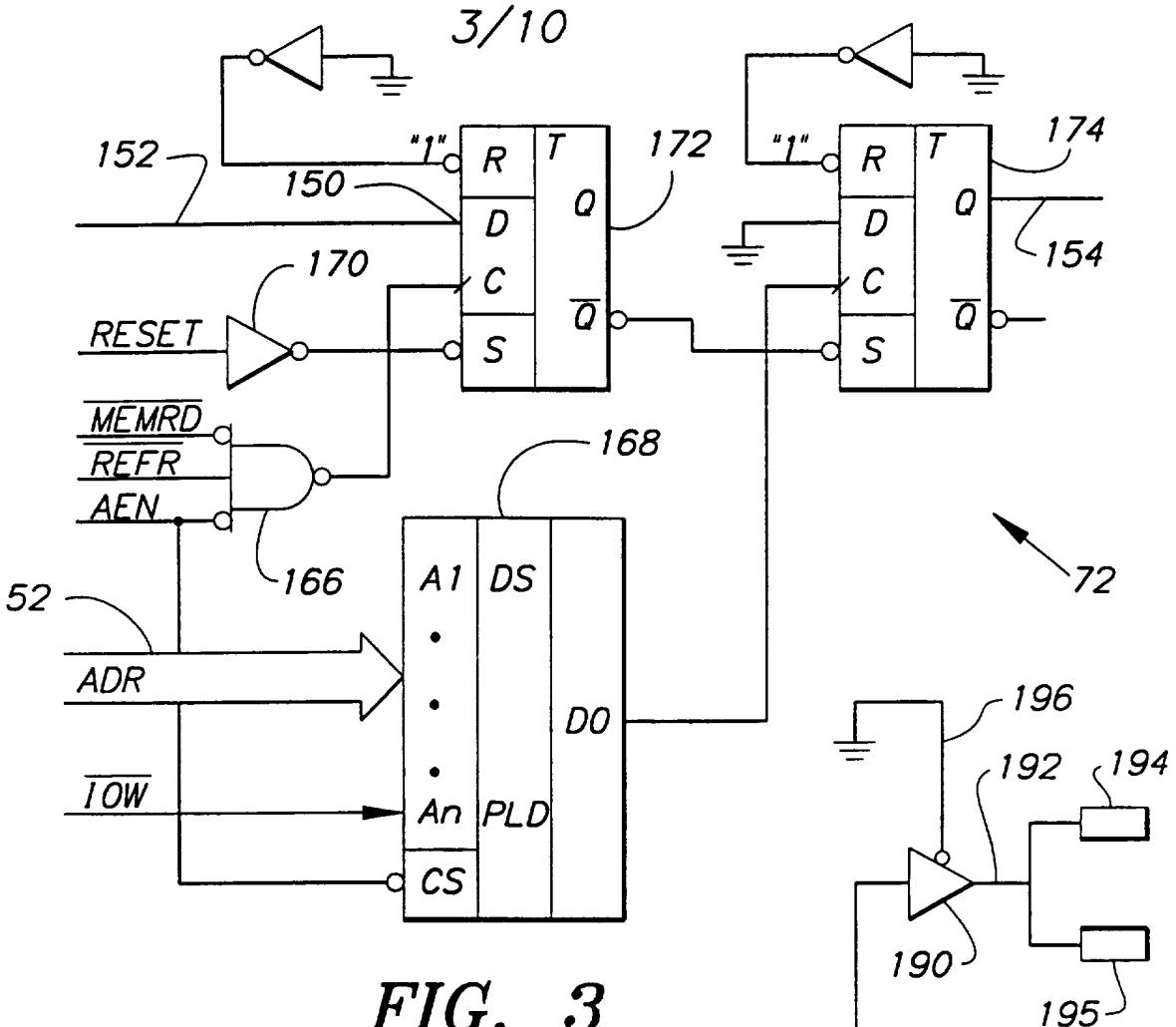

152
150
"1"
R
T
172
D
Q
C
S
Q
"1"
R
T
174
D
Q
C
S
Q
154
170
RESET
MEMRD
REFR
AEN
166
168
72
52
ADR
A1
DS
DO
IOW
An
PLD
CS
196
192
194
190
195

FIG. 3

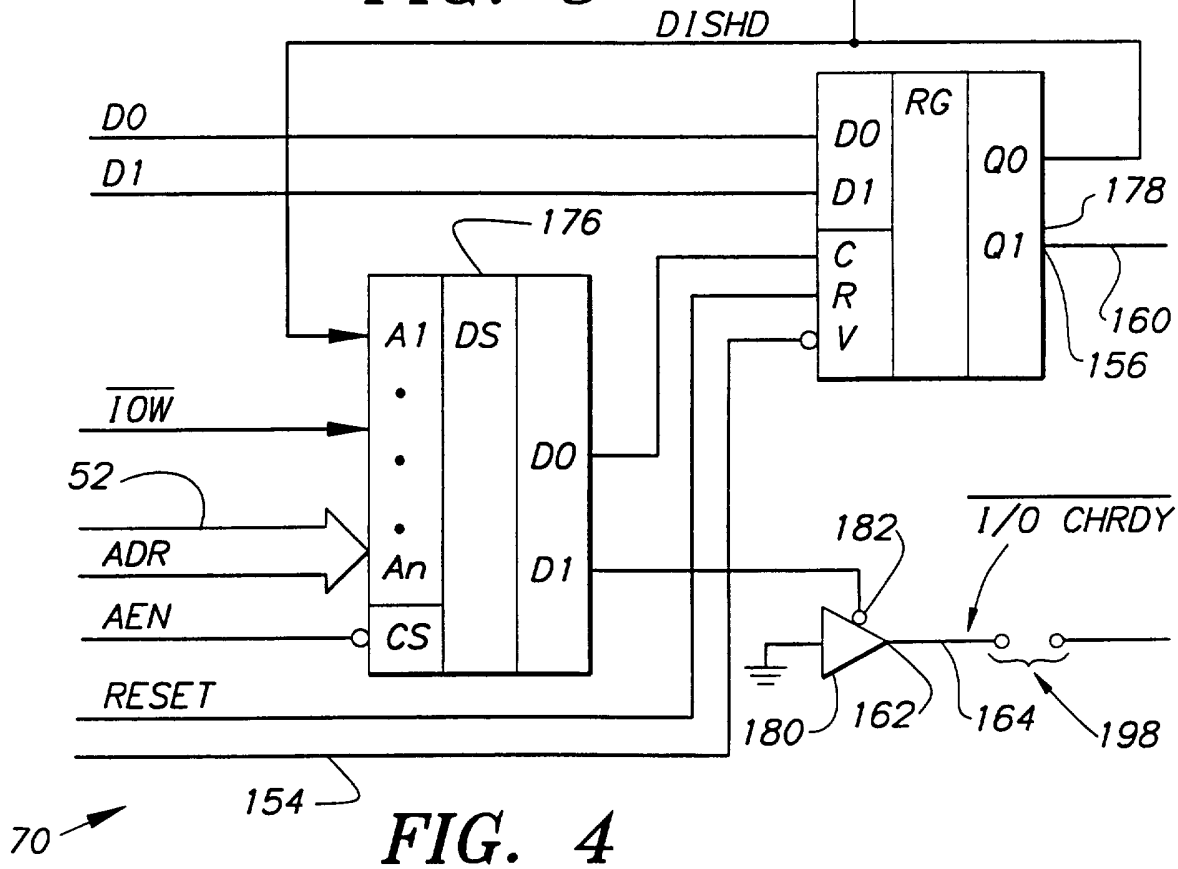

DISHD
DO
D1
DO
D1
RG
QO
Q1
178
C
R
V
160
156
176
A1
DS
IOW
DO
52
ADR
An
D1
AEN
CS
RESET
182
I/O CHRDY
180
162
164
198
154
70

FIG. 4

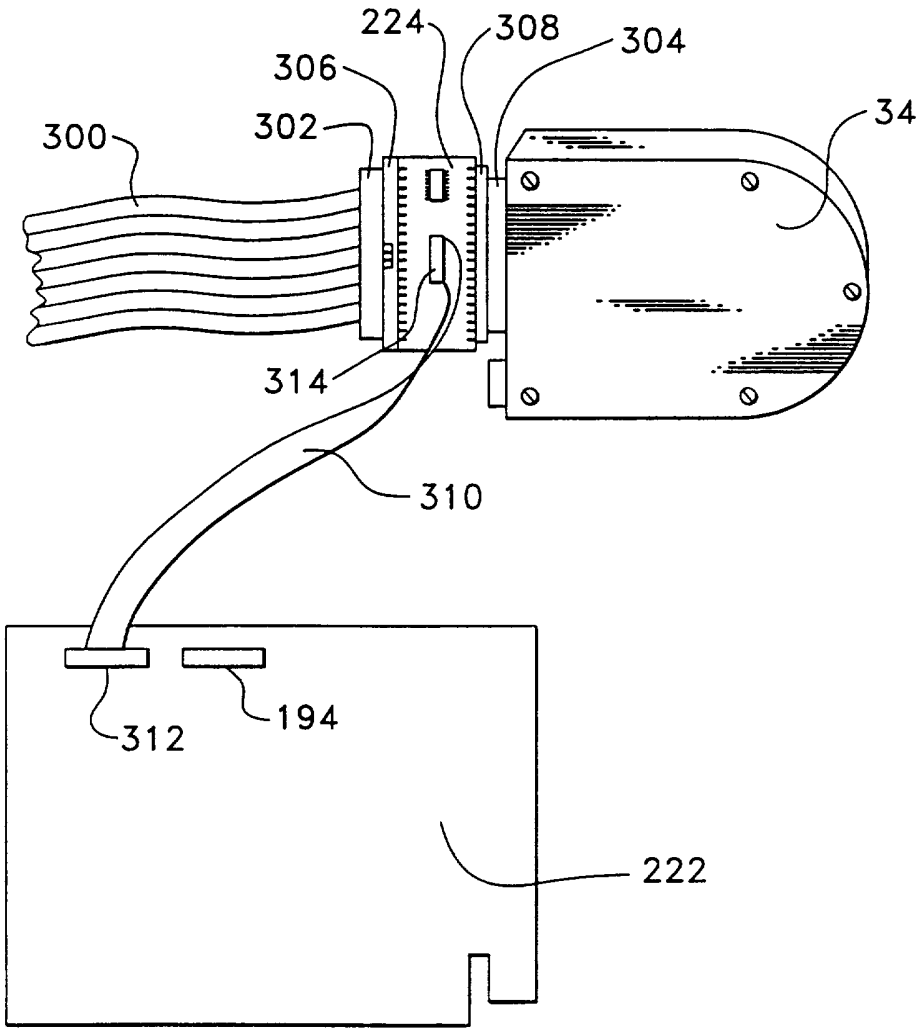


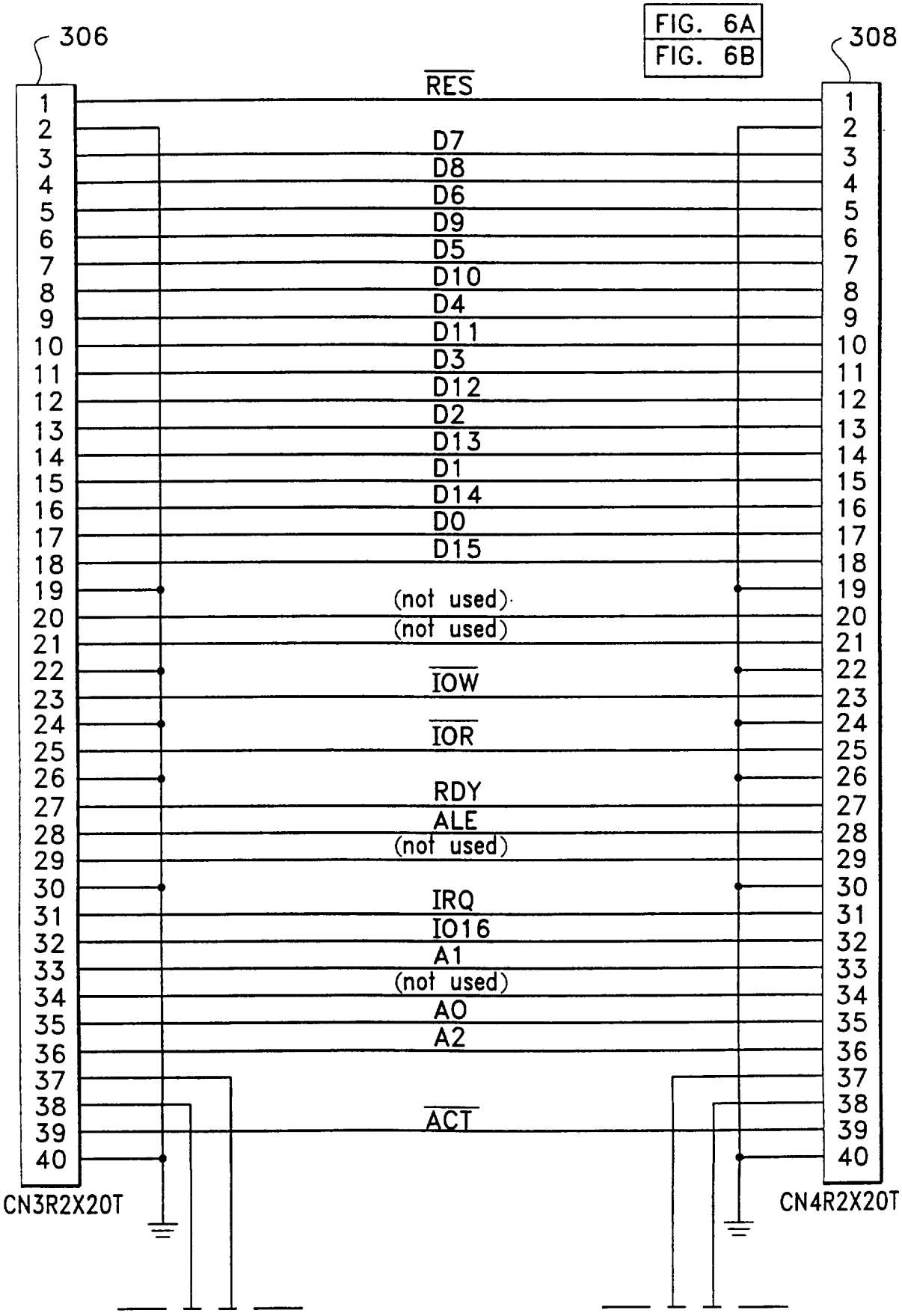
FIG. 5

5/10

FIG. 6A

FIG. 6

FIG. 6A
FIG. 6B



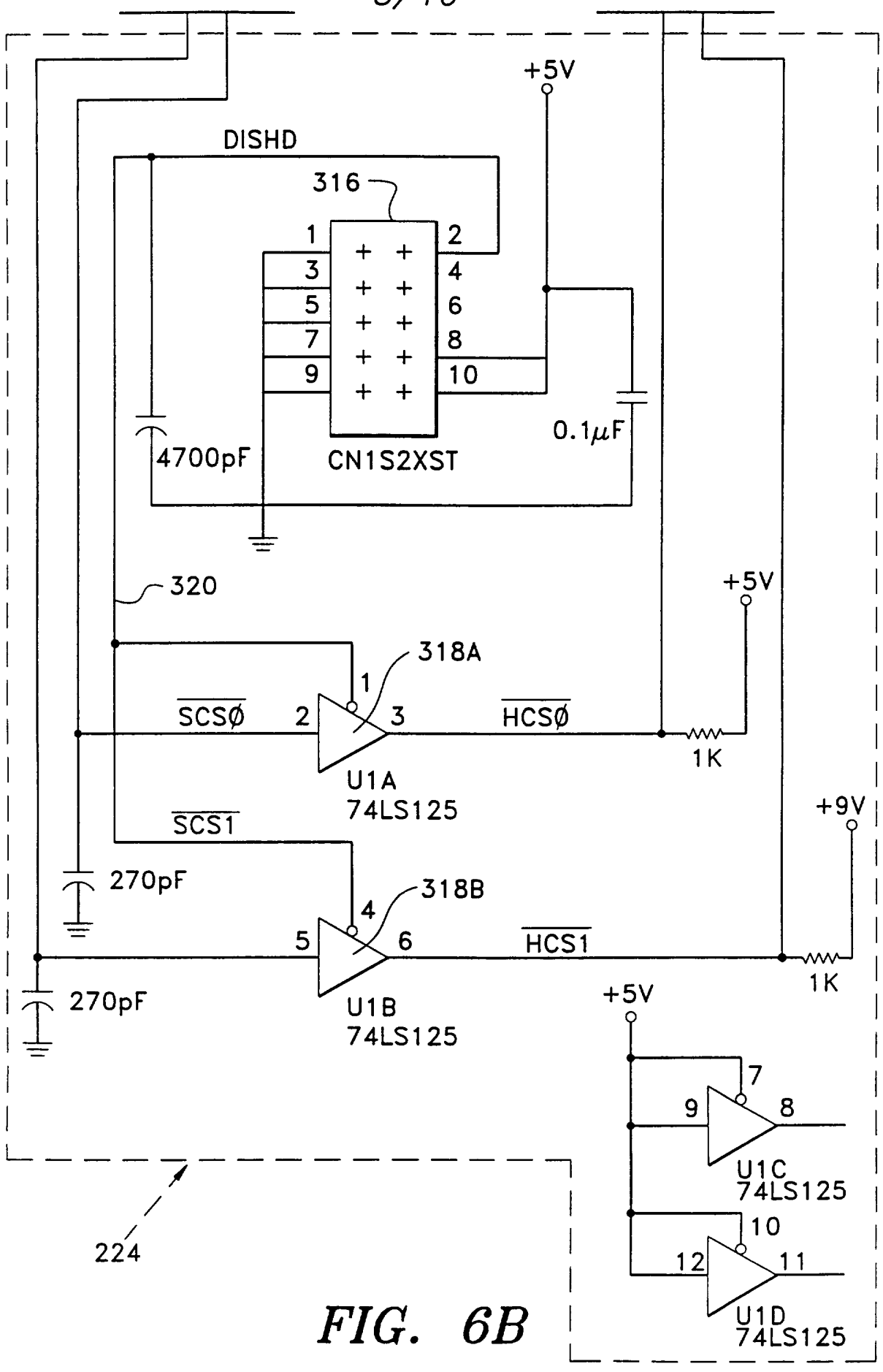

+5V
DISHD
316
1
2
3
4
5
6
7
8
9
10
4700pF
CN1S2XST
0.1μF
320
+5V
318A
SCSØ
2
1
3
HCSØ
1K
U1A
74LS125
SCS1
+9V
270pF
318B
4
5
6
HCS1
1K
270pF
U1B
74LS125
+5V
7
9
8
U1C
74LS125
10
12
11
U1D
74LS125
224

FIG. 6B

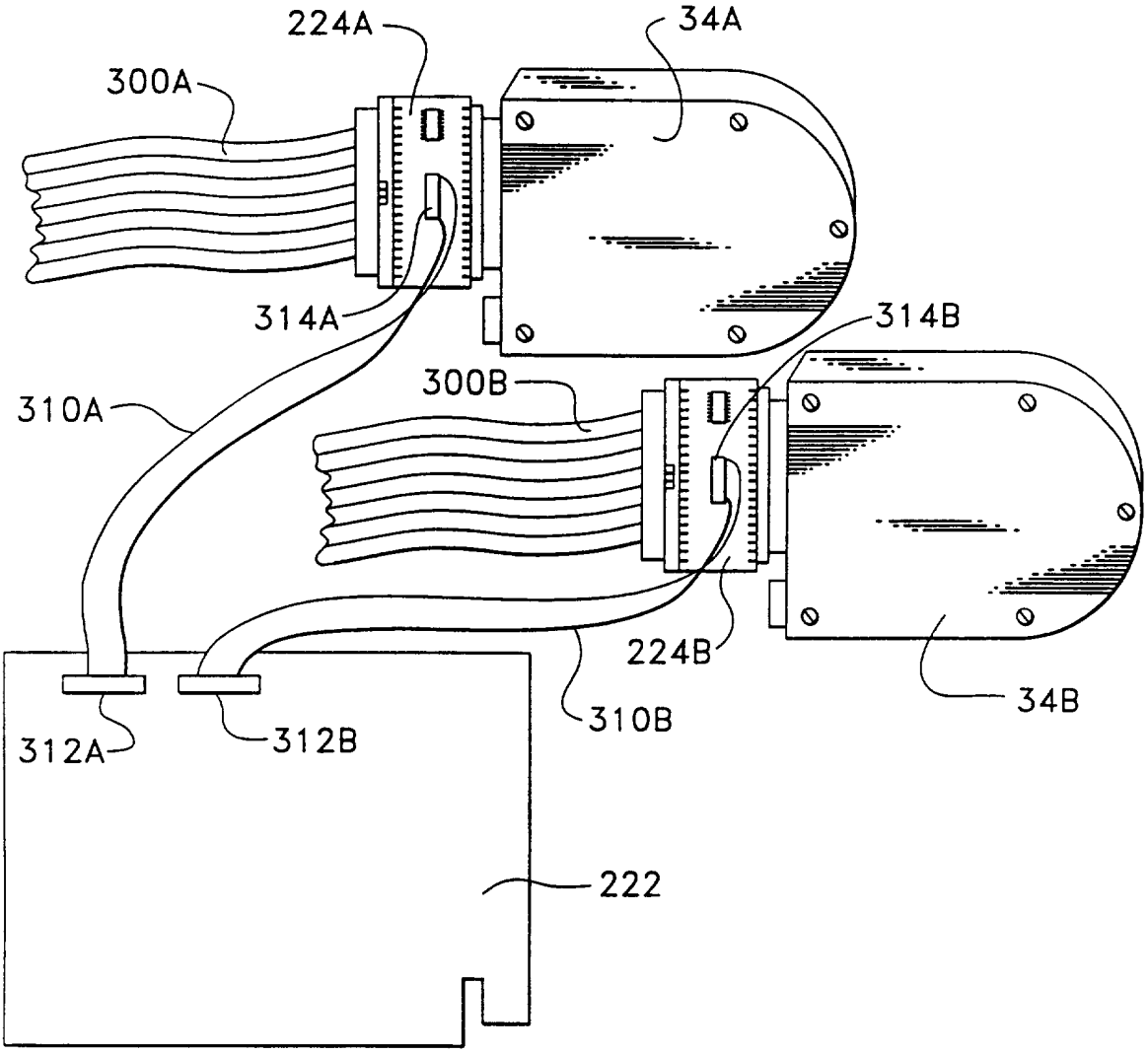


FIG. 7

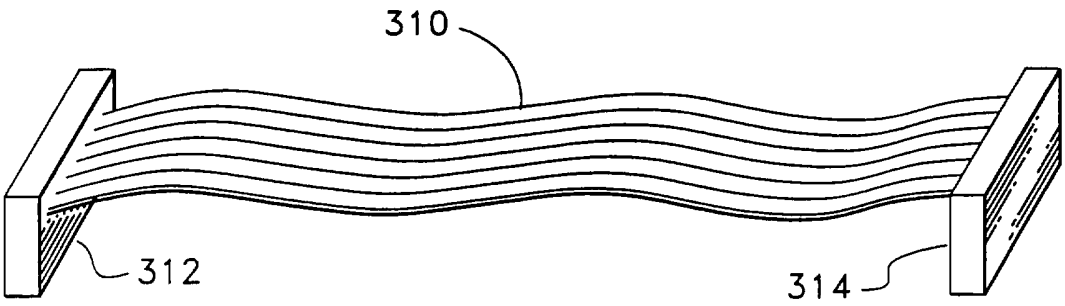


FIG. 8

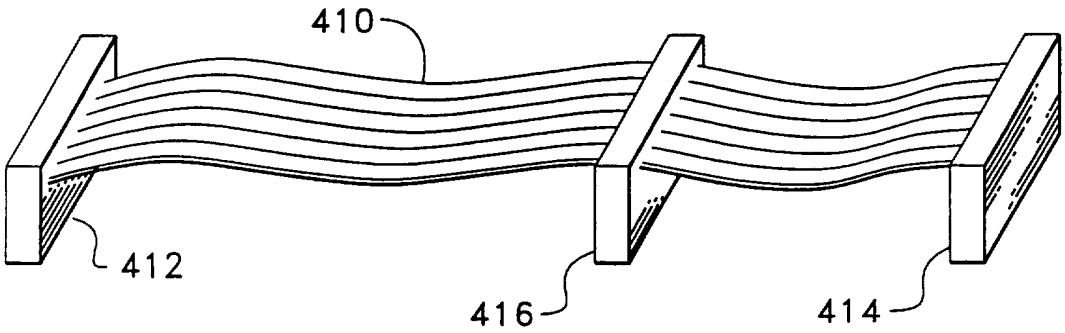


FIG. 9

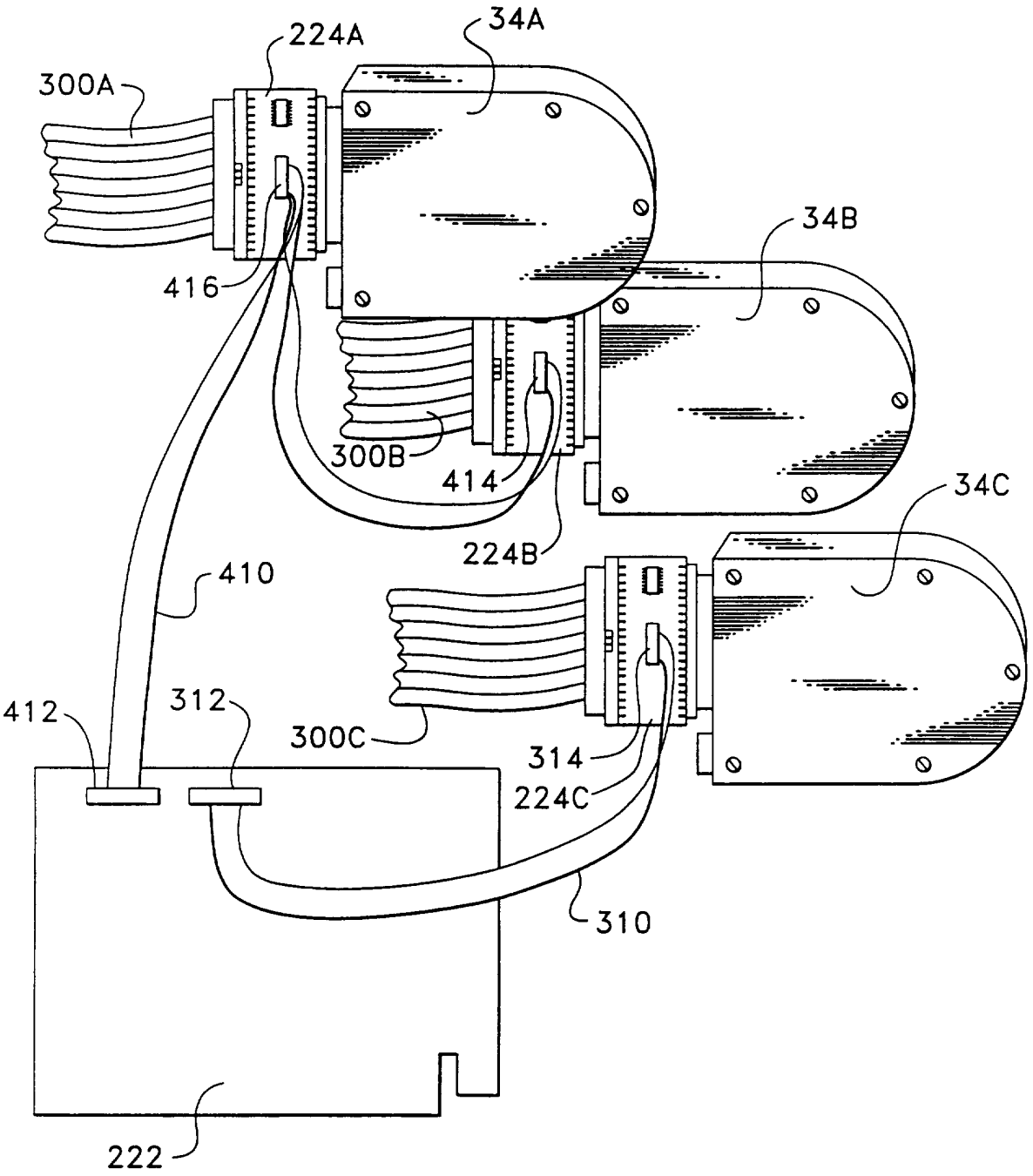

224A
34A
300A
34B
416
300B
414
224B
34C
410
412
312
300C
314
224C
310
222

FIG. 10

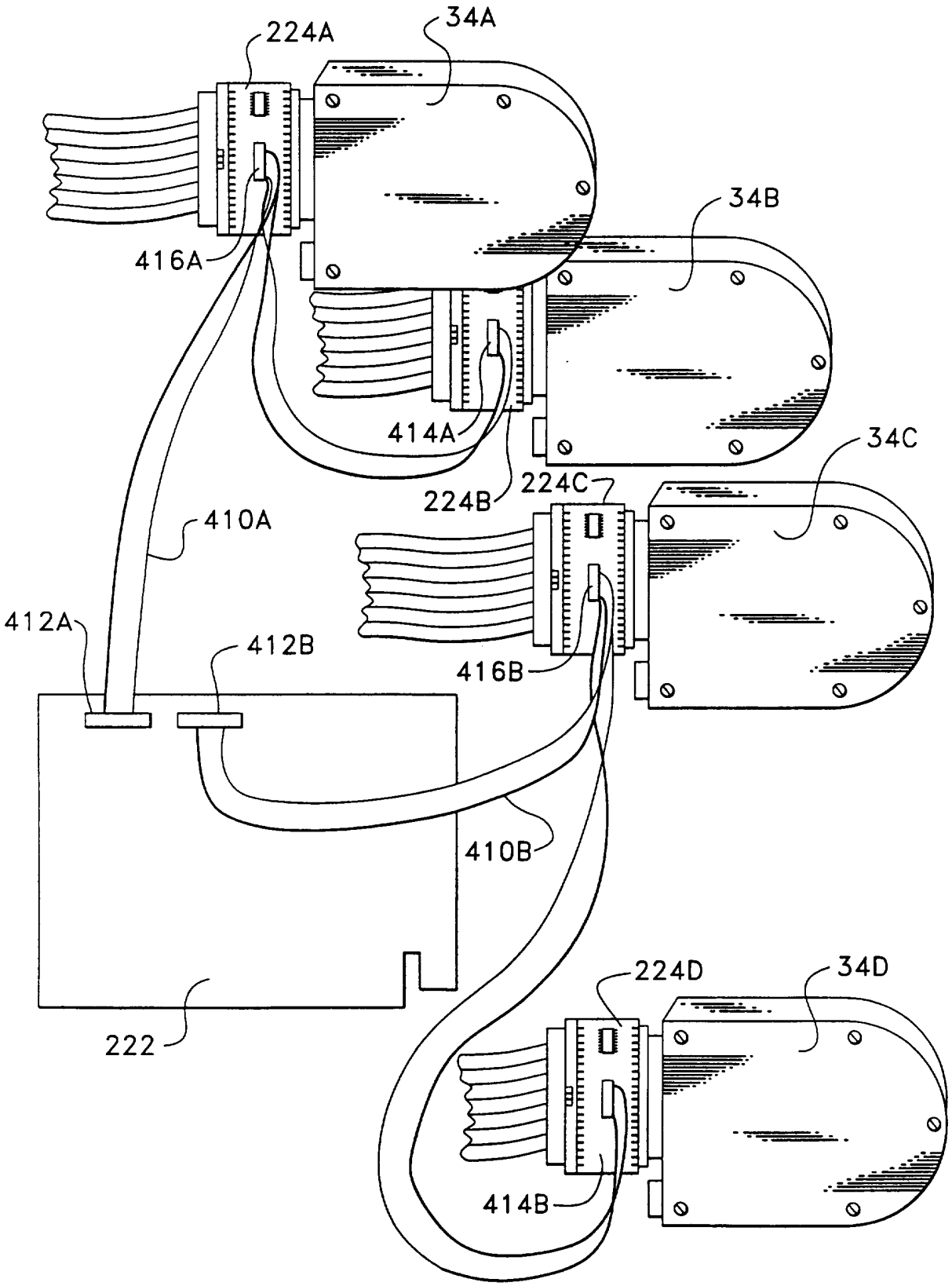

224A
34A
34B
416A
414A
224B
224C
34C
410A
412A
412B
416B
410B
222
224D
34D
414B

FIG. 11

INTERNATIONAL SEARCH REPORT

In tional Application No
PCT/US 96/15343

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

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)
IPC 6 G06F

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 practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	WO,A,96 15486 (YBM TECHNOLOGIES INC) 23 May 1996 see the whole document	1-29
X	WO,A,90 13084 (EMPIRICAL RESEARCH SYSTEMS INC) 1 November 1990 cited in the application see abstract see page 4, line 28 - page 6, line 2 see page 9, line 24 - page 10, line 4 see page 13, line 16 - line 39	1,20
Y		2-6,12, 14, 17-19, 21,30,31

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"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)

"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

"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

"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

"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.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 December 1996	10.01.97

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Moens, R

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 96/15343

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US,A,4 757 533 (ALLEN MICHAEL J ET AL) 12 July 1988 see the whole document	1
Y		2-6,14, 17-19,21

Y	GB,A,2 222 899 (ROSE ANTHONY MORRIS) 21 March 1990	12,30,31
A	see page 4, line 3 - page 5, line 7 see page 7, line 21 - page 11, line 7; figures 1-3	1,32-34

A	WO,A,90 12464 (LANG GERALD S) 18 October 1990 see the whole document	3,20

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

In tional Application No
PCT/US 96/15343

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO-A-9615486	23-05-96	AU-A-	4129796	06-06-96
WO-A-9013084	01-11-90	US-A-	5144659	01-09-92
		AU-A-	5448390	16-11-90
		CA-A-	2014868	19-10-90
		EP-A-	0422184	17-04-91
		US-A-	5289540	22-02-94
US-A-4757533	12-07-88	NONE		
GB-A-2222899	21-03-90	AU-A-	4099589	08-03-90
		US-A-	5144660	01-09-92
WO-A-9012464	18-10-90	CA-A-	1329657	17-05-94
		EP-A-	0465571	15-01-92
		US-A-	5065429	12-11-91
		US-A-	5191611	02-03-93