



Europäisches Patentamt
European Patent Office
Office européen des brevets

Publication number:

**0 104 767
B1**

12

EUROPEAN PATENT SPECIFICATION

45 Date of publication of patent specification: 21.03.90

51 Int. Cl.⁵: G 07 C 9/00, G 07 C 1/14

21 Application number: 83304917.4

72 Date of filing: 25.08.83

54 Card reader for security system.

30 Priority: 27.08.82 US 412385

43 Date of publication of application:
04.04.84 Bulletin 84/14

45 Publication of the grant of the patent:
21.03.90 Bulletin 90/12

14 Designated Contracting States:
BE DE FR GB IT

56 References cited:
EP-A-0 016 276
US-A-3 838 395
US-A-4 148 012
US-A-4 216 375

TN NACHRICHTEN TELEFONBAU UND
NORMALZEIT, vol. 84, 1982, pages 47-56,
Dreieich, DE; W.D. HAASS et al.: "Zeiterfassung
und Zutrittskontrolle mit dem TN-Datensystem
Tenodat 9020"

73 Proprietor: FIGGIE INTERNATIONAL INC.
(Delaware Corporation)
1000 Virginia Center Parkway
Richmond Virginia 23260 (US)

72 Inventor: Khandwala, Bhupendra J.
595 South College Avenue
Claremont California 91711 (US)
Inventor: Young, Jorge A.
2134 Capuchin Way
Claremont California 91711 (US)
Inventor: Kalustian, Sarkis V.
6313 Elmer Avenue
North Hollywood California 91606 (US)

74 Representative: Rushton, Ronald et al
SOMMERVILLE & RUSHTON 11 Holywell Hill
St. Albans Hertfordshire AL1 1EZ (GB)

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European patent convention).

Courier Press, Leamington Spa, England.

EP 0 104 767 B1

Description

Background of the Invention

This application relates to the field of door access security systems and, particularly, to the field of card readers for door access security systems.

Door access security systems, utilizing magnetic card readers at doors to be controlled, are known in the prior art. Such systems include central controllers coupled to a plurality of readers, each of which is located at a specific door to be controlled. Authorized persons wishing to gain access through a door, insert magnetic cards into slots in the reader. Magnetic codings on the cards are then read and data is sent to the controller which authorizes or refuses entry and tells the reader either to keep the door locked or unlock the door.

Such a system can advantageously be used as a time clock to keep a record of the hours worked by hourly employees. However, a problem with system throughput arises when a large number of employees all try to clock in or out at the same time. The delays caused by reading of a card, waiting for a poll signal to come to the reader from the controller, sending the card data to the controller and waiting for the controller to process the information and send back a "Go" or "No Go" signal can create impatience in the workers at the end of the line.

Such card reader systems can also be used to monitor alarm contacts located at strategic locations throughout a facility. In the prior art, a centrally located alarm contact monitoring device was located near the controller with individual wires coupling the contact monitoring device to the alarm contacts located throughout the plant. Such systems were effective but required an individual polling protocol and the associated hardware for the alarm contact monitoring device. Further, individual wires had to be strong between all the contacts to be monitored and the central monitoring device. This could result in large expenditures for wire. Further, such central contact monitoring devices were generally not well suited to applications where only a single alarm contact needed to be monitored since the function rarely justified the expense.

The prior art systems also had room for improvement in the area of operation during times when the communication lines between the reader and the central controller were down. In such a situation, if all access was denied, people would be inconvenienced or, worse, trapped in an undesirable emergency situation. The alternative would be to allow free access through all doors. However, with record-keeping functions done at the central controller, there would be no record of the individuals who entered and left specific areas during specific times while the lines were down. As a result, if theft occurred during the down time, there would be no record to use in the investigation.

One solution to the problems hereabove men-

tioned has been provided by a data recording and access control system as disclosed in T. N. Nachrichten, 1982, No. 84, pp. 47—56, "Telefonbau und Normalzeit." This system gathers and processes data read from a card by an access terminal in a data processing unit. The access terminal can function in a stand-alone operation in the event of failure of transmission line or of the central station. The terminal can perform at three different levels: it can check data input such as the project; specific installation number of the I.D.; and the format of the secret number.

In the expanded stand-alone operation, the access terminal stores the I.D. numbers of all persons who have authorised access at the specific gate. In addition, there may be other individual check parameters, e.g., the secret number. In normal operation, the check data are sent from the central station to the terminal.

In the third performance stage of stand-alone operation, the terminal stores the data of input events as well as of other important events and sends them to the central station after completion of the stand alone operation.

However, it is not indicated how and when the data read from a card during a reading transaction in a stand-alone mode are sent to the central controller, thereby leaving unresolved the problem of system throughput during rush hours. Nor does this disclosure describe how and when loss of communication between the central controller and the terminal is detected by the terminal.

Among prior apparatuses for attempting to improve the technique, there is an apparatus for time clock recording disclosed in EP—A—16276. This disclosure is mostly concerned with time clock recording and computation that, through a novel clock track and separate clock track and data channel optical reading, in cooperation with microprocessor calculation, storage and control, enables automating employee time and attendance and similar data in a format directly recordable on the card and also directly usable by payroll or other processing computers. This apparatus, however, does not resolve the problem of a failure to communicate between a terminal and the central controller.

Summary of the disclosure

There is disclosed herein a card reader for use in a security system for controlling access through key doors, said security system having a central controller. The card reader-reads magnetic data stored on cards held by employees, etc. The cards have a system code and an I.D. code on them. The card readers can do time and attendance functions to serve as a time clock by reading data stored permanently on the card and sending it to the central controller for processing. The central controller then grants or denies access based on the card data. Optionally the improved card reader can also make the decision whether to grant or deny access locally without dialogue with the controller by reading some of the data on the

card and storing the rest for later transmission to the central controller. Typically, this is done by reading the system code and granting authorization if the system code on the card matches the system code on user programmable switches. The I.D. code is then stored in the buffer with the time of day of the transaction for later transmission to the central controller. This feature increases the throughput of the system by eliminating the need for each employee to wait for authorization from a controller which may be delayed while processing other messages from other readers.

The improved card reader can also sense when communications with the central controller are lost and grant or deny access without consulting the controller, based upon data on the card. During times when communications with the central controller are lost, the card reader stores the I.D. data from the card, for each employee who was granted authorization, in a buffer for later transmission to the central controller.

The improved card reader can also monitor alarm contacts for changes in status and signal these changes to the central controller. The central controller can be programmed to make a conditioned response to the reader coupled to the changed contact or to any other reader in the system. The response message can cause a relay or relays in the reader to change states, thereby signalling any devices coupled to the relay or relays that an action in response to the changed alarm contact is desired.

Brief description of the drawings

Figure 1 is a block diagram of a security system in which the improved reader of the invention could be used.

Figure 2 is a block diagram of the improved reader.

Figure 3 is a logic diagram of the optical isolator board.

Figures 4A and B are a logic diagram of the switch and relay board.

Figures 5A and B are a circuit diagram of the RAM buffer board and power fail detect circuit.

Figures 6A, 6B and 6C are circuit diagrams of the CPU reader board.

Figure 7 is a logic diagram of the CCM/COM logic.

Figures 8A and 8B are a logic diagram of the circuitry of the delayed transmission buffer.

Figure 9 is a flow diagram of the sequence of steps performed by the card reader in performing a time and attendance function.

Figure 10 is a flow diagram of the steps which are taken to unload the time and attendance data from the buffer and transmit it to the central controller 20.

Figure 11 is a flow diagram of the time offset routine performed by the card reader.

Figure 12 is a flow diagram of the steps taken by the card reader in buffering transactions during a degraded mode when communication is lost with the central controller.

Figure 13 is a flow diagram of the manner in which the card reader CPU unloads the delayed transmission buffer when communications are restored.

Figure 14 is a flow diagram of the manner in which the card reader CPU senses alarm contacts.

Figure 15 is a flow diagram for reporting of the status of alarm contacts by the card reader CPU.

Figure 16 is a flow diagram for the central controller process for an automatic response to a change in an alarm contact.

Detailed description of the preferred embodiment

Referring to Figure 1 there is disclosed a system diagram of a typical magnetic card reading security system. A controller 20 is coupled to a plurality of card readers of which readers 22 and 24 are typical. The controller 20 is coupled to each reader by an enable pair and a data pair by which the controller can communicate with any card reader in the system.

For example, the controller 20 communicates with the reader 22 by an enable pair 26 and a data pair 28. The controller 20 polls the reader 22 for messages and sends commands to it by the enable pair 26. Data is sent to the controller 20 from the reader 22 via the data pair 28. Serial format is used on both lines.

The reader 22 is typically located at a door that needs to be access-controlled while the controller 20 can be located at some distance from the door. The structural details of the controller 20 are well known in the art, and it can be purchased under the model designation MAC 530/40 from Rusco Electronic Systems in Glendale, California. The object code software for the controller is also well known and can be purchased from the same source.

In operation, the reader 22 receives a magnetic card in a card slot 32. The details of a typical magnetic card structure will be found in U.S. Patents 3,717,749 or 3,811,977. Other structures could also be used; the details of the structure of the magnetic card are not critical to the invention. Any structure capable of holding data encoded in a card and converting it to electrical signals capable of being transmitted over a line will be satisfactory.

When the card is read, the data on the card is stored in a temporary RAM location until a polling signal from the controller 20 arrives on the enable lines 26. Upon receipt of the polling signal on the line 26, the data from the card is transferred on the data lines 28 to the controller 20 unless certain options are present which cause the reader to independently make the authorization decision. The controller 20 processes the data and sends back a "Go" or "No Go" command which causes the reader 22 to take the appropriate action. If the command is "Go", the reader 22 unlocks the door latch via the lines 34 and lights a green LED. If the command is "No Go", the reader 22 lights a red LED and, optionally, energizes a No Go relay.

The reader 22 can also incorporate circuitry to monitor a plurality of alarm contacts connected to

the lines 30. When one of the contacts changes state, the reader 22 senses the change and signals the controller 20 on the next poll. The controller 20 can then print out a pre-programmed message on a printer 36. More importantly, the controller 20 can automatically send back a command to cause a switch closure by energizing a relay in the reader 22 or in any other reader in the system. This automatic response can also be any other command that the reader receives normally from the controller. The relay can be connected to an emergency device via the lines 38. The emergency device can be any device such as an automatic phone dialer, a sprinkler system, an alarm or whatever other device that is desired.

The reader 24 is a different type of improved reader which can be used to keep time records for the attendance of hourly employees' on their jobs. The reader 24 has a display 40, a card slot 42, and "in" and "out" buttons, 44 and 46. In operation, an employee would place his card in the card slot 42 and press either the "in" button 44 or the "out" button 46. The data on his card plus the time of day displayed in the display 40 would then be stored in a buffer in the reader 24. Based upon the system code data on the card, the reader 24 would authorize or deny entry to the employee. If entry is authorized by the reader 24 and a green LED will be lit, the door will be unlocked via the lines 48. If entry is denied, the reader 24 will so indicate by lighting a red LED on the face plate. All authorization or denial decisions are made locally by the reader 24, and the data regarding each transaction is stored in the local buffer in the reader 24.

The controller 20 is coupled to the reader 24 by an enable pair 50 and a data pair 52. The controller 20 polls the reader 24 by sending a poll signal on the line 50. Upon receipt of the poll signal, the reader 24 transfers the data for one transaction out of its buffer to the controller 20 via the data lines 52. The controller then can process the data in any fashion including printing it out on the printer 36. The details of the structure and operation of the controller 20 are exemplified by U.S. Patents 4,216,375 and 4,218,690.

The reader 24 can also include means to offset the time displayed in the display 40 from the time kept by the controller 20 in the case that the controller is in a different time zone from the reader. Normally the controller 20 keeps the master time for the system and the reader 24 keeps its own time. Every 15 minutes, the reader 24 inquires the time of the controller 20 and synchronizes the reader's local time with the master time kept by the controller. When the reader 24 is in a different time zone from the controller 20, a group of offset switches in the reader 24 are set to indicate the number of minutes of offset between the local reader time and the controller time.

The reader 22 can also include a local buffer for keeping a record of all transactions which occur during times when communications with the controller 20 are lost due to cutting of the wire

pairs, power failure or for other reasons. When the reader 22 has not received a poll from the controller for a predetermined time, the reader will start storing the data for transactions during the downtime in its local buffer. Each magnetic card has a system code and an ID code. The system code is used by the reader to determine whether or not to grant authorization for entry to the individual. If the individual is permitted to enter, his ID code and the local time will be stored in the local buffer. When communications with the controller 20 are restored, the data in the buffer will be sent to the controller via the data lines for processing there.

Referring to Figure 2, there is shown a block diagram of a card reader for use in a security system such as is shown in Figure 1. Although in reality two different types of readers exist, the core circuits of each type of reader are the same with one type of reader having certain additional optional circuits which the other does not have. Figure 2 represents a combined functional block diagram of a reader with the common core circuits and with all the optional circuit elements of both types of readers also present.

The card reader of Figure 2 communicates with the controller 20 of Figure 1 through an isolation board 54. The isolation board 54 serves to isolate the data on the enable pair 26 and data pair 28 from the logic circuitry of the rest of the card reader. The isolation board 54 passes the signals from the enable line 26 through to the RX data lines 56 and passes the data from the Tx data lines 58 through to the data lines 28.

The RX data lines 56 are coupled to a multiplexer 60 in a switch and relay board 62. The purpose of the multiplexer 60 is to select various data channels for connection to a data line D7, 63, of a bus 64. The bus 64 is coupled between the switch and relay board 62 and the data, address and control terminals of a microprocessor CPU 66 on a reader CPU board 67. Address lines A0-A2 from the bus 64 are also coupled to the multiplexer 60. Through these address lines, the CPU 66 causes the multiplexer 60 to select one of the data channels connected to it for connection to its data output coupled to the line D7. The microprocessor 66 can then read the data on the selected data channel through the D7 line 63. In Figure 2 the only data channels which are shown are the Rx data line 56 through which commands and polling signals are received and the coil detect line 57 which carries data read from the card. Other data channels are used for other features of the reader not relevant to the present discussion.

Data to be transmitted from the card reader to the central controller 20 are input from the D0 line 68 of the data bus 64 to a driver 70. The driver 70 is also coupled to the A0-A2 address lines of the data bus 64 which supply an address from the microprocessor 66. The driver 70 has several addressable outputs, one of which is the Tx data lines 58. The address supplied to the driver 70 causes it to apply the signal on the D0 line 68 to

the selected output. To transmit data, the microprocessor 66 places the data to be sent on the D0 bus line and writes the proper address on the address lines A0-A2 of the bus 64. The serial data on the D0 line is then applied to the Tx data lines 58.

The central controller 20 receives the data on the data line 28 and acts upon the data message in some fashion depending upon what the message is and may or may not send a command back to the card reader via the enable line 26.

A go relay 71 is coupled to a door latch device by the lines 34. The lines 34 can be coupled to relay contacts or other switching devices to provide an interruptible current flow path to control whether the door latch is in a locked or unlocked state. The go relay is also coupled to the driver 70 by a switching line 72. The switching line controls the state of the go relay and thereby controls the state of the door latch device. The switching line is addressable by the microprocessor 66 through the driver 70 such that the microprocessor 66 controls the state of the go relay 70.

The microprocessor 66 is also coupled to a card reader coil circuit 74 by the bus 64. The card reader coils 74 consist, in the preferred embodiment, of a plurality of coils coupled to the address and data line of the bus 64 and physically arranged so as to individually magnetically interact with a plurality of magnetized spots on a card inserted in the card slots 42 or 32. The microprocessor 66 can individually address and read each coil in the card reader coil circuit 74 to determine the data in the magnetic spots on the card. The details of the card reading coil circuit are known to those skilled in the art and are not critical to the invention.

The microprocessor 66 is also coupled to an optional display 40 by the bus 64. In readers which are being used for time and attendance functions, i.e., as time clocks, it is desirable that the time of day be displayed externally for the benefit of workers who are lined up and waiting to put their cards into the reader 24 to start or end their work shifts. The display 40 can be any conventional display, and the details of its construction are not critical to the invention.

The microprocessor 66 is also coupled to a random access memory (RAM) board 78. The RAM board 78 contains a RAM buffer memory 80, a battery backup system comprised of a battery 82 and a power fail detect circuit 84. The power fail detect circuit 84 monitors the 12 volt unregulated D.C. voltage derived from the A.C. power line and connects the battery 82 to the power terminals of the RAM buffer 80 when the A.C. line power fails so as to preserve the data stored in the RAM 80. The RAM 80 is selected by the microprocessor 66 through connection of a decoder 86 to the address and control lines of the bus 64. When the microprocessor 66 wishes to write a word in the RAM 80, the microprocessor generates the proper address to select the RAM 80 and places it on the bus 64 thereby enabling the RAM 80 through the decoder 86. The data to be written

into the RAM 80 is then placed on the data lines of the bus 64.

A delayed transmission buffer 88 is also coupled to the microprocessor 66 through the bus 64. The purpose of the delayed transmission buffer 88 is to store data read from the magnetic cards during times when communication with the central controller 20 are lost.

A CCM/COM board 90 is also coupled to the microprocessor 66 by the bus 64. The purpose of the CCM/COM board 90 is to monitor the condition of an alarm device or devices external to the card reader and to generate data indicating the condition of the alarm devices for transmission to the central controller. The CCM/COM board 90 also can receive data from the central controller which causes a switch closure on the CCM/COM board. This switch is coupled to an emergency device by the lines 38. The alarm contacts are coupled to the CCM/COM board 90 by the lines 30.

When the card reader is being used for a time and attendance function, the In and Out buttons 44 and 46 are used to tell the card reader whether the cardholder wishes to enter or leave an area. The In and Out buttons 44 and 46 are coupled to the MUX 60 in the switch and relay board 62 by the line 92.

A red and a green indicator LED, represented by block 97 are each coupled to the MUX 60 by the bus 96. The LED's are used by the microprocessor 66 to signal whether authorization has been granted or denied.

The microprocessor 66 is coupled to a feature memory 98 and to a program memory 100 by the bus 64. The program memory 100 stores the instructions for the microprocessor 66 and the feature memory 98 stores data indicating which options are in effect for the microprocessor 66.

Referring to Figure 3, there is shown a circuit diagram for the isolation board 54 in Figure 2. The data lines 28 are coupled to the collector and emitter of a transistor 106 in the optical isolator 102. The light emitting diode 108 of the optical isolator 102 is coupled across the TX data lines 58. When the current is flowing in the TX data lines 58, the LED 108 is energized and emits light causing the transistor 106 to assume one of its two switching states. The opposite state is assumed when the LED 108 is de-energized.

The enable lines 26 are coupled through a noise suppression circuit 110 to the LED 112 of an optical isolator 116. The transistor 114 of the optical isolator has its collector and emitter coupled to the RX data lines 56. In the preferred embodiment, the optical isolator 116 is a Monsanto MCT2. The optical isolator 102 is a Monsanto 4N33.

The details of the circuit of the switch and relay board 62 are given in Figures 4A and B which are a logic diagram of that board. The RX data line 56 is coupled to the data input D1 of the multiplexer 60A. A resistor 59 couples a +5 volt supply to the line 56 to positively clamp it at a logic 1 level except where the transistor 114 on the isolation board clamps the line 56 to ground potential. The

other data inputs of the multiplexer 60A are coupled to other data channels. For example the card reader coil circuit 74 is coupled to the D0 input of the multiplexer 60A by a line 57. The coil detect signal line 57 carries the data from each coil in the card reader coil circuit 74 as it is addressed by the microprocessor 66. The out switch 46 and the in switch 44 are coupled to the D2 and D3 inputs respectively by the lines 118 and 120.

The address inputs 122 of the multiplexer 60A are coupled to the A0-2 address lines of the bus 64. The output 63 of the multiplexer 60A is coupled to the D7 data line of the bus 64. The microprocessor 66 controls which of the data inputs are coupled to the data output 63 by the address it supplies on the address lines 122. The chip select input 126 is coupled to the address lines in the bus 64 of the microprocessor 66 through a decoder on the reader CPU board to be discussed more fully below. The microprocessor 66 can enable the multiplexer 60A by writing the proper address on the address lines driving the decoder coupled to the line 126 (not shown).

A multiplexer 60B has its data output coupled to the D7 data line 63. The data inputs of the multiplexer 60B are coupled to various data channels. The X0 data input is coupled by the line 128 to a "tamper" switch (not shown). The tamper switch is physically situated so as to change states when the faceplate of the card reader is removed causing an alarm message to be transmitted to the controller 20. The X1 data input is coupled to a "card in" switch (not shown). The "card in" switch is situated so as to change states when a card is inserted in the card slot. By periodically checking the condition of these two switches, the microprocessor 66 can tell whether tampering is occurring or whether there is a card to be read in the card slot.

There are three groups of eight switches of the switch and relay board 62. A time offset group of switches 136 is comprised of 8 switches 136A-H which are used to set a binary number representing the number of minutes of time offset at the local card reader. In those cases where the local card reader is in a different time zone than the central controller 20, the switches 136 are set for the number of minutes by which the local time at the card reader differs from the time at the central controller.

A second group of switches 138 has several purposes. The switches 138A-D are used to set the amount of time that the unlock signal on the lines 34 to the door latch device causes the door latch to remain unlocked. The switches 138A-D also determine the time of energization of a No Go relay 166 and the time the red and green LEDs (not shown) in the block 97 in Figure 2 are energized during certain times in the operation. The switch 138E is used to signal whether a 12 hour or 24 hour time display format is desired. The switch 138F is used to enable and disable the buffer RAM 80 as an option. The switches 138G and H are not used.

The switches 140 are used by the customer to set the system code. The system code is one of the items of data which is magnetically stored on each cardholder's card. When the card reader makes the authorization decision locally without consulting the central controller 20, it is the system code stored on the switches 140A-H which is compared to the system code on the cardholder's card to determine if authorization will be granted.

The switches 136, 138 and 140 are individually addressable by the microprocessor 66 through the multiplexers 60A and 60B and a decoder 140. The decoder 140 has address inputs 142 coupled to the address lines in the bus 64. The address supplied on the lines 142 is converted in the BCD to decimal decoder 140 to a logic zero signal on one of the output lines 0-6 which comprises a bus 144. Each of lines in the bus 144 is coupled to one terminal of a plurality of switches in the switch groups 136, 138 and 140. When the group address appears on the address lines 142, one of the outputs in the bus 144 goes low thereby activating that group. The other terminal of each switch is coupled to the cathode of a diode which has its anode coupled to one of the X0-X3 inputs of the multiplexer 60B via the lines 132, 134, 130, 128, 146 or 148. All of the X0-X3 inputs are also coupled to a +5 volt supply through the resistors 150, 152, 154 and 156. The X0-X3 inputs will be held in a logic one condition except if the line coupling that input is also coupled to a group of switches of which one has been enabled by a logic zero from the decoder 140 and the switch is closed.

The groups of switches coupled to the X0-X3 inputs of the multiplexer 60B intersect with the groups connected to the bus 144 such that for any particular output of the decoder 140 which has been enabled, and for any particular input of the multiplexer 60B which has been enabled, only one switch is coupled to both enabled lines. Thus the microprocessor 66 can individually read each switch in the groups 136, 138 and 140 by changing the address signals on the address lines of the bus 64.

The multiplexer 60B has its inhibit line grounded by the line 158 and its disable input held high by connection through a resistor 160 to a +5 volt supply. The disable input is pulled low to take the D7 output out of the high impedance state when the signal $\overline{\text{CSSW}}$ is true on the line 162. The line 162 is coupled to a decoder on the reader CPU board 67 which is coupled to address and control lines of the microprocessor 66 in the bus 64.

Data to be transmitted to the microprocessor 66 is placed on the Tx data line 58 by a driver 70. The driver 70 also has several other outputs. For example, the output line 164 can be connected to an optional No Go relay 166. When the line 164 is grounded by the driver 70, a +5 volt supply coupled to the other terminal of the coil of the No Go relay 166 causes current to flow through the relay coil, thereby energizing it and causing the

electrical conditions on the lines 168 coupled to the relay contacts to change.

In the preferred embodiment, the decoder 140 is a 74145 type TTL decoder such as made by Signetics, the MUX 60A is a 74LS 251 type multiplexer such as is made by Texas Instruments, the MUX 60B is a MC14512, (CMOS type decoder such as is made by Motorola, and the driver 70 is an NE590 type amp driver such as made by Signetics.

An output line 96 from the driver 70 is coupled to the GO LED (not shown) to energize it when authorization to access has been granted. An output line 72 from the driver 70 is coupled to a terminal of the coil of a GO Relay 71. When the driver 70 grounds the line 72, a +5 volt supply coupled to the other terminal of the relay coil energizes the coil, causing the relay contacts to change the condition on the lines 34 coupled to the door locking device.

The driver 70 has a data input, the D_0 data bit on the line 68, and it has address inputs on the lines 172. The address inputs 172 are coupled to the microprocessor 66 by the bus 64. The address at these inputs determines which of the outputs of the driver 70 will be coupled to the data input 68. The microprocessor 66 can thus write a logic 0 or 1 to any of the outputs of the driver 70 by controlling the address on the lines 172 and the data on the data input line 68 which is coupled to data bit zero of the bus 64. The chip enable and clear inputs are coupled to decoder 250 of Figure 6C and a gate 282 in Figure 6B by the signal lines $\overline{CSOUT}$ and $\overline{RST}$.

Referring to Figure 5, there is shown a circuit diagram of the RAM buffer and power fail detect board. The RAM buffer 80 has address lines 174 which are coupled to the address lines of the microprocessor 66 in the bus 64. Data inputs and outputs 176 are also coupled to the microprocessor 66 data lines in the bus 64. A write enable line 178 is coupled to a control line in the bus 64 from the microprocessor 66 to control whether the RAM buffer 80 is reading or writing data through the data lines 176 to the address specified on the lines 174.

A chip select line 180 is coupled to a decoder 86. The decoder 86 has a VMA signal input line 184 coupling one input of a NOR gate 182 to a VMA control line of the microprocessor 66 in Figure 6B. The VMA signal is true when there is a valid memory address on the address lines 174. Because the other input to the NOR gate 182 is grounded, the NOR gate 182 serves as an inverter with the output on the line 186 false when a valid memory address is present on the address lines 174. The resistor 188 couples a positive voltage supply to the VMA input of the gate 182 to hold it at logic one except when VMA is false. The VMA signal on the line 184 is a control signal from the CPU 66 which indicates when a valid memory address exists on the address lines of the CPU. A NOR gate 190 has one input coupled to the output of the NOR gate 182 and the other input coupled to a $\overline{CSRAM_0}$ signal from a decoder 248 in Figure

6C. The CPU 66 can cause $\overline{CSRAM_0}$ to be true, i.e., logic zero, and can assert VMA on the line 184. This causes two logic 0's at the inputs of the NOR gate 190 and a logic 1 appears on the line 194. This logic 1 is inverted in a NOR gate 196 and appears as a logic 0 on the line 198.

A NOR gate 200 serves to gate a power fail detect signal on a line 202 from a power fail detector 84 through to the chip select input at pin 18 of the RAM buffer 80 if power fails. When power has not failed, however, the signal on the line 198 controls whether the RAM 80 is selected or deselected. Normally, the signal from the power fail detector 84 on a line 20 is a logic 0 indicating no power failure. When the signal on the line 198 is a logic 0, the RAM 80 is selected because the signal on the line 204 is a logic 1 which is inverted by a NOR gate to assert the CS signal on the line 180 at logic zero thereby enabling the RAM buffer 80 to read and write data.

A $\overline{RST}$ signal on a line 208 comes from a reset circuit on the reader CPU board which will be described below. The $\overline{RST}$ signal is a logic 0 at power up but becomes logic 1 1.2 seconds later as will be explained in connection with Figure 6B. A NOR gate 210 inverts the signal such that its output line 212 which is coupled to one input of a NOR gate 214 is normally low after power has been on for 1.2 seconds.

The NOR gate 214 has its other input coupled to the output of a comparator 222 in the power fail detect circuit 84. The comparator 222 has its inverting input 224 coupled to a voltage reference of approximately 5.3 volts when the power has not failed. The line 224 is held at this reference level by the voltage divider effect of the resistors 228 and 226 which couple a +12 volt D.C. supply of line power to ground.

The non-inverting input 230 of the comparator 222 is coupled to a 3.6 volt reference source derived from battery power. This reference voltage is generated by a resistor 232 which couples a battery 82 (not shown) to ground through a zener diode 234. The zener has a 3.6 volt breakdown voltage, and has its cathode coupled to the line 230. The comparator 222 has a resistor 236 coupled between the output and its non-inverting input to provide positive feedback. The output on the line 216 will be a logic 0 as long as the power has not failed. When the power fails, the battery reference on the line 230 exceeds the voltage on the line 224, and the output on the line 216 rises to a logic 1 level indicating power has failed.

The logic 1 on the line 216 with the logic zero on the line 212 causes the NOR gate 214 to lower its output on the line 218 to a logic zero. This 0 on the line 218 is inverted to a 1 on the line 202 by the NOR gate 220 which causes the output of the gate 200 to change to a 0, thereby deselecting the buffer 80 if it was in a selected condition. When the RAM buffer 80 is deselected, no data may be written into or read out of the buffer. The power input 238 of the RAM buffer 80 will be coupled through any known switching mechanism 240 to

the battery 82 (not shown) via a line 242 upon power failure.

Referring to Figures 6A, 6B, and 6C, there is shown a circuit diagram of the reader CPU board. The microprocessor 66 is coupled to a feature memory 98 by data lines 240 and address lines 242. The feature memory contains data regarding which options are incorporated into the card reader. The microprocessor 66 is also coupled to a program memory 100 by the data lines 240 and the A0-A4 address lines 242. The enable inputs of the memories 100 and 98 are coupled via the lines 244 and 246 to the microprocessor's address lines 242 through decoders 248 and 250, respectively, in Figure 6C. A clock 252 generates timing signals for the IRQ and NMI inputs on the lines 254 and 256, respectively. The details of the construction and operation of the clock and of the feature and program memories will be appreciated by those skilled in the art. Any mechanism which generates signals periodically on the lines 254 and 256 will suffice for purposes of the invention.

The microprocessor 66 executes the instructions which are stored in the program memory 100. Within the program, which will be described below, there are certain subroutines which accomplish various housekeeping routines. The IRQ and NMI inputs on the lines 254 and 256 cause vectoring to certain of these subroutines. For example, the IRQ line 254, when asserted true, will cause the program control of the microprocessor 66 to be vectored to a routine which reads all the switches described herein.

When the NMI line 256 is asserted true, the microprocessor 66 is vectored to a transmit routine which transmits data to the central controller 20 via the Tx data lines 58 and data lines 28.

The microprocessor 66 must be reset to the beginning of the program upon the initial application of power to the circuit. A power on reset circuit 254 accomplishes this purpose. A comparator 256 has its non-inverting input 258 coupled to a reference voltage defined by a resistive voltage divider comprised of the resistors 262 and 264 coupling the power supply to ground. The inverting input 260 is coupled to one terminal of a capacitor in an RC circuit comprised of a resistor 266 and a capacitor 268. When the power is first turned on, the capacitor 268 acts as an initial short to ground and the voltage on the line 258 will exceed the voltage on the line 260, and the output of the comparator 256 on the line 270 will be a logic 1. The line 270 is coupled to the input of a NOR gate 272 which acts as an inverter. The resistors 274 and 276 serve as a voltage divider to hold the line 270 in a logic 1 condition except when the comparator 256 asserts the line 270 low.

The logic 1 at power up on the line 270 is inverted once in the NOR gate 272 and again in a NOR gate 278 to become the PONCLR signal on the line 280.

As the voltage on the capacitor 268 rises, it exceeds the voltage on the line 258 at a time determined by the values of the resistor 266 and the capacitor 268. When this happens, the 1 on the output line 270 changes to a 0 and line 280 follows

suit. The initial 1 on the line 280 is communicated to the reset line 284 of the CPU 66 as a 0 by passage through a NOR gate 282. The other input to the NOR gate 282 is a line 286 from a deadman reset circuit 288. The line 286 is normally a logic 0 except when there is a problem, as will be described below. With the line 286 normally logic 0, the initial logic 1 on the line 280 is inverted by the NOR gate 282 and resets the microprocessor 66 to the beginning address of the program. Thereafter, the line 280 goes to a logic 0 and stays there.

The deadman reset circuit 288 serves to reset the microprocessor 66 in case there is a software problem. Normally, the deadman reset circuit 288 will attempt to reset the microprocessor 66 periodically unless the software gives a trigger signal "D/M trigger" on the line 290. Thus if for some reason the signal D/M trigger does not occur, program control is lost, and the deadman reset circuit will cause the program counter to be reset to the beginning program location.

The manner in which the deadman reset function is accomplished is through the use of two retriggerable monostable multi-vibrators 292 and 294. The one shot 292 has its B and clear (R_{D2}) inputs coupled to a +5 volt source through a resistor 296 and are therefore always in a logic 1 state. The 0 output on the line 298 is normally low until a negative transition occurs on the D/M trigger line 290, at which time the 0 output line 298 goes to a logic 1 state for a time determined by the values of the resistor 300 and the capacitor 302 coupled to the external RC circuit terminals. However, the pulse time established by the resistors 300 and 302 is longer than the period of the D/M trigger signal. Thus, the output line 298 will not return to zero after the initial trigger pulse because the D/M trigger signal on the line 90 continues to retrigger the one shot 292.

The signals on the lines 298 and 280 are coupled to the inputs of a NOR gate 304. The output line 306 of the NOR gate 304 is coupled to the clear input of the one shot 294. The B input of the one shot 294 is held in a logic 1 condition by connection to a +5 volt supply through the resistor 296. The A input of the one shot 294 is coupled by a line 308 to the clock 252 and carries a 600 Hertz clock signal.

After the initial power up period, the NOR gate 304 will have a logic 0 at the input coupled to the line 280 and a logic 1 at the line 298 input unless the D/M trigger signal on the line 290 does not occur. The output line 306 will remain in a logic 0 state at all times which causes the one shot 294 to ignore all signals at the A and B inputs. However, if the D/M trigger signal on the line 290 fails to occur on schedule, indicating some problem with the program execution, the one shot 292 will time out and enable the one shot 294. The clock signal on the line 308 will then trigger the one shot 294 causing a logic 0 to 1 transition on the line 286. This causes the line 284 to drop from logic 1 to 0 and resets the microprocessor 66.

Referring to Figure 6C, there is shown a logic diagram of the decoder circuitry which forms part of the decoder 86 in Figure 2. The decoder chip 248

has its select inputs coupled to the AI2-AI4 lines of the address bus 242 of the microprocessor 66. The G1 enable input 310 is coupled to the $\emptyset 2$ output from the microprocessor 66 which is the clock signal for the rest of the system. The G2A enable input low by virtue of being coupled to a logic 1 through a resistor 312 and an inverter 314. The G2B input is coupled to the power on clear signal PONCLR on the line 280.

The decoder 250 has its A and B select inputs coupled to the address bus 242 and its C select input coupled to the R/W signal from the microprocessor 66. The G1 enable input is coupled to the $\emptyset 2$ clock signal from the microprocessor 66, and the G2A enable signal is connected to the Y0 output from the decoder 248. The G2B enable input is coupled to the A7 line of the address bus 242 from the microprocessor 66.

Both the decoders 248 and 250 are 74L5138 one of eight decoders such as are manufactured by Texas Instruments. The outputs of the two decoders 248 and 250 are coupled to the various chip select inputs in the system as labelled in Figure 6C. By writing the proper addresses on the address lines 242, the microprocessor 66 can enable any chip in the system needed for a particular operation.

Turning to Figure 7 there is shown a logic diagram of the CCM/COM board 90 in Figure 2. A plurality of alarm contacts are connected to the board by a plurality of wire pairs together comprising the bus 30. Each pair in the bus 30 is energized by connection of one of the lines through one of the resistors 313—320 to a 5-volt power supply. The other line from the pair is coupled through a parallel RC noise suppression circuit to the anode of the diode in one of the optical isolators 321—328. The diodes are energized as long as the external contacts coupled to the wire pairs are closed.

The transistors in the optical isolators have their collectors coupled to a +5-volt regulated power supply through one of the resistors in the resistor block 329. The collectors are also coupled to the data channels of a multiplexer 330 which is typically a 14512B type multiplexer such as is made by Motorola. The data input of the multiplexer is coupled to the D7 data line 63 of the microprocessor 66. The select inputs 332 are coupled to the A0-A2 address lines of the microprocessor 66 such that the microprocessor can individually read each external contact condition through the D7 data line 63.

The microprocessor 66 is programmed to periodically check the condition of each of the external contacts coupled to the bus 30. After the contact is read, the microprocessor 66 operates on a flag to indicate the status of the alarm contact corresponding to that flag. The flags are address positions in a RAM memory 334 which can be a 6116 type CMOS static RAM such as is made by Hitachi. The address inputs of the RAM 334 are coupled to the address lines 242 of the microprocessor 66, and the data I/O ports of the RAM 334 are coupled to the data lines 240 of the

microprocessor 66. The R/W input line 335 of the RAM 334 is coupled to the R/W control signal from the microprocessor 66 to control the direction of the data flow on the data lines 240.

The chip select input line 336 of the RAM 334 is coupled to the Y3 output of a decoder 338 which has its A and B select inputs coupled to the VMA control signal line 184 and A11 address line respectively of the microprocessor 66. The enable input signal $\overline{\text{CSRAM0}}$ on the line 192 for the decoder 338 is coupled to a chip select output from the decoder 248 in Figure 6C such that the microprocessor 66 can enable the RAM 334 by enabling the decoder 338 and writing the proper bit on the A11 line of the address bus.

Only two outputs from the decoder 338 are used so only one address bit is needed to specify which output is active. The other output on the line 342 is coupled to the chip select input 342 of a relay driver 344. This driver 344 has three address inputs 346 which are coupled to the address lines of the microprocessor 66. The relay driver also has a data line 348 coupled to the buffered D0 data line of the microprocessor 66 through a 74L504 buffer 349 on Figure 6C. The relay driver 344 has an output 350 which is coupled to the coil of a COM relay 352. When the microprocessor 66 selects the relay driver 344, and writes the proper address on the lines 346, the line 348 will control the state of the line 350, thereby controlling the state of the relay contacts 354.

Turning to Figures 8A and 8B there is shown a logic diagram of the circuitry of the delayed transmission buffer 88 of Figure 2. A battery backup circuit 356 in Figure 8B serves to protect the information in the RAM chips shown in Figure 8B. Each of the RAM chips is a 6116LP-4 CMOS static RAM such as is manufactured by Hitachi. The +5-volt line supply voltage on the line 358 normally causes a forward bias on the diode 360 and the +5 volt signal is thus coupled to the output line 362. However, when the power fails, the positive voltage on the line 364 from the battery 366 exceeds the voltage on the line 358 which causes a reverse bias on the diode 360. The diode 368, however, will be forward biased such that the battery power will be coupled to the line 362 to keep the information in the RAM intact.

A series of decoders 370—372 are coupled to the A11 line of the address bus 242. These decoders are 74L5139 one of four decoders in the preferred embodiment. The decoders have outputs 373—378 which are coupled to the chip select inputs of the 6 RAM chips of Figures 8B through a power fail detect circuit 382. Each decoder has its B enable input coupled to the VMA output 184 from the microprocessor 66 to enable the decoder to read the A11 bit when the decoder has been enabled. The decoders 370—372 are enabled by enable signals on the lines 379—381 coupled to the decoder 248 in Figure 6C. A power fail circuit 382 senses when the line power represented by the voltage on the line 358 has failed by comparing the voltage at node 386 maintained by the line to the voltage at

a node 388 maintained by the battery 366. A comparator 390 changes the state of its output 392 when the battery voltage at the node 388 exceeds the line voltage at the node 386. The comparator is a National LM311 in the preferred embodiment.

The chip select signals on the lines 373—378 are individually coupled through 74L532 OR gates 393—398 to the chip select inputs of the RAM chips in Figure 8B. Each chip select input is also coupled through the OR gates 393—398 to the output 392 from the comparator 390 such that when the comparator finds a failure of line power, all the RAM chips in Figure 8B will be deselected so as to maintain the integrity of the data.

The connections and functioning of the RAM chips of Figure 8B will be apparent to those skilled in the art. Data from the microprocessor 66 is input and output on the lines 240 to and from the addresses on the lines 242.

Turning now to Figure 9 there is shown a flow diagram of the steps taken by the card reader in performing a time and attendance function. In this function, the card reader reads cards and locally authorizes entry or departure based upon the system code on the card without consulting the central controller and stores the data for each transaction with the local time for later reporting to the central controller.

In an initialization step 410, the microprocessor CPU 66 clears the RAM 80 on power-up. Thereafter, the CPU 66 transfers on the path 412 to the executive routine 414 where several housekeeping functions are performed. One of these functions is to check for the presence of a card in the card slot. This function is represented by the transfer on the path 417 to the state 413. Where the card switch is checked via the line 130 and the MUX 60B in Figure 4 to determine if there is a card in the card slot. If no card is in the slot, the CPU returns to the executive routine 414 by the path 416. In the executive routine, certain basic tasks are performed. For example, the CPU checks whether a command from the central controller 20 has been received, whether a poll from the central controller needs to be acknowledged or whether there is a request for time from the local controller. Periodically, the CPU returns to the state 413.

If a card was found in the card slot, the CPU transfers to a decision state 418 along the path 420 to determine if the system code on the card in the slot matches the system code set on the switches 140 in Figure 4. To do this, the CPU 66 individually addresses the reading coils in the card reader 74 in Figure 2 via the bus 64. The data from each coil is transferred to the CPU 66 via the coil detect line 57, MUX 60A, D7 line 63 and the bus 64 in Figure 2.

If there is no match, the CPU 66 transfers to a no authorization state 422 via the path 424. In this state, the CPU causes the display 40 in Figure 2 for a preset time to blink in a manner known to those skilled in the art and turns on the red LED in the LED block 97 in Figure 2 for a preset time via the

line 96, the driver 70, the D0 line 68 and the bus 64. The CPU 66 then returns the executive state 414 via the path 423.

If the system code matches, the CPU 66 transfers to a buffer full decision state 424 via a path 426 to determine if there is room in the RAM buffer 80 in Figure 2 to store the present transaction. If the buffer is full, the CPU transfers to a state 427 via a path 428 to ignore the card and display a message on the display 40 in Figure 2 indicating that the buffer is full. The CPU then transfers back to the executive state 414 by the path 430.

If the buffer is not full, the CPU transfers to an authorization state 432 by a path 434. In the authorization state the CPU performs 5 tasks. First the ID code from the magnetic card is stored in the buffer 80 along with the time of day in states 436 and 438. Then the Go relay 71 in Figure 2 is energized for a preset time via the bus 64, the D0 data bit line 68, the address line A0-2 and the driver 70. The Go relay is energized for the time set by the switches 138 in Figure 4 so they must be read via the multiplexer 60B and the D7 data bit line 63.

Finally, the green LED in the LED block 97 in Figure 2 is turned on for a preset time via the line 96 and the CPU displays a "Go" message in the display 40 as represented by the states 442 and 444. The CPU 66 then returns to the executive state 414 via the path 446.

Turning to Figure 10 there is shown a flow diagram of the steps which are taken to transmit the data in the buffer 80 to the central controller 20. The steps of Figure 10 are taken each time a poll signal comes in from the controller 20. The CPU normally operates in an executive mode symbolized by the state 441 in Figure 10. The executive jumps to various subroutines which perform housekeeping and command scan functions as mentioned earlier. These subroutines are symbolized by the state 443. One of the functions is to periodically check for the presence of a poll signal from the controller 20 in Figure 1. The poll signal is sent periodically to each card reader in the system via the enable pair 26 coupled to that card reader. The check for the presence of a poll signal is symbolized by the state 447 in Figure 10. If no poll has been received, the CPU returns to its other housekeeping functions in the state 443 via the path 449.

If a poll has been received, the CPU will check an internal counter which is incremented each time a transaction is stored in the buffer 80. This operation is symbolized by the block 451 in Figure 10. If the count is non-zero, then, the CPU knows that there is data in the buffer 80 which needs to be transmitted to the central controller 20. Transfer is then made to a state 448 by a path 450. If the count is zero, the CPU returns to its other functions because there is no data in transmit. This transfer is symbolized by the path 453.

In the state 448, the CPU determines if the buffer option data is present in the feature memory 98 in Figure 2. If the feature is present,

the CPU will retrieve the data for one transaction from the buffer 80 and transmit it to the central controller 20. This operation is symbolized by the state 454 in Figure 10 and is accomplished by addressing one of the transactions in the buffer 80 and reading the data there by the bus 64. The data is then converted to serial format in the CPU 66 and sent via the D $\emptyset$ data bit line 68 to the driver 70 in Figure 2. The driver then places the data on the Tx data lines 58 and it is sent through the optical isolator board 54 onto the data line 28 to the central controller 20. The CPU then returns to the executive routine via the path 456.

If the buffer option is not present, the CPU 66 will transfer to a state 460 by a path 458 where it checks for the presence of a card in the card slot. If there is a card in the card reader, the card data will be read by the CPU 66, converted to serial format and transmitted to the central controller 20. This step is symbolized by the block 462. Control is then returned to the executive.

If there is no card in the reader, the CPU will transfer to the state 464 via the path 466 to determine if there is a time request pending. The card readers which have the time and attendance function keep the local time but periodically request the time from the central controller so as to synchronize the local time with the central controller time. If there is a time request pending, the card reader will ask the time of the central controller 20 as symbolized by the state 466 and return to the executive via the path 468.

If no time request is pending, the CPU will acknowledge the poll as symbolized by the state 470 and return to the executive routine by the path 472.

Turning to Figure 11, there is shown a flow diagram of the time offset routine performed by the CPU 66 to keep track of the local time from the central controller time when the central controller is in a different time zone from that of the reader.

The first step in the process is to read the offset switches 136 in Figure 4 through the MUX 60B. The value of those switches is stored in RAM at a specific address. This is done 600 times per second in the state 474.

Next, the CPU 66 converts the data in the RAM switch data address to minutes and hours of offset. The data from the 8th switch determined whether the offset is positive or negative while the first 7 switches provide a binary number representing up to 127 minutes of offset. Any number of switches could be used, however. This is symbolized by the states 476 and 478.

Finally, the local time is offset in a state 480 and stored in a local buffer offset time address. Control is then returned to the executive routine.

Referring to Figure 12 there is shown a flow diagram for the steps taken by the CPU 66 in handling transactions during a degraded mode when communication with the central controller 20 is lost. The block 415 symbolizes the executive routine. The background block 443 symbolizes all the routine housekeeping checks and functions that the card reader does when it is not doing one

of the foreground routines to handle certain conditions the CPU discovers during the executive routine. Part of the normal executive routine is to check for the periodic appearance of a poll signal from the central controller. This check is symbolized by the block 490. This function is implemented by the CPU 66 in determining whether a poll signal has arrived in the preceding 30 seconds. If a poll signal has arrived during the last 30 seconds, then there is no degraded mode and the CPU 66 determines what type of command has been received, if any, and processes the command as symbolized by the block 492. Control is then returned to the executive routine by the path 494.

If a poll signal has not arrived during the preceding 30 seconds, the card reader CPU 66 knows that something is wrong and enters the degraded mode. This is symbolized by the path 496. The first step is to determine if there is a card in the reader slot. This step is symbolized by the block 500. If there is not a card in the reader, control is returned to the executive background loop 443 as symbolized by the path 498.

If there is a card in the reader, the CPU 66 addresses the feature memory 98 in Figure 2 to determine if the buffer option is present. This is symbolized by the block 502 in Figure 12.

If the buffer option is not present, then no storage of transactions during the degraded mode will occur. However, it is still possible to authorize or deny access to a card holder based upon the system code that is on his card without storing the I.D. code and time of day in a buffer. To determine whether or not to do this, the CPU 66 must again address the feature memory 98 to determine whether the degraded mode option is present. This operation is symbolized by the block 504 in Figure 12. If the degraded mode option is not in effect, the CPU returns to the background loops 443 by the path 506.

If the degraded mode option is present, the CPU reads the system code on the magnetic card in the reader slot via the card reader coils 74 and then reads the switches 140 in Figure 4. The CPU 66 compares the system code on the card to the system code on the switches for a match. This comparison is symbolized by the block 508 in Figure 12.

If there is no match, the CPU 66 turns on the red LED for a time set by the switches on the switch and relay board 62 in Figure 2. This indicates no authorization as symbolized by the state 510. The CPU 66 then addresses the feature memory 98 to determine if the no go option is in effect, as symbolized by the state 512. If it is not in effect, the CPU 66 returns to the background loops 443 via the path 514. If the option is in effect, the CPU addresses the no go relay 166 in Figure 4 through the driver 70 by placing the proper address on the lines 172 and writing a logic 1 on the buffered D $\emptyset$ data bit line 68. The no go relay 166 is thereby energized for a time set by the switches on the switch and relay board 62, and whatever external device that is coupled to the no go relay contacts

through the lines 167 will be signalled that an unauthorized person has attempted an entry. This operation is symbolized by the block 516 in Figure 12.

If the system code on the switches match that on the card, the CPU 66 energizes the green LED in the LED block 97 of Figure 2 for a predetermined time. The CPU 66 also energizes the go relay 71 in Figure 4 for a time set by the switches 138. This is done in a similar manner to that just described for the no go relay. This operation is symbolized by the block 518 in Figure 12. Control is then returned to the background loops 442 via the path 520.

Returning to the state 502 in Figure 12, if the buffer option is present, the CPU 66 checks its internal counter to determine if the buffer 88 in Figure 2 is full of transaction data. This is symbolized by the block 528 in Figure 12. If the buffer is full, the CPU 66 ignores the card and transfers back to the background loops 443 as symbolized by the path 531 through the state 522.

If the buffer is not full, the CPU 66 will read the system code switches in Figure 4 and the system code data on the card and compare them as symbolized by the block 530. If there is no match, the red LED in the LED block 97 in Figure 2 will be turned on for a time as symbolized by a transfer to the state 510 via the path 532 in Figure 12. Processing from the state 510 will continue as previously described.

If the system code does match, the CPU will store the I.D. code from the card along with the local time in the delayed transmission buffer 88 of Figure 2 as symbolized by the block 533. The green LED and Go relay are then energized for a preset time in state 518.

The buffer 88 is unloaded one transaction at a time when communications are restored. Referring to Figure 13, there is shown a flow diagram of the manner in which the CPU unloads the buffer. During the executive background routine, the CPU 66 continually checks for the presence of a poll signal from the central controller. When a poll finally arrives, the reader knows that communications have been restored. This monitoring function is symbolized by the block 540 in Figure 13. If no poll has arrived, the CPU returns to its other background functions as symbolized by the path 542.

If a poll has arrived, the CPU 66 will check to see if any higher priority messages are waiting to be sent as symbolized by the block 544. If there is such a message, it is sent, as symbolized by the block 546, and control is returned to the background routine of the executive.

If no higher priority message is waiting, the CPU 66 will determine if there are any transactions stored in the buffer waiting to be sent as symbolized by the block 548. This is done by consulting the internal counter in the CPU 66 to determine how full the buffer 88 is. If no data, is in the buffer 88, the CPU determines whether there is a time request pending as symbolized by the block 550. If there is, the CPU 66 moves to the

state 552 to request the time from the central controller and then returns to the executive routine. If there is no time request pending, the CPU 66 will acknowledge the poll in a state 554 and return to the executive routine.

Returning to the state 548 in Figure 13, if there are transactions in the buffer 88 to be sent, the CPU 66 will retrieve one transaction data group, format it for serial transmission and transmit it in the manner previously discussed, using the D0 data bit line 68, the driver 70, the address lines A0-2, the Tx data lines 58 and the isolation board 54. The format for the transmission in the preferred embodiment is a header identifying the type of reader with the data, followed by a condition code indicating the type of transaction that has been retrieved. Following the condition code, the I.D. data from the card is sent along with the time of day when the transaction occurred. These steps are symbolized by the block 556. Any format for transmission will do, however. Control is then returned to the executive routine.

Turning now to Figure 14, there is shown a flow diagram of the steps the card reader CPU 66 takes in monitoring the alarm contacts connected to the lines 30 from the CCM/COM board 90. The routine illustrated in Figure 14 is executed by the CPU 600 times per second and is intended to sense the condition of the flags which symbolize the state of the alarm contacts. The first step is to read a CCM flag N to determine the last state of the flag. This step is symbolized by the block 560 in Figure 14. To do this the CPU 66 picks the address for the flag N in the RAM 334 of Figure 7 and writes that address on the lines 242 after selecting the RAM with the A11 and VMA lines coupled to the decoder 338 to drive the line 336 low. The R/W input of the RAM 334 is driven to the read state by the microprocessor 66 in Figure 6A.

There are four possible states for the flag symbolizing the state of its corresponding alarm contact. The flag can show "open and reported", "closed and unreported", "open and unreported" or "closed and reported". One 8 bit byte is used to symbolize these states.

If the flag shows "closed and reported", the CPU 66 must know whether the alarm contact N has changed status since its last state as indicated by the flag N. Therefore, the CPU 66 causes the alarm contact N to be read. This step is represented by the transfer on the path 561 to the block 566 and is physically accomplished by selecting the contact N address and writing that address to the multiplexer 330 on the lines 332 in Figure 7. The CPU 66 also enables the multiplexer 330 in any known manner utilizing the CSCCM signal connected to pin 15 of the multiplexer 330. The CSCCM signal can be generated by decoders coupled to the address bus of the CPU 66 or in any other known manner. With the address on the lines 332 set, the multiplexer 330 will select the one of its outputs X0-X7 for connection to the D7 line coupled to the CPU 66 data bus 64. The CPU 66 can then read the desired contact through one of the optical isolators 321-328.

If the alarm contact N is open, the CPU 66 knows that the alarm contact has changed its status since the last time it was read and that this fact must be reported. Therefore the CPU changes the state of the flag N to an "open and unreported" status. This operation is symbolized by the transfer on the path 567 to the block 568 in Figure 14. Because the status of the alarm contacts has changed, the CPU 66 must update one bit of the status word that is kept in RAM to indicate the status of the alarm contacts. The status word has one bit for each alarm contact, and the bit for contact N is changed to indicate the most current status. This operation is symbolized by the transfer to the block 570 on the path 569.

After the status word has been updated, the CPU 66 is ready to move on to read the next flag. To do this, N must be incremented. This step is represented by the path 571 to the block 572. After N is incremented, the CPU 66 must know whether it has completed reading all the flags and contacts. To do this, the CPU compares the value of N after it has been incremented to the total number of alarm contacts connected to the lines 30 in Figure 2. In the preferred embodiment, this number is 7, but it can be any number depending upon how much hardware is available. This comparison operation is represented by the block 574 in Figure 14. If N is less than or equal to 7, the CPU returns to the state 560 by the path 576. If, however, N is greater than 7, the flag reading task is finished and the CPU 66 returns to the executive routine as symbolized by the block 578.

If the flag N has been in the "open and reported" state, the CPU would again like to know if there has been any change of status of the alarm contact associated with the flag N. To determine this, the CPU 66 reads the contact N. This operation is symbolized by the path 582 to the state 584.

If the contact N is open, there has been no change from its last status and the CPU 66 is ready to read the next flag. N will be incremented and processing continues as previously described. This operation is symbolized by the path 586 to the state 572 previously discussed.

If the contact N is closed, the CPU 66 knows there has been a change in status since the last check. Accordingly, the CPU 66 must set the flag N to indicate the contact N is now closed and unreported. This operation is symbolized by the transfer on the path 588 to the state 90 in Figure 14.

Because there has been a change in the status of one of the alarm contacts, the status word must be updated. This operation is symbolized by the transfer on the path 592 to the state 570. Processing then continues as previously described.

Returning to the state 566, if after reading flag N and finding its status to be "closed and reported", the CPU 66 then reads the contact N and finds that it is still closed, there has been no change in the alarm contact condition since the last reading. Thus there is no need to change the flag status and there is no need to change the status word.

Accordingly, the CPU 66 merely increments N as symbolized by the transfer on the path 567 to the state 572. Processing then continues as previously described.

If in the state 560, the CPU 66 determines the flag N is either "closed and unreported" or "open and unreported", there is no need to read the alarm contact because the central controller has not yet been notified of the change in status of the alarm contact which caused the flag to be set in either of these two states. Since notification is the first priority, the CPU 66 will merely update the status word to indicate the new status and continue reading the other flags. This operation is symbolized by the transfer on the path 600 to the previously described state 570.

Referring to Figure 15, there is shown a flow diagram of the steps taken by the CPU in reporting the changing conditions on the alarm contacts coupled to the lines 30 to the central controller 20 in Figure 1. The routine shown in Figure 15 is periodically executed when program control of the CPU 66 is transferred from the background tasks of the executive routine represented by the block 602 to the routine of Figure 15.

The first step is for the CPU 66 to read the flag N to determine if it has been reported or is currently in an unreported status. If the alarm contact N change in status has not yet been reported as indicated by an unreported status of the flag N, then the CPU 66 sends a CCM message to the central controller 20 reporting the changed condition of the alarm contacts N. These operations are represented by the block 604 where the flag N is read and the transfer on the path 606 to the block 608 where the CCM message is transmitted to the central controller. Referring to Figure 2, the CCM message is transmitted by formulation of the serial format message inside the CPU 66 and placing it on the D₀ data bit line 68 to drive the driver 70. The address bit lines A0-A2 are held by the CPU 66 at the address which connects the D₀ data bit line to the Tx data lines 58. The serial data CCM message then passes through the optical isolators on the isolation board 54 and over the data lines 28 to the central controller 20 in Figure 1.

The next step after transmitting the CCM message is for the CPU 66 to determine if the flag is open or closed to determine whether to change the flag to a "closed and reported status" or an "open and reported status". This step is represented by the transfer to the state 612 by the path 610.

If the flag is open, the CPU 66 transfers to the state 614 by the path 613 to change the flag status to "open and reported". Control is then transferred to the state 602 by the path 616. If the flag is closed, the CPU 66 must change the flag to indicate that the condition has now been reported. The CPU 66 then changes the flag status to "closed and reported" status. This is represented by a transfer to the state 620 on the path 618. Control is then returned to the state 602 by a path 622. From the state 602 processing con-

tinues. The CPU 66 then transfers to the state 604 where flag N is again read. This time, the flag N will show that it has been reported so the CPU 66 will increment N. This is represented by the transfer to the state 624 by the path 642. The CPU 66 then compares the value of N to the maximum number of flags to be read as represented by a transfer on a path 626 to a state 628. If N is less than the maximum number of flags in the system, control is transferred back to the executive via a path 630. The next time the executive jumps to the routine of Figure 15, the CPU 66 will read flag N+1.

If N is equal to the maximum number of flags in the system, the CPU 66 is finished reading all the flags and need only determine whether the central controller 20 has requested the CCM status word. This determination is represented by a transfer to the state 634 by the path 632. If the central controller 20 has not requested the CCM status word, control is transferred back to the executive via the path 636. If the central controller has requested the CCM status word, the status word is sent as represented by transfer to the state 640 on the path 638. Thereafter, control is returned to the executive via the path 642.

Referring to Figure 16 there is shown a flow diagram of the steps taken by the central controller 20 in Figure 1 to process messages from the card readers regarding changes in the status of the alarm contacts. The blocks 620, 622 and 624 represent individual readers in the system which are coupled to the central controller 20. Each reader has its own data lines, such as data line 28 for the reader N, upon which data is transmitted from the reader to the central controller 20. The controller 20 is also coupled to each reader by enable lines, such as the enable line 26 coupled to the reader N, upon which commands are sent from the controller 20 to the reader.

As represented by the blocks 620, 622 and 624, each reader formulates and sends a number of messages to the central controller.

The messages received by the central controller 20 are deciphered to determine what type of message it is and what is the data in the message. This operation is symbolized by the block 626.

One of the questions asked by the controller is whether or not the received message is a CCM message. This decision is represented by the block 628.

If the message is a CCM message, the controller must determine from the data in the message which alarm contact has changed. This determination is represented by the block 630. The reason for this determination is that the controller may not be programmed by the user to do anything in response to changes in certain alarm contacts. What the controller does in response to a change in status of a particular alarm contact is user programmable. The controller keeps a table of user programmable entries. The table can have an entry for each alarm contact in the system or it may only have entries for some of the alarm contacts. This table is called the CRO table, which

stands for Conditioned Response Option. A typical table entry would include the alarm contact number, the contact condition, the reader location, the condition response location, a CRO override command and time limitation data.

The controller, after deciphering the CCM message, must consult the CRO table to determine if there is an entry for that alarm contact. If there is, the controller will examine the contact condition code, the alarm contact number, and the reader location data in the CCM message to determine if it matches the entry in the CRO table. This operation is symbolized by the block 632 in Figure 16.

The time zone data in the CRO table can be user-programmed to only allow the specified conditioned response if the CCM message for the contact in question comes in within the time parameter. Alternatively, the time zone may be unlimited if the user programs the appropriate code, such that the conditioned response will occur any time a message matching the CRO entry comes into the controller. This operation is symbolized by the block 634.

If there is a CRO table entry and the CCM message comes in within the time parameters of the CRO table entry, the controller will send a CRO command to the location specified in the CRO table entry. This could be to the reader coupled to the CCM contact which changed to cause the CCM message in question, or it could be to some other reader location in the system. This operation is symbolized by the block 636. The CRO response message is sent to a buffer which holds messages to be sent to particular readers until their turn for transmission over the enable lines come up. The messages are sent on a first come, first serve basis. This message buffering and the periodic polling function of the central controller are represented by the block 638. The messages are sent on one of the enable pairs 640.

The central controller also searches the CRO table for other entries regarding the same alarm contact. That is, the central controller may send one or more CRO responses to one or more locations in the system in response to a change on an alarm contact. The CRO response can be any of the reader commands associated with the other reader functions such as "go off line" or "send CCM status word". In particular, it may be a command to energize a COM relay anywhere in the system. This "energize COM relay", command, when received by the CPU 66 in the reader, causes it to address the relay 352 in Figure 7 through the address lines 346 after selecting the driver 344 using the line 342 and the decoder 338. The coil of the relay 352 is then connected to the D0 data bit line 348 from the CPU 66 in Figure 2 such that the CPU 66 can energize the relay coil by writing a logic zero on the line 348. This changes the state of the relay contact 354 which notifies an external device coupled to the relay contacts 354 by the lines 38 that some action is needed. The external device can be a fire alarm, sprinkler system, telephone dialer or any other device.

After the CRO message is sent, the central controller continues on with processing all the incoming messages. This is symbolized by the transition on the path 642 to the state 644. The same would be true if there were either no CRO table entry corresponding to the CCM message or if the CCM message were outside the time zone set by the CRO table entry. These two transitions are represented by the paths 646 and 648, respectively, to the state 644. The central controller then sends data to be printed regarding any or all of the incoming messages to a printer as represented by the block 650. The central controller may send a message to the printer regarding the CCM message if desired.

Claims

1. A card reader (24) for a security system having a central controller (20), which controller keeps the time of day; said card reader comprising a reader circuit (74) for reading data stored permanently on a card: a memory (88); and an authorization circuit (71) in said reader for authorizing or refusing authorization independent of the central controller, based upon the data on said card, said card reader being characterized by:

a time reader (40) for determining the time of day;

a circuit (66) for causing said data read from said card and said time of day to be stored in said memory (88) at a first time; and

a sending circuit (70) for sending said data read from said card and said stored time of day data from said memory (88) to said central controller (20) at a second time controlled by said central controller (20).

2. A card reader as defined in Claim 1, characterized in that said sending circuit (70) causes only data from one card reading transaction to be sent from said memory (88) to said central controller (20) upon a signal from said central controller (20).

3. A card reader as defined in Claim 1, characterized in that said time reader comprises a synchronization circuit (66) for synchronizing the local time at the reader with the time at said central controller.

4. A card reader as defined in Claim 3, characterized in that said time reader further comprises an offset circuit (136) for offsetting the local time kept in said card reader from the time kept by said central controller.

5. A card reader as defined in Claim 1, characterized in that said card contains at least two data items and in that an access circuit (66) in said card reader is enabled by one of said data items.

6. A card reader as defined in Claim 5, characterized in that said memory (88) stores the other of said data items.

7. A card reader as defined in Claim 1, further characterized by an access circuit (66) for controlling physical access to an area and said authorization circuit (71) for communicating with said

access circuit (66) for granting or denying access to said area based upon the data on said card.

8. A card reader as defined in Claim 7, characterized in that said access circuit (66) selectively provides access to a controlled location based upon one of the items of data read from said card.

9. A card reader as defined in Claims 5 or 8, characterized in that said access circuit (66) generates a first signal if access is to be provided and a second signal if access is to be denied.

10. A card reader as defined in Claim 9, further characterized by a disable circuit (71) for disabling said access circuit in response to said second signal.

11. A card reader as defined in Claim 1, characterized in that the circuit (66) comprises circuitry for inhibiting the storage of data from card reading transactions when authorization is denied.

12. A card reader as defined in Claim 1, characterized in that the circuit (66) comprises:

circuitry for determining whether the memory (88) is full; and

circuitry for inhibiting the storage of data in the memory (88) when the memory (88) is full.

13. A method of operating card reader in a security system having a central controller (20) and plural remote card readers, comprising the step of storing card data from cards in a memory (88) at said reader, said method being characterized by the steps of:

reading card data from cards at a first rate determined by the frequency of card insertions at said reader;

producing an authorization signal in said card reader, independent from the central controller (20), in response to appropriate data read from the card; and

transmitting said card data from said memory (88) to said central controller (20) at a second rate determined by said controller (20).

14. A method of operating a card reader as defined in Claim 13, further characterized by the step of storing the time of day in the memory (88) at the card reader, and the step of transmitting the time of day corresponding to the transmitted card data from the memory to the central controller.

15. A method of operating a card reader as defined in Claim 14, further characterized by the step of synchronizing local time kept in the card reader with the time at the central controller.

16. A method of operating a card reader as defined in Claim 15, further characterized by the step of keeping the local time offset from the time at the central controller by a predetermined amount.

17. Use of a card reader according to any of Claims 1—12 for the function of controlling access to a secured area.

18. Use of a card reader according to Claim 17, further characterized by the additional function of identifying who was granted access to the secured area.

19. Use of a card reader according to Claim 17 or 18, further characterized by the additional function of identifying the time at which access to

the secured data was granted.

20. A card reader (24) for a security system having a central controller (20) which communicates with said card reader, said card reader comprising:

a memory (88);

a card reader circuit (74) for reading data stored on cards;

a receiver (54) for receiving data from said central controller;

a memory (80) for storing said data from said card reader in said memory (80) during times when communication with said central controller is lost, characterized in that said central controller (20) periodically polls said card reader (24); and in that

a sensor (84) coupled to said receiver senses when communication with said central controller (20) is lost by the absence of a poll signal from said central controller (20) for a predetermined time, said memory (80) being responsive to said sensor (84).

21. A card reader as defined in Claim 20, further characterized by a time keeper circuit (66) for keeping the local time at said card reader (24) and for synchronizing it with time kept by said central controller (20).

22. A card reader as defined in claim 21, further characterized by an authorization circuit (71) coupled to said card reader circuit (74) for granting or denying access to a controlled location based upon data read from said card.

23. A card reader as defined in Claim 22, further characterized in that said memory (88) includes an inhibit circuit to inhibit the storage of data from card reading transaction when authorization is denied.

24. A card reader as defined in Claim 20, further characterized by:

a memory monitor for determining whether said memory (88) is full; and

an inhibit circuit for inhibiting storage of data in said memory when said memory (88) is full.

25. A card reader as defined in Claim 24, further characterized by an authorization circuit (71) for authorizing access to a controlled location in response to data read from said card, said authorization circuit (71) including an inhibit circuit to ignore data from said circuit card reader circuit (74) when said memory (88) is full.

26. A card reader as defined in Claim 25, further characterized by a time keeper circuit (66) for determining the time of day, said memory (88) storing the time of day with said data from said card reader when said card is read.

27. A card reader as defined in Claim 25, further characterized in that said authorization circuit (71) includes a signalling circuit for generating a first signal when authorization is granted and a second signal when authorization is denied.

28. A card reader as defined in any one of Claims 20 to 27, further characterized by a transmitter for transmitting the data stored by said means for storing, to said central controller (20) when communication is restored.

29. A card reader as defined in Claim 28, further characterized in that said transmitter transmits data for one card reading transaction from said memory at the time of each signal poll from said central controller.

30. A card reader as defined in Claim 22, 25, 26 or 27, characterized in that said card contains a first portion of data and a second portion of data, and in that said authorization circuit (71) includes a circuit for granting or denying authorization based upon said first portion of data only.

31. A card reader as defined in Claim 30, characterized in that said memory (88) stores said second portion of data only.

32. A card reader as defined in Claim 31, characterized in that said memory (88) includes means for storing the local time at the time when said second portion of data is read.

33. A method of operating a security system which controls access to a location and which includes a local card reader (24) and a central controller (20) which communicate to limit access based on card data, comprising the steps of:

storing card data at said local card reader (24) during periods of inability to communicate; and

transmitting stored card data from said local card reader (24) to said central controller (20) when communication is restored, characterized by the steps of:

periodically sending a poll signal from said central controller (20) to said card reader (24); and

sensing at said local card reader (24) for inability to communicate with said central controller (20) by the absence of said poll signal from said central controller (20) for a predetermined time.

34. A method as defined in Claim 33, further characterized by the step of storing the time of day with said card data at said local card reader (24).

35. A security system comprising:

a central controller (20), which keeps the time of the day;

a card reader (22, 24) remote from said central controller (20), said card reader comprising a reader circuit (74) for reading data stored permanently on a card, a memory (88), an authorization circuit (71) in said reader for authorizing or refusing authorization independent of the central controller (20), based upon the data on said card, and a monitor (90) for monitoring the condition of an alarm device external to said card reader and for generating data indicating a change in condition of said alarm device for transmission to said central controller (20); and

a transceiver (26, 28) for transmitting the data from said card reader (22, 24) to said central controller (20) and for receiving data from said central controller (20);

said security system being characterized in that said card reader further includes a time reader (40) for determining the time of day;

a circuit (66) for causing said data read from said card and said time of day to be stored in said memory (88) at a first time; and

a sending circuit (70) for sending said data read

from said card and said stored time of day data from said memory (88) to said central controller (20) at a second time controlled by said central controller (20).

36. A security system comprising:

a central controller (20);

a card reader (22, 24) remote from said central controller (20), said card reader comprising a memory (88), a card reader circuit (74) for reading data stored on cards, a receiver (54) for receiving data from said central controller, a memory (80) for storing said data from said card reader in said memory (80) during times when communication with said central controller is lost, and a monitor (30) for monitoring the condition of an alarm device external to said card reader and for generating data indicating a change in condition of said alarm device for transmission to said central controller (20); and

a transceiver (26, 28) for transmitting the data from said card reader (22, 24) to said central controller (20) and for receiving data from said central controller (20),

said security system being characterized in that said central controller (20) periodically polls said card reader (24) and in that a sensor (84) coupled to said receiver senses when communications with said central controller (20) is lost by the absence of a poll signal from said central controller (20) for a predetermined time, said memory (80) being responsive to said sensor (84).

Patentansprüche

1. Kartenleser (24) für ein Sicherheitssystem mit einer Zentralsteuerung (20), welche die Tageszeit verfolgt, wobei der Kartenleser eine Leseschaltung (74) zum Auslesen von permanent auf einer Karte gespeicherten Daten umfaßt, ferner einen Speicher (88) und eine Autorisierungsschaltung (71) in dem Leser zur Autorisierung oder Verweigerung der Autorisierung unabhängig von der Zentralsteuerung auf der Grundlage der Daten auf der Karte, gekennzeichnet durch:

Einen Zeitleser (40) zur Bestimmung der Tageszeit; eine Schaltung (66), um zu bewirken, daß von der Karte abgelesene Daten und die Tageszeit in dem Speicher (88) an einem ersten Zeitpunkt gespeichert werden und eine Sendeschaltung (70) zum Senden von aus der Karte ausgelesenen Daten und der gespeicherten Tageszeit aus dem Speicher (88) zur Zentralsteuerung (20) zu einem zweiten Zeitpunkt, die von der Zentralsteuerung (20) gesteuert wird.

2. Kartenleser nach Anspruch 1, dadurch gekennzeichnet, daß die Sendeschaltung (70) bewirkt, daß nur Daten aus einer Kartenlesetransaktion von dem Speicher (88) an die Zentralsteuerung (20) aufgrund eines Signals aus der Zentralsteuerung (20) gesendet werden.

3. Kartenleser nach Anspruch 1, dadurch gekennzeichnet, daß der Zeitleser eine Synchronisationsschaltung (66) umfaßt, um die Lokalzeit am Leser mit der Zeit in der Zentralsteuerung zu synchronisieren.

4. Kartenleser nach Anspruch 3, dadurch gekennzeichnet, daß der Zeitleser ferner eine Versetzungsschaltung (136) umfaßt, um die in dem Kartenleser gehaltene Lokalzeit von der in der Zentralsteuerung gehaltenen Zeit zu versetzen.

5. Kartenleser nach Anspruch 1, dadurch gekennzeichnet, daß die Karte wenigstens zwei Datengegenstände enthält und daß eine Zugangsschaltung (66) in dem Kartenleser durch einen der Datengegenstände freigegeben wird.

6. Kartenleser nach Anspruch 5, dadurch gekennzeichnet, daß der Speicher (88) die anderen Datengegenstände speichert.

7. Kartenleser nach Anspruch 1, ferner gekennzeichnet, durch eine Zugangsschaltung (66) zur Steuerung des physischen Zugangs zu einem Bereich und die Autorisierungsschaltung (71) zur Inverbindungsetzung mit der Zugangsschaltung (66), um den Zugang zu dem Bereich auf der Grundlage der Daten auf der Karte zu gewähren oder zu versagen.

8. Kartenleser nach Anspruch 7, dadurch gekennzeichnet, daß die Zugangsschaltung (66) selektiv Zugang zu einer kontrollierten Stelle gewährt, und zwar auf der Grundlage der von der Karte gelesenen Datengegenstände.

9. Kartenleser nach Anspruch 5 oder 8, dadurch gekennzeichnet, daß die Zugangsschaltung (66) ein erstes Signal erzeugt, wenn Zugang gewährt werden soll, sowie ein zweites Signal, wenn der Zugang versagt werden soll.

10. Kartenleser nach Anspruch 9, ferner gekennzeichnet durch eine Sperrschaltung (71) zum Sperren der Zugangsschaltung in Abhängigkeit von dem zweiten Signal.

11. Kartenleser nach Anspruch 1, dadurch gekennzeichnet, daß die Schaltung (66) Schaltungsteile umfaßt, welche die Speicherung von Daten von Kartenlesetransaktionen verhindert, wenn die Autorisierung verneint ist.

12. Kartenleser nach Anspruch 1, dadurch gekennzeichnet, daß die Schaltung (66) umfaßt:

Schaltungsteile zur Bestimmung, ob der Speicher (88) voll ist; und

Schaltungsteile zur Unterbindung der Speicherung von Daten in dem Speicher (88) wenn der Speicher (88) voll ist.

13. Verfahren zum Betreiben eines Kartenlesers in einem Sicherheitssystem mit einer Zentralsteuerung (20) und mehreren fernegelegenen Kartenlesern, umfassend den Verfahrensschritt der Speicherung von Kartendaten von Karten in einem Speicher (88) in dem Leser, wobei das Verfahren durch die folgenden Schritte gekennzeichnet ist:

Lesen von Kartendaten von Karten mit einer ersten Geschwindigkeit, die durch die Frequenz von Karteneinsetzungen am Leser bestimmt wird;

Erzeugen eines Autorisierungssignals in dem Kartenleser unabhängig von der Zentralsteuerung (20) in Abhängigkeit von geeigneten, von der Karte ausgelesenen Daten; und

Übertragen der Kartendaten aus dem Speicher

(88) an die Zentralsteuerung (20) mit einer zweiten Geschwindigkeit, die durch die Steuerung (20) bestimmt wird.

14. Verfahren zum Betreiben eines Kartenlesers nach Anspruch 13, ferner gekennzeichnet durch den Verfahrensschritt, daß die Tageszeit in dem Speicher (88) am Kartenleser gespeichert wird, und durch den Schritt der Übertragung der Tageszeit entsprechend den Übertragenen Kartendaten von dem Speicher zur Zentralsteuerung.

15. Verfahren zum Betreiben eines Kartenlesers nach Anspruch 14, ferner gekennzeichnet durch den Verfahrensschritt, daß die Lokalzeit im Kartenleser mit der Zeit in der Zentralsteuerung synchronisiert wird.

16. Verfahren zum Betreiben eines Kartenlesers nach Anspruch 15, ferner gekennzeichnet durch den Verfahrensschritt, daß die Lokalzeit von der Zeit in der Zentralsteuerung um einen vorbestimmten Betrag versetzt gehalten wird.

17. Verwendung eines Kartenlesers nach einem der Ansprüche 1 bis 12 für die Funktion der Steuerung des Zugangs zu einem gesicherten Bereich.

18. Verwendung eines Kartenlesers nach Anspruch 17, ferner gekennzeichnet durch die zusätzliche Funktion der Identifizierung derjenigen Person, der Zugang zu dem gesicherten Bereich gewährt wurde.

19. Verwendung eines Kartenlesers nach Anspruch 17 oder 18, ferner gekennzeichnet durch die zusätzliche Funktion der Identifizierung der Zeit, an dem Zugang zu dem gesicherten Bereich gewährt wurde.

20. Kartenleser (24) für ein Sicherheitssystem mit einer Zentralsteuerung (20), welche mit dem Kartenleser in Nachrichtenverbindung steht, wobei der Kartenleser umfaßt:

Einen Speicher (88);

eine Kartenleseschaltung (74) zum Auslesen von auf Karten gespeicherten Daten;

einen Empfänger (54) zum Empfang von Daten aus der Zentralsteuerung;

einen Speicher (80) zur Speicherung der Daten von dem Kartenleser in dem Speicher (80) während Zeiten, in denen die Nachrichtenverbindung mit der Zentralsteuerung verloren ist.

dadurch gekennzeichnet, daß die Zentralsteuerung (20) den Kartenleser (24) periodisch abfragt, und daß ein Fühler (84), der mit dem Empfänger gekoppelt ist, feststellt, wenn die Nachrichtenverbindung mit der Zentralsteuerung (20) verloren ist, und zwar durch die Abwesenheit eines Abfragesignals aus der Zentralsteuerung (20) für eine vorbestimmte Zeitdauer, wobei der Speicher (80) auf den Fühler (84) anspricht.

21. Kartenleser nach Anspruch 20, ferner gekennzeichnet durch eine Zeithalteschaltung (66) zum Halten der Lokalzeit in dem Kartenleser (24) und zur Synchronisierung dieser Lokalzeit mit der in der Zentralsteuerung (20) gehaltenen Zeit.

22. Kartenleser nach Anspruch 21, ferner gekennzeichnet durch eine Autorisierungsschal-

tung (71), die mit der Kartenleseschaltung (74) gekoppelt ist, um Zugang zu einer kontrollierten Stelle auf der Grundlage von aus der Karte ausgelesenen Daten zu gewähren oder zu versagen.

23. Kartenleser nach Anspruch 22, ferner gekennzeichnet dadurch, daß der Speicher (88) eine Sperrschaltung umfaßt, um die Speicherung von Daten aus Kartenlesetransaktionen zu unterbinden, wenn die Autorisierung versagt wird.

24. Kartenleser nach Anspruch 20, ferner gekennzeichnet durch einen Speichermonitor zur Bestimmung, ob der Speicher (88) voll ist, und eine Sperrschaltung zur Verbinderung der Speicherung von Daten in dem Speicher, wenn der Speicher (88) voll ist.

25. Kartenleser nach Anspruch 24, ferner gekennzeichnet durch eine Autorisierungsschaltung (71) zur Autorisierung des Zugangs zu einer kontrollierten Stelle in Abhängigkeit von aus der Karte ausgelesenen Daten, wobei die Autorisierungsschaltung (71) eine Sperrschaltung umfaßt, um Daten aus der Kartenleseschaltung (74) zu ignorieren, wenn der Speicher (88) voll ist.

26. Kartenleser nach Anspruch 25, ferner gekennzeichnet durch eine Zeithalteschaltung (66) zur Bestimmung der Tageszeit, wobei der Speicher (88) die Tageszeit mit den Daten aus dem Kartenleser speichert, wenn die Karte gelesen wird.

27. Kartenleser nach Anspruch 25, ferner gekennzeichnet dadurch, daß die Autorisierungsschaltung (71) eine Signalschaltung zur Erzeugung eines ersten Signals umfaßt, wenn eine Autorisierung gewährt wird, sowie ein zweites Signal, wenn die Autorisierung versagt wird.

28. Kartenleser nach einem der Ansprüche 20 bis 27, ferner gekennzeichnet durch einen Sender zur Übertragung der durch die Speichereinrichtung gespeicherten Daten an die Zentralsteuerung (20), wenn die Nachrichtenverbindung wieder errichtet worden ist.

29. Kartenleser nach Anspruch 28, ferner gekennzeichnet dadurch, daß der Sender Daten für eine Kartenlesetransaktion von dem Speicher zu dem Zeitpunkt jeder Signalabfrage durch die Zentralsteuerung überträgt.

30. Kartenleser nach Anspruch 22, 25, 26 oder 27, dadurch gekennzeichnet, daß die Karte einen ersten Datenabschnitt und einen zweiten Datenabschnitt enthält, und daß die Autorisierungsschaltung (71) eine Schaltung zur Gewährung oder Versagung der Autorisierung auf der Grundlage nur des ersten Datenabschnitts umfaßt.

31. Kartenleser nach Anspruch 30, dadurch gekennzeichnet, daß der Speicher (88) nur den zweiten Datenabschnitt speichert.

32. Kartenleser nach Anspruch 31, dadurch gekennzeichnet, daß der Speicher (88) Einrichtungen zur Speicherung der Lokalzeit zu dem Zeitpunkt umfaßt, an dem der zweite Datenabschnitt gelesen wird.

33. Verfahren zum Betrieb eines Sicherheitssystems, das Zugang zu einer Stelle gewährt und einen lokalen Kartenleser (24) und eine Zentral-

steuerung (20) aufweist, welche miteinander in Nachrichtenverbindung stehen, um den Zugang auf der Grundlage von Datenkarten zu begrenzen, und zwar mit den folgenden Verfahrensschritten:

Speicherung von Kartendaten an dem lokalen Kartenleser (24) während Zeitspannen der Unfähigkeit zur Nachrichtenverbindung; und

Übertragen von gespeicherten Kartendaten von dem lokalen Kartenleser (24) an die Zentralsteuerung (20), wenn die Nachrichtenverbindung wieder aufgenommen ist, gekennzeichnet durch die folgenden Verfahrensschritte:

Periodisches Senden eines Abfragesignals aus der Zentralsteuerung (20) an dem Kartenleser (24); und Überwachung der Unfähigkeit zur Nachrichtenverbindung mit der Zentralsteuerung (20) an dem lokalen Kartenleser (24), und zwar durch die Abwesenheit des Abfragesignals aus der Zentralsteuerung (20) für eine vorbestimmte Zeitspanne.

34. Verfahren nach Anspruch 33, ferner gekennzeichnet durch den Verfahrensschritt, daß die Trageszeit mit den Kartendaten in dem lokalen Kartenleser (24) gespeichert wird.

35. Sicherheitssystem umfassend:

Eine Zentralsteuerung (20), welche die Tageszeit verfolgt;

einen Kartenleser (22, 24) entfernt von der Zentralsteuerung (20), welcher eine Leseschaltung (74) zum Auslesen von permanent auf einer Karte gespeicherten Daten umfaßt, einen Speicher (88), eine Autorisierungsschaltung (71) in dem Leser zur Autorisierung oder Verweigerung der Autorisierung unabhängig von der Zentralsteuerung (20) auf der Grundlage von Daten auf der Karte, und einen Monitor (90) zur Überwachung des Zustands einer außerhalb des Kartenlesers gelegenen Alarmvorrichtung und zur Erzeugung von Daten, welche eine Veränderung des Zustandes der Alarmvorrichtung anzeigen, und zwar zur Übertragung an die Zentralsteuerung (20); und

einen Sendeempfänger (26, 28) zur Übertragung der Daten aus dem Kartenleser (22, 24) an die Zentralsteuerung (20) und zum Empfang von Daten aus der Zentralsteuerung (20);

wobei das Sicherheitssystem dadurch gekennzeichnet ist, daß der Kartenleser ferner einen Zeitleser (40) zur Bestimmung der Tageszeit umfaßt, eine Schaltung (66), welche bewirkt, daß auf der Karte ausgelesene Daten und die Tageszeit in dem Speicher (88) an einem ersten Zeitpunkt gespeichert werden, und eine Sendeschaltung (70) zum Senden von von der Karte ausgelesenen Daten und den gespeicherten Tageszeitdaten aus dem Speicher (88) an die Zentralsteuerung (20) zu einem zweiten Zeitpunkt, der durch die Zentralsteuerung (20) gesteuert ist.

36. Sicherheitssystem umfassend:

Eine Zentralsteuerung (20);

einen Kartenleser (22, 24) entfernt von der Zentralsteuerung (20), wobei der Kartenleser einen Speicher (88) umfaßt, eine Kartenleseschaltung (74) zum Auslesen von auf Karten gespeicherten Daten, einen Empfänger (54) zum Emp-

fang von Daten aus der Zentralsteuerung, einen Speicher (80) zum Speichern von Daten aus dem Kartenleser in dem Speicher (80) während Zeiten, wenn die Nachrichtenverbindung mit der Zentralsteuerung verloren ist und einen Monitor (30) zur Überwachung des Zustandes einer Alarmvorrichtung, die außerhalb des Kartenlesers gelegen ist, sowie zur Erzeugung von Daten, welche eine Veränderung des Zustandes der Alarmvorrichtung anzeigen, und zwar zur Übertragung an die Zentralsteuerung (20); und

einen Sendeempfänger (26, 28) zur Übertragung der Daten aus dem Kartenleser (22, 24) an die Zentralsteuerung (20) und zum Empfang von Daten aus der Zentralsteuerung (20),

wobei das Sicherheitssystem dadurch gekennzeichnet ist, daß die Zentralsteuerung (20) periodisch den Kartenleser (24) abfragt und daß ein Fühler (84) mit dem Empfänger gekoppelt ist und feststellt, wenn die Nachrichtenverbindung mit der Zentralsteuerung (20) verloren ist, und zwar durch die Abwesenheit eines Abfragesignals aus der Zentralsteuerung (20) für eine vorbestimmte Zeitspanne, wobei der Speicher (80) auf den Fühler (84) anspricht.

Revendications

1. Lecteur (24) de cartes pour un système de sécurité comportant un dispositif central (20) de commande, lequel dispositif de commande converge l'heure du jour; ledit lecteur de cartes comprenant un circuit (74) de lecteur destiné à lire des données enregistrées de façon permanente sur une carte; une mémoire (88); et un circuit (71) d'autorisation dans ledit lecteur pour autoriser ou refuser une autorisation indépendamment du dispositif central de commande, sur la base des données sur ladite carte, ledit lecteur de carte étant caractérisé par:

un lecteur (40) de l'heure destiné à déterminer l'heure du jour;

un circuit (66) destiné à amener lesdites données lues sur ladite carte et ladite heure du jour à être enregistrées sur ladite mémoire (88) en un premier temps; et

un circuit (70) d'émission destiné à émettre lesdites données lues sur ladite carte et ladite donnée enregistrée de l'heure du jour de ladite mémoire (88) audit dispositif central (20) de commande en un second temps commandé par ledit dispositif (20) de commande.

2. Lecteur de cartes selon la revendication 1, caractérisé en ce que ledit circuit (70) d'émission provoque l'émission uniquement de données provenant d'une transaction de lecture d'une carte de ladite mémoire (88) audit dispositif central (20) de commande à la suite d'un signal provenant dudit dispositif central de commande.

3. Lecteur de cartes selon la revendication 1, caractérisé en ce que ledit lecteur de temps comprend un circuit (66) de synchronisation destiné à synchroniser l'heure locale au lecteur avec l'heure audit dispositif central de commande.

4. Lecteur de cartes selon la revendication 3,

caractérisé en ce que ledit lecteur de l'heure comprend en outre un circuit de décalage (136) destiné à décaler l'heure locale conservée dans ledit lecteur de cartes par rapport à l'heure conservée par ledit dispositif central de commande.

5. Lecteur de cartes selon la revendication 1, caractérisé en ce que ladite carte contient au moins deux éléments de données et en ce qu'un circuit (66) d'accès dans ledit lecteur de carte est validé par l'un desdits éléments de données.

6. Lecteur de cartes selon la revendication 5, caractérisé en ce que ladite mémoire (88) enregistre l'autre desdits éléments de données.

7. Lecteur de cartes selon la revendication 1, caractérisé en outre par un circuit d'accès (66) destiné à commander l'accès physique à une zone et ledit circuit (71) d'autorisation pour communiquer avec ledit circuit d'accès (66) afin d'accorder ou de refuser l'accès à ladite zone sur la base des données sur ladite carte.

8. Lecteur de cartes selon la revendication 7, caractérisé en ce que ledit circuit d'accès (66) établit sélectivement l'accès à un emplacement contrôlé sur la base de l'un des éléments de données lu sur ladite carte.

9. Lecteur de cartes selon les revendications 5 ou 8, caractérisé en ce que ledit circuit d'accès (66) génère un premier signal si l'accès doit être établi et un second signal si l'accès doit être refusé.

10. Lecteur de cartes selon la revendication 9, caractérisé en outre par un circuit (71) d'invalidation destiné à invalider ledit circuit d'accès en réponse audit second signal.

11. Lecteur de cartes selon la revendication 1, caractérisé en ce que le circuit (66) comprend un circuit destiné à interdire la mémorisation de données à partir de transactions de lecture de carte lorsque l'autorisation est refusée.

12. Lecteur de cartes selon la revendication 1, caractérisé en ce que le circuit (66) comprend:

un circuit destiné à déterminer si la mémoire (88) est pleine; et

un circuit destiné à interdire l'enregistrement de données dans la mémoire (88) lorsque la mémoire (88) est pleine.

13. Procédé de mise en oeuvre d'un lecteur de carte dans un système de sécurité comportant un dispositif central (20) de commande et plusieurs lecteurs de cartes éloignés, comprenant l'étape qui consiste à enregistrer des données de cartes à partir de cartes dans une mémoire (88) située audit lecteur, ledit procédé étant caractérisé par les étapes qui consistent:

à lire des données de carte sur des cartes à une première cadence déterminée par la fréquence d'insertions de carte audit lecteur;

à produire un signal d'autorisation dans ledit lecteur de carte, indépendamment du dispositif central (20) de commande, en réponse à la lecture de données appropriées sur la carte; et

à transmettre lesdites données de carte de ladite mémoire (88) audit dispositif central (20)

de commande à une seconde cadence déterminée par ledit dispositif (20) de commande.

14. Procédé de mise en oeuvre d'un lecteur de cartes selon la revendication 13, caractérisé en outre par l'étape qui consiste à enregistrer l'heure du jour dans la mémoire (88) au lecteur de carte, et l'étape qui consiste à transmettre l'heure du jour correspondant aux données de carte transmises, de la mémoire au dispositif central de commande.

15. Procédé de mise en oeuvre d'un lecteur de cartes selon la revendication 14, caractérisé en outre par l'étape qui consiste à synchroniser l'heure locale conservée dans le lecteur de cartes avec l'heure au dispositif central de commande.

16. Procédé de mise en oeuvre d'un lecteur de cartes selon la revendication 15, caractérisé en outre par l'étape qui consiste à conserver l'heure locale décalée d'une quantité prédéterminée de l'heure au dispositif central de commande.

17. Utilisation d'un lecteur de cartes selon l'une quelconque des revendications 1 à 12 pour la fonction de contrôle de l'accès à une zone de sécurité.

18. Utilisation d'un lecteur de cartes selon la revendication 17, caractérisée en outre par la fonction supplémentaire consistant à identifier à qui a été accordé l'accès à la zone de sécurité.

19. Utilisation d'un lecteur de cartes selon la revendication 17 ou 18, caractérisée en outre par la fonction supplémentaire consistant à identifier l'heure à laquelle l'accès à la zone de sécurité a été accordé.

20. Lecteur (24) de cartes pour un système de sécurité comportant un dispositif central (20) de commande qui communique avec ledit lecteur de cartes, ledit lecteur de cartes comprenant:

une mémoire (88);

un circuit (74) de lecteur de cartes destiné à lire des données enregistrées sur des cartes;

un récepteur (54) destiné à recevoir des données provenant dudit dispositif central de commande;

une mémoire (80) destinée à enregistrer lesdites données provenant dudit lecteur de cartes dans ladite mémoire (80) durant des périodes au cours desquelles la communication avec ledit dispositif central de commande est perdue, caractérisé en ce que ledit dispositif central (20) de commande interroge périodiquement ledit lecteur (24) de cartes; et en ce que

un capteur (84) couplé audit récepteur détecte lorsque les communications avec ledit dispositif central (20) de commande sont perdues par l'absence d'un signal d'interrogation provenant dudit dispositif central (20) de commande pendant un temps prédéterminé, ladite mémoire (80) réagissant audit capteur (84).

21. Lecteur de cartes selon la revendication 20, caractérisé en outre par un circuit (66) de conservation de l'heure destiné à conserver l'heure locale audit lecteur (24) de carte et à la

synchroniser avec l'heure conservée par ledit dispositif central (20) de commande.

22. Lecteur de cartes selon la revendication 21, caractérisé en outre par un circuit (71) d'autorisation couplé audit circuit (74) de lecteur de cartes pour accorder ou refuser l'accès à un emplacement contrôlé sur la base de données lues sur ladite carte.

23. Lecteur de cartes selon la revendication 22, caractérisé en outre en ce que ladite mémoire (88) comprend un circuit d'interdiction destiné à interdire l'enregistrement de données à partir d'une transaction de lecture de carte lorsque l'autorisation est refusée.

24. Lecteur de cartes selon la revendication 20, caractérisé en outre par:

un moniteur de mémoire destiné à déterminer si ladite mémoire (88) est pleine; et

un circuit d'interdiction destiné à interdire l'enregistrement de données dans ladite mémoire lorsque ladite mémoire (88) est pleine.

25. Lecteur de cartes selon la revendication 24, caractérisé en outre par un circuit (71) d'autorisation destiné à autoriser l'accès à un emplacement contrôlé en réponse à des données lues sur ladite carte, ledit circuit (71) d'autorisation comprenant un circuit d'interdiction destiné à ignorer des données provenant dudit circuit (74) du lecteur de cartes lorsque ladite mémoire (88) est pleine.

26. Lecteur de cartes selon la revendication 25, caractérisé en outre par un circuit (66) de conservation de l'heure destiné à déterminer l'heure du jour, ladite mémoire (88) enregistrant l'heure du jour avec lesdites données provenant dudit lecteur de cartes lorsque ladite carte est lue.

27. Lecteur de carte selon la revendication 25, caractérisé en outre en ce que ledit circuit (71) d'autorisation comprend un circuit de génération de signaux destiné à générer un premier signal lorsqu'une autorisation est délivrée et un second signal lorsqu'une autorisation est refusée.

28. Lecteur de carte selon l'une quelconque des revendications 20 à 27, caractérisé en outre par un émetteur destiné à émettre les données enregistrées par lesdits moyens d'enregistrement, vers ledit dispositif central (20) de commande lorsqu'une communication est rétablie.

29. Lecteur de carte selon la revendication 28, caractérisé en outre en ce que ledit émetteur émet des données pour une transaction de lecture de carte à partir de ladite mémoire au temps de chaque interrogation de signal à partir dudit dispositif central de commande.

30. Lecteur de carte selon la revendication 22, 25, 26 ou 27, caractérisé en ce que ladite carte contient une première partie de données et une seconde partie de données, et en ce que ledit circuit (71) d'autorisation comprend un circuit destiné à accorder ou refuser une autorisation sur la base de ladite première partie de données seulement.

31. Lecteur de carte selon la revendication 30, caractérisé en ce que ladite mémoire (88) enregistre ladite seconde partie de données seulement.

32. Lecteur de carte selon la revendication 31,

caractérisé en ce que ladite mémoire (88) comprend des moyens destinés à enregistrer l'heure locale à l'instant où ladite seconde partie de données est lue.

5 33. Procédé de mise en oeuvre d'un système de sécurité qui contrôle l'accès à un emplacement et qui comprend un lecteur local (24) de cartes et un dispositif central (20) de commande qui communique pour limiter l'accès sur la base de données de cartes, comprenant les étapes qui consistent:

10 à enregistrer des données de carte audit lecteur local (24) de carte durant des périodes d'impossibilité à communiquer; et

15 à transmettre des données de carte enregistrées dudit lecteur local (24) de cartes audit dispositif central (20) de commande lorsqu'une communication est rétablie, caractérisé par les étapes qui consistent:

20 à envoyer périodiquement un signal d'interrogation dudit dispositif central (20) de commande audit lecteur (24) de cartes; et

25 à détecter audit lecteur (24) de cartes l'impossibilité de communiquer avec ledit dispositif central (20) de commande par l'absence dudit signal d'interrogation provenant dudit dispositif central (20) de commande pendant un temps prédéterminé.

30 34. Procédé selon la revendication 33, caractérisé en outre par l'étape qui consiste à enregistrer l'heure du jour avec lesdites données de carte audit lecteur local (24) de cartes.

35 35. Système de sécurité comprenant:

un dispositif central (20) de commande qui conserve l'heure du jour;

un lecteur (22, 24) de cartes à distance dudit dispositif central (20) de commande, ledit lecteur de carte comprenant un circuit (74) de lecteur destiné à lire des données enregistrées de façon permanente sur une carte, une mémoire (88), un circuit (71) d'autorisation dans ledit lecteur pour autoriser ou refuser une autorisation indépendamment du dispositif central (20) de commande, sur la base des données sur ladite carte, et un moniteur (90) destiné à contrôler l'état d'un dispositif d'alarme extérieur audit lecteur de cartes et à générer des données indiquant un changement d'état dudit dispositif d'alarme pour les transmettre audit dispositif central (20) de commande; et

50 un émetteur-récepteur (26, 28) destiné à émettre les données dudit lecteur (22, 24) de carte vers ledit dispositif central (20) de commande et à recevoir des données dudit dispositif central (20) de commande;

55 ledit système de sécurité étant caractérisé en ce que ledit lecteur de cartes comprend en outre un lecteur (40) de l'heure destiné à déterminer l'heure du jour;

un circuit (66) destiné à provoquer l'enregistrement dans ladite mémoire (88), à un premier temps, desdites données lues sur ladite carte et de ladite heure du jour; et

60 un circuit (70) d'envoi destiné à envoyer lesdites données lues sur ladite carte et lesdites données d'heure du jour enregistrées de ladite

mémoire (88) audit dispositif central (20) de commande en un second temps commandé par ledit dispositif central (20) de commande.

36. Système de sécurité comprenant:

un dispositif central (20) de commande;

un lecteur (22, 24) de cartes à distance dudit dispositif central (20) de commande, ledit lecteur de carte comprenant une mémoire (88), un circuit (74) de lecteur de carte destiné à lire des données enregistrées sur des cartes, un récepteur (54) destiné à recevoir des données dudit dispositif central (20) de commande, une mémoire (80) destinée à enregistrer lesdites données provenant dudit lecteur de cartes dans ladite mémoire (80) durant des périodes au cours desquelles la communication avec ledit dispositif central de commande est perdue, et un moniteur (30) destiné à contrôler l'état d'un dispositif d'alarme extérieur audit lecteur de carte et à générer des données

indiquant un changement d'état dudit dispositif d'alarme pour les transmettre audit dispositif central (20) de commande; et

un émetteur-récepteur (26, 28) destiné à émettre les données dudit lecteur (22, 24) de cartes audit dispositif central (20) de commande et à recevoir des données dudit dispositif central (20) de commande,

ledit système de sécurité étant caractérisé en ce que ledit dispositif central (20) de commande interroge périodiquement ledit lecteur (24) de carte et en ce qu'un capteur (84), couplé audit récepteur, détecte lorsque les communications avec ledit dispositif central (20) de commande sont perdues, par l'absence d'un signal d'interrogation provenant dudit dispositif central (20) de commande pendant un temps prédéterminé, ladite mémoire (80) réagissant audit capteur (84).

20

25

30

35

40

45

50

55

60

65

22

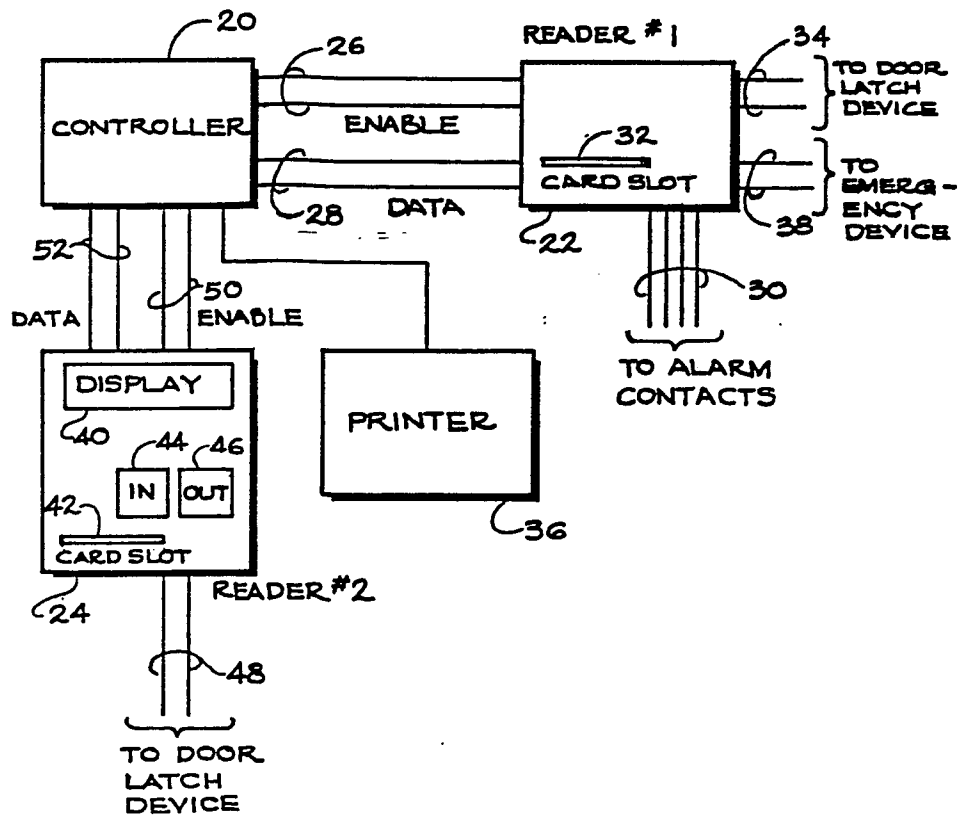


FIG.1

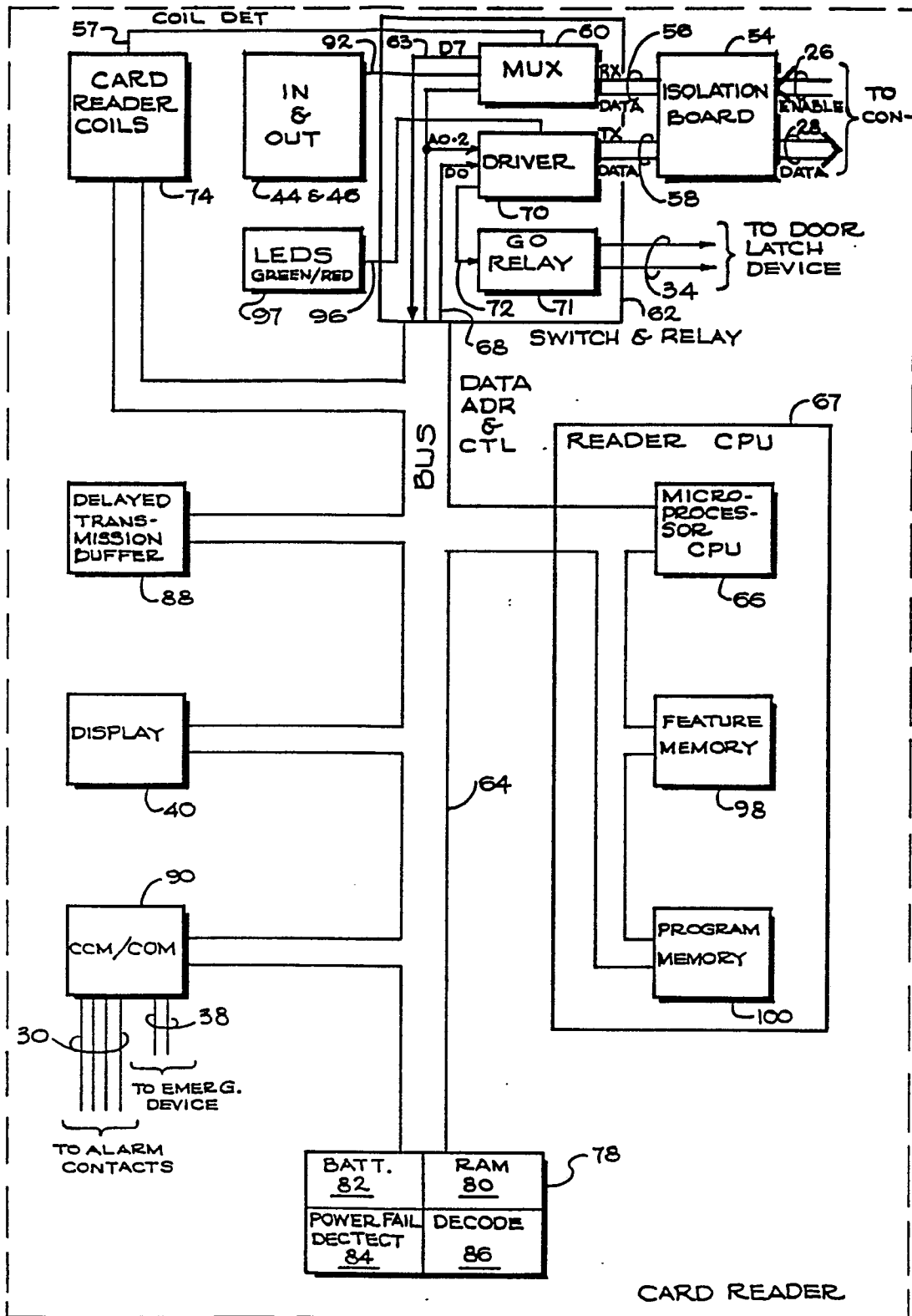


FIG. 2

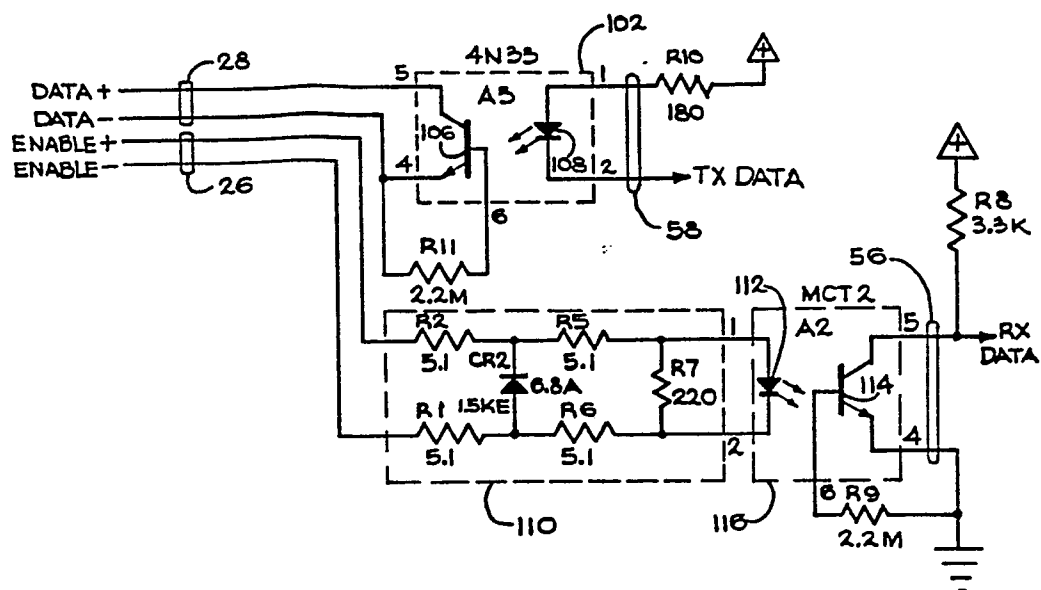


FIG. 3

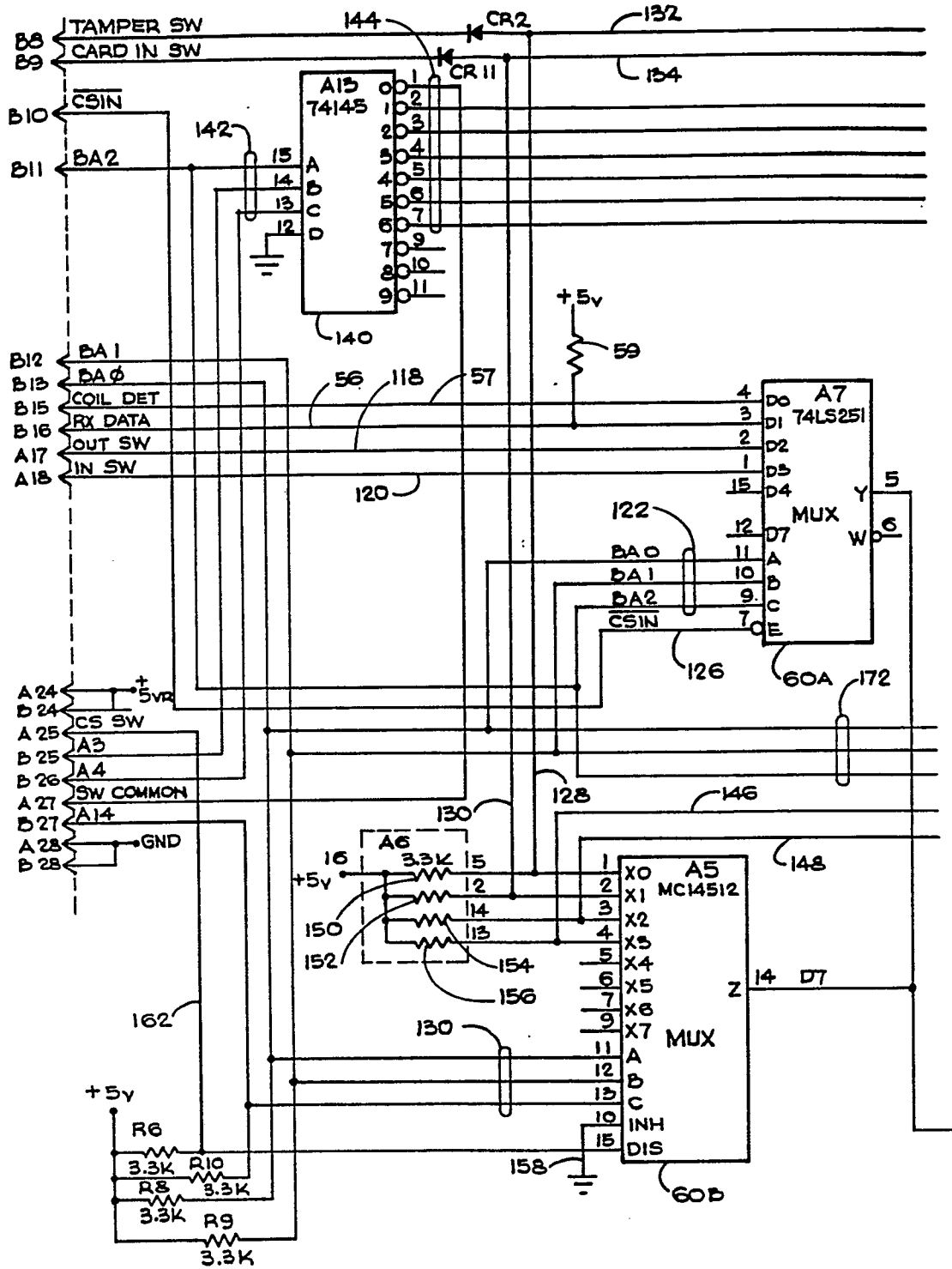


FIG. 4a

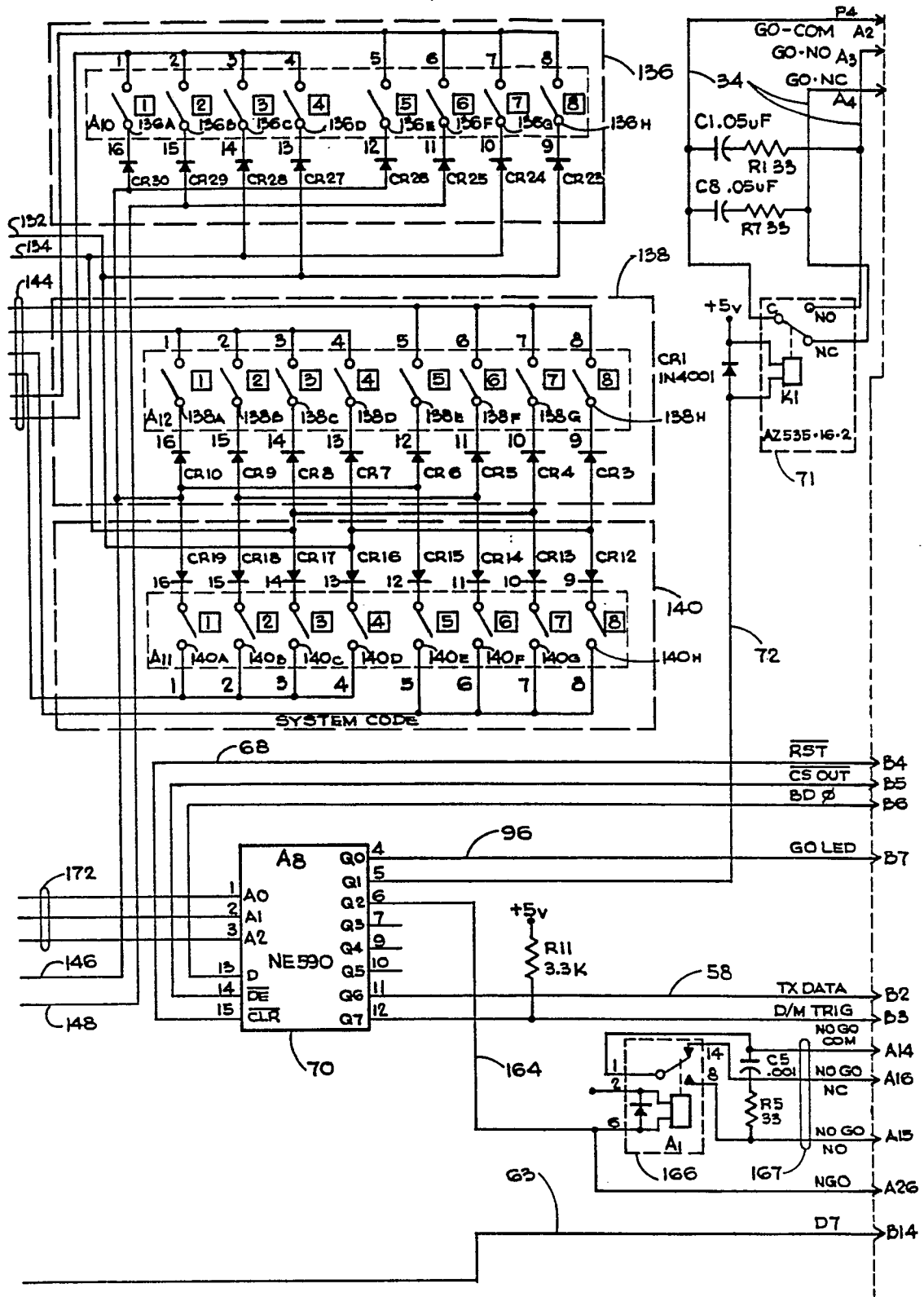


FIG. 4b

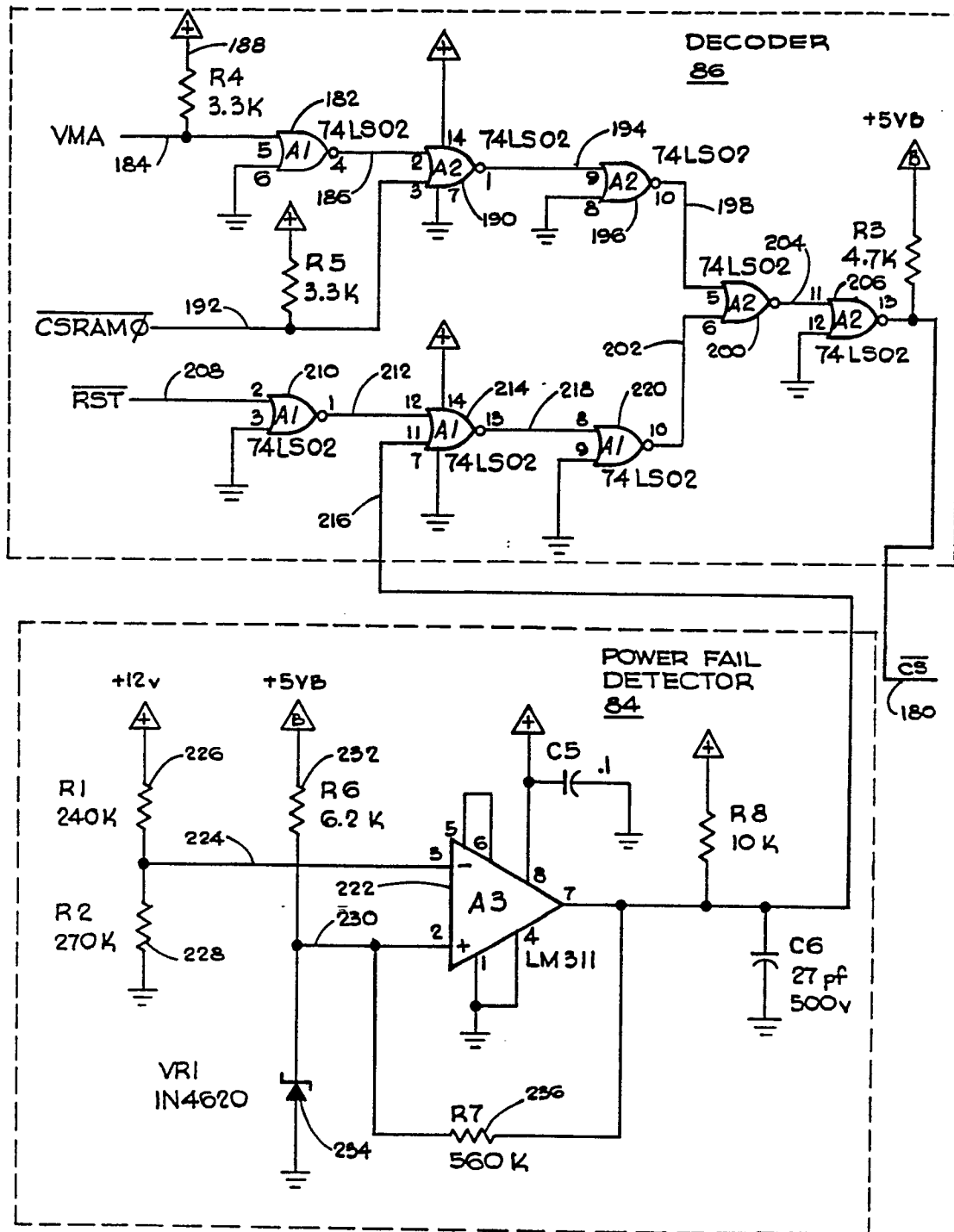


FIG. 5a

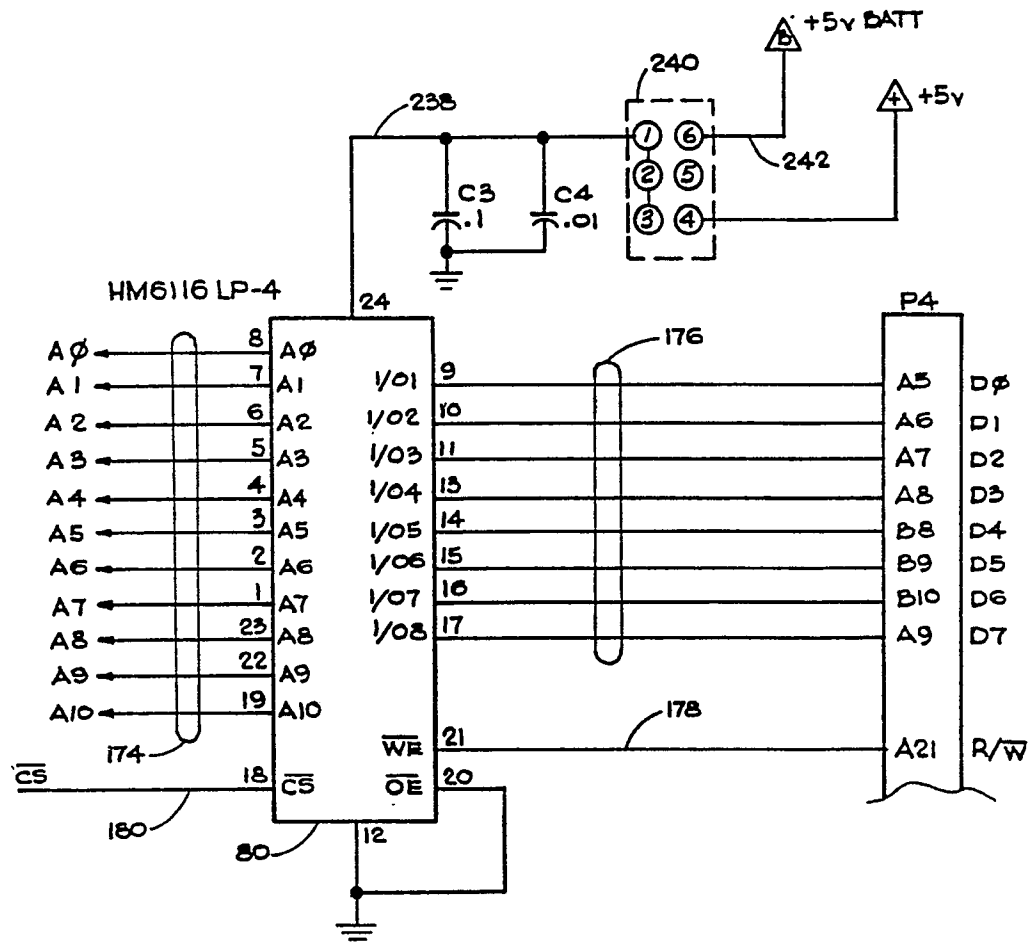


FIG. 5b

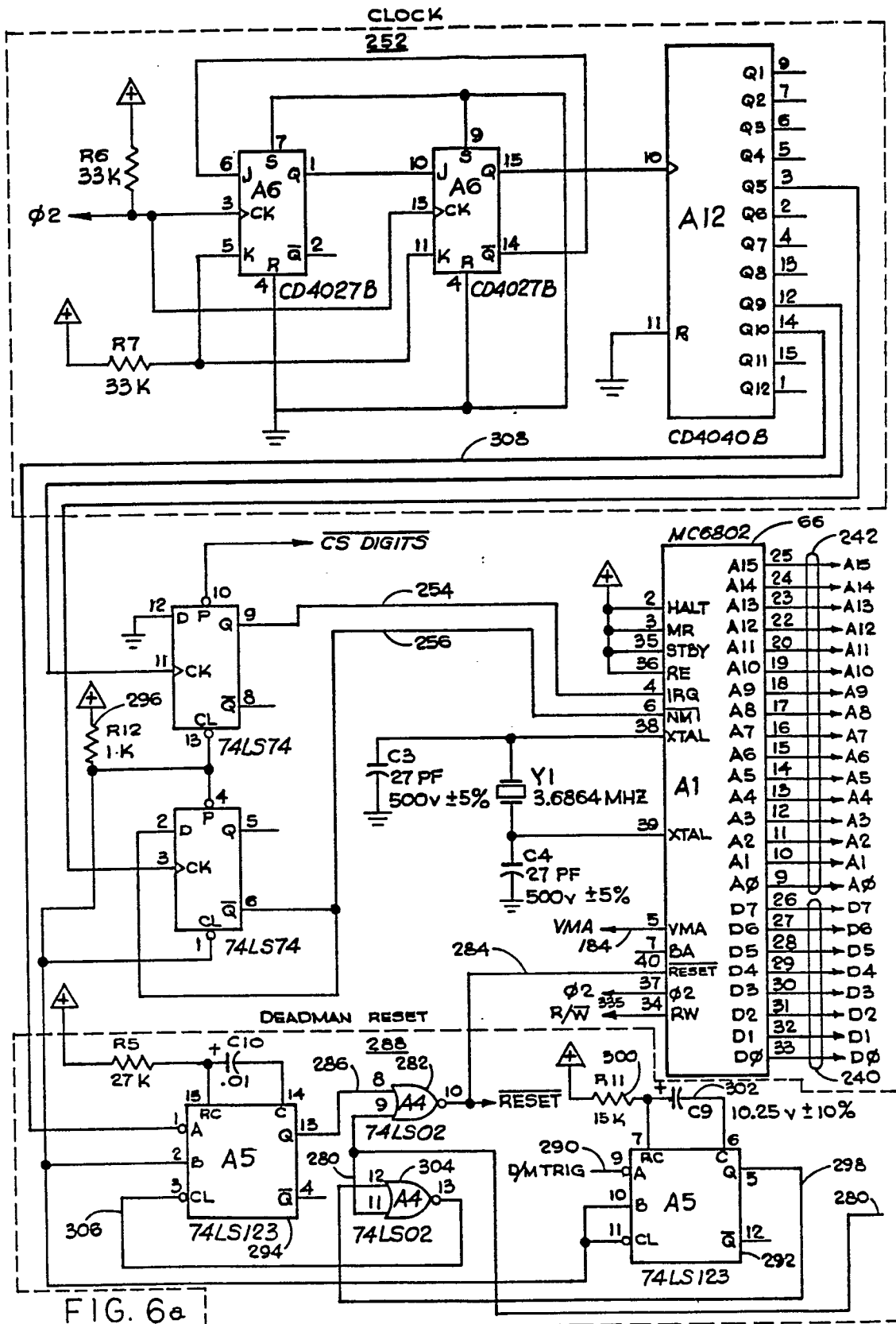


FIG. 6a

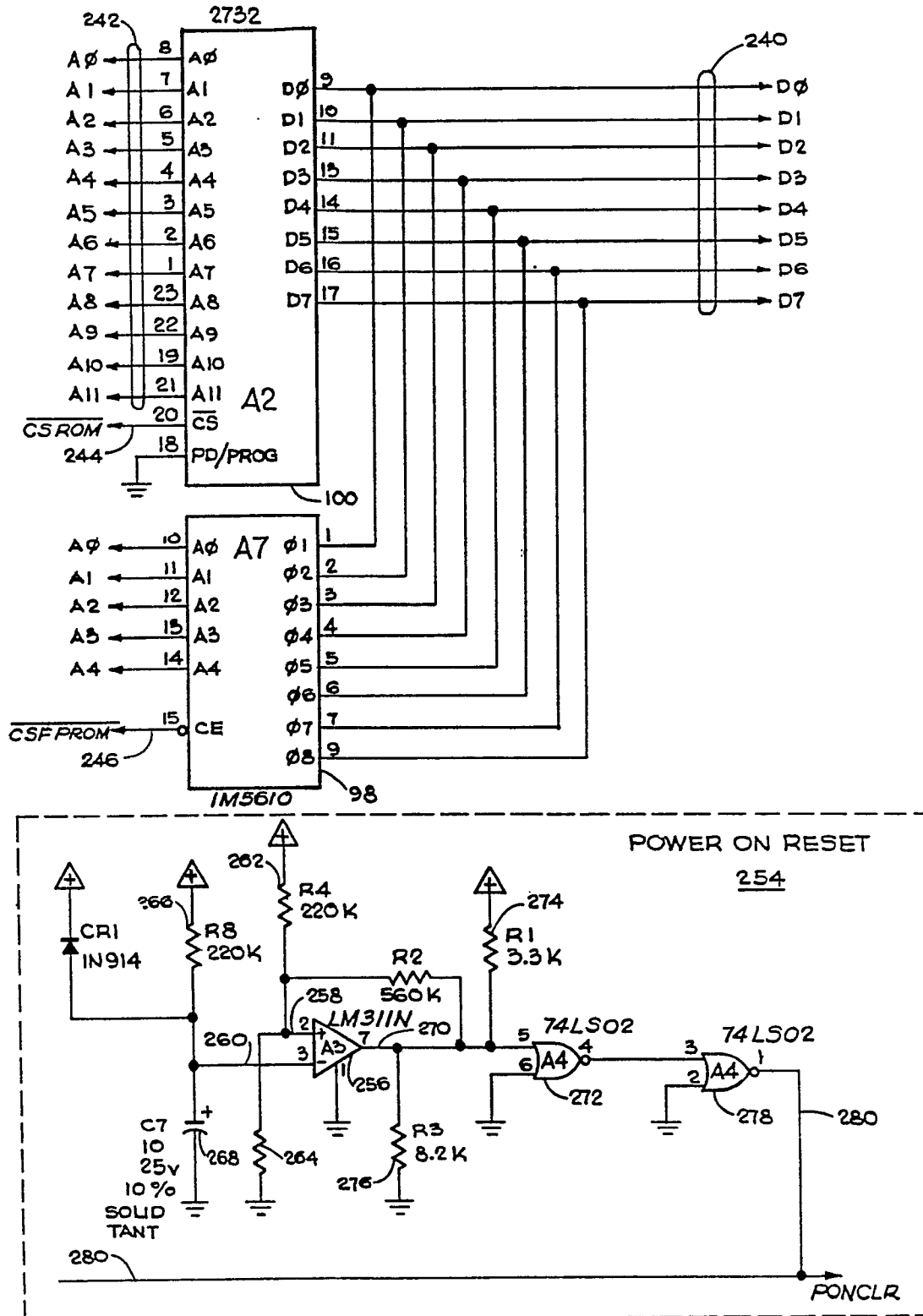


FIG. 6b

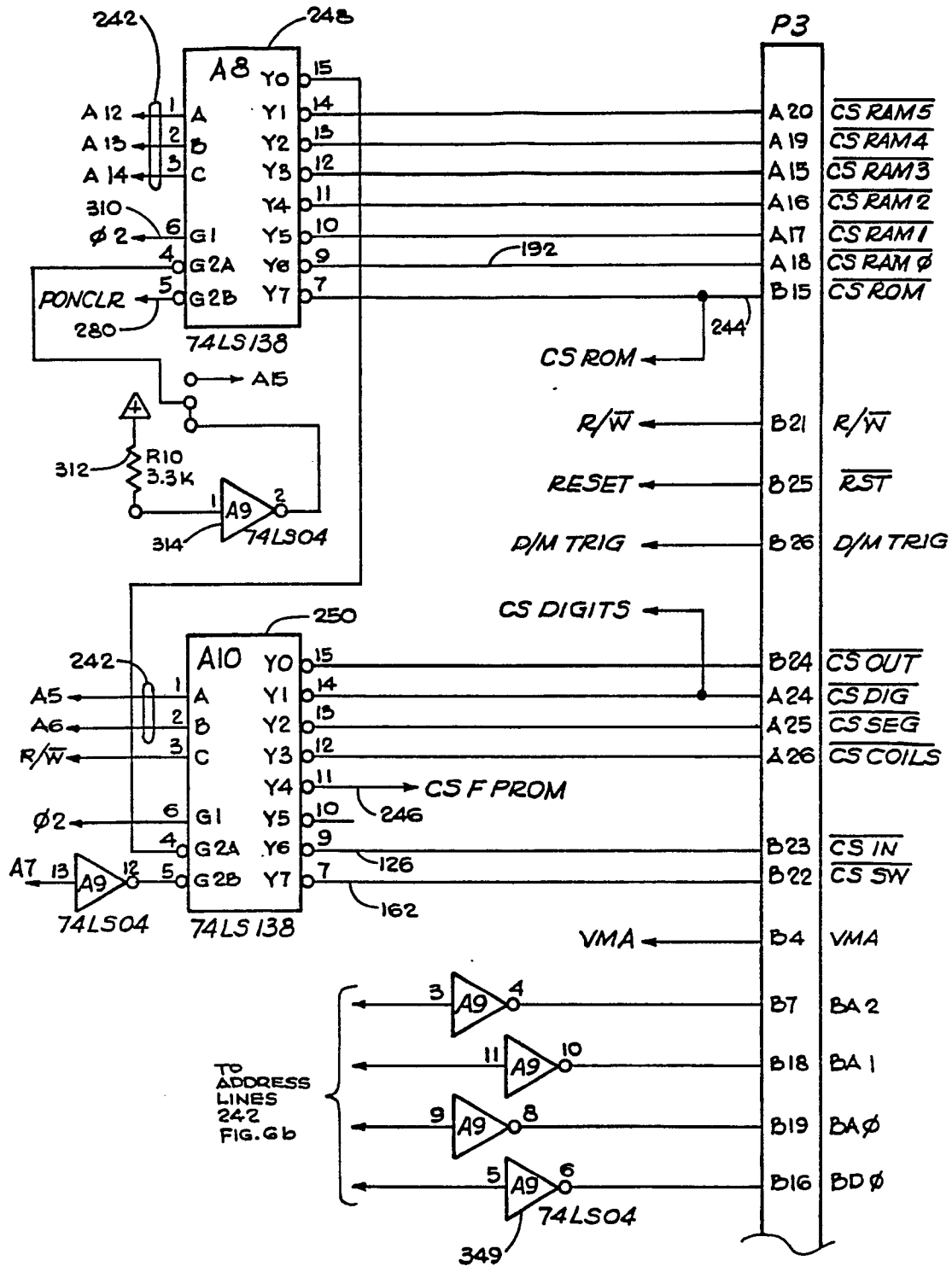


FIG. 6c

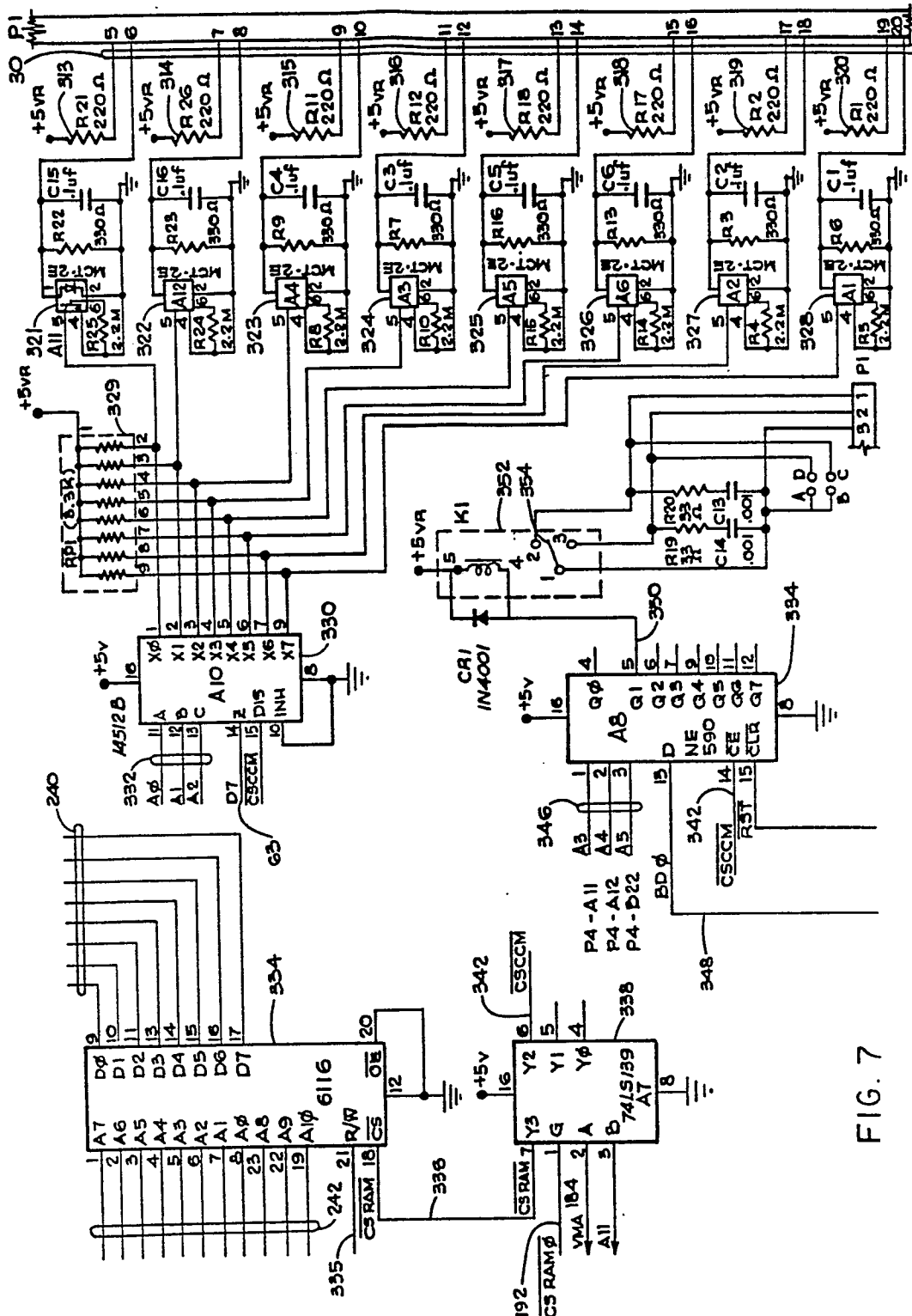


FIG. 7

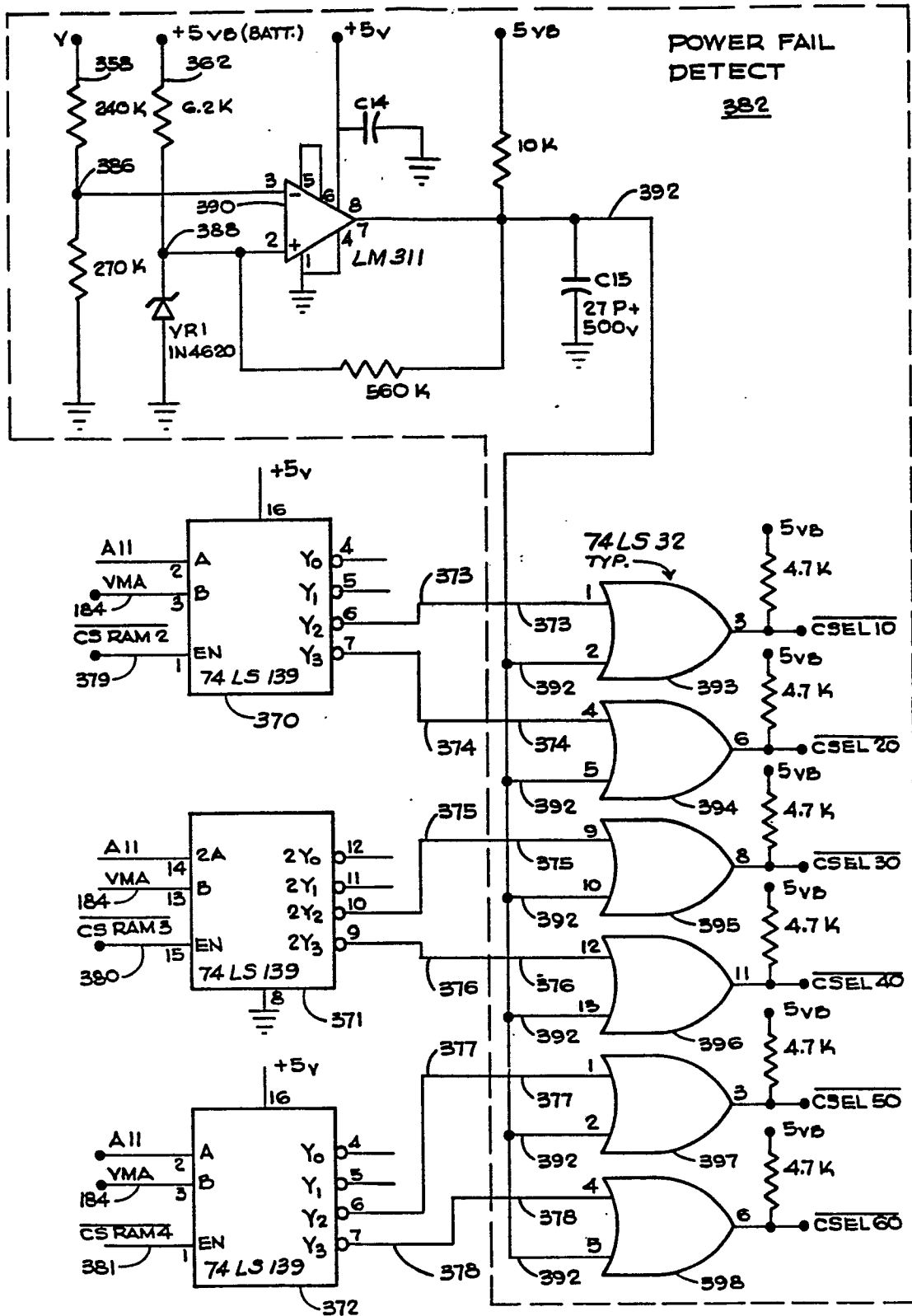


FIG. 8a

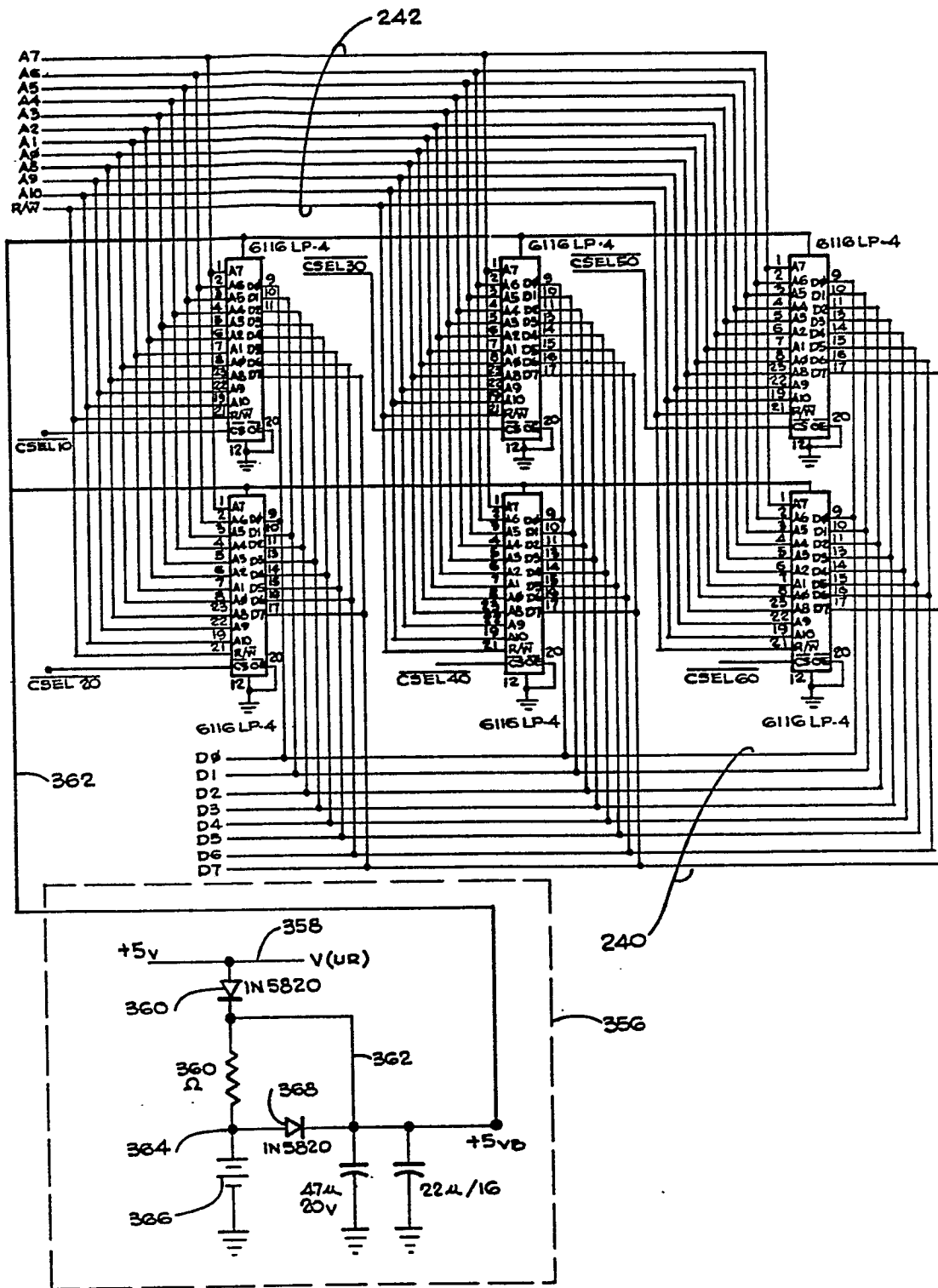


FIG. 8b

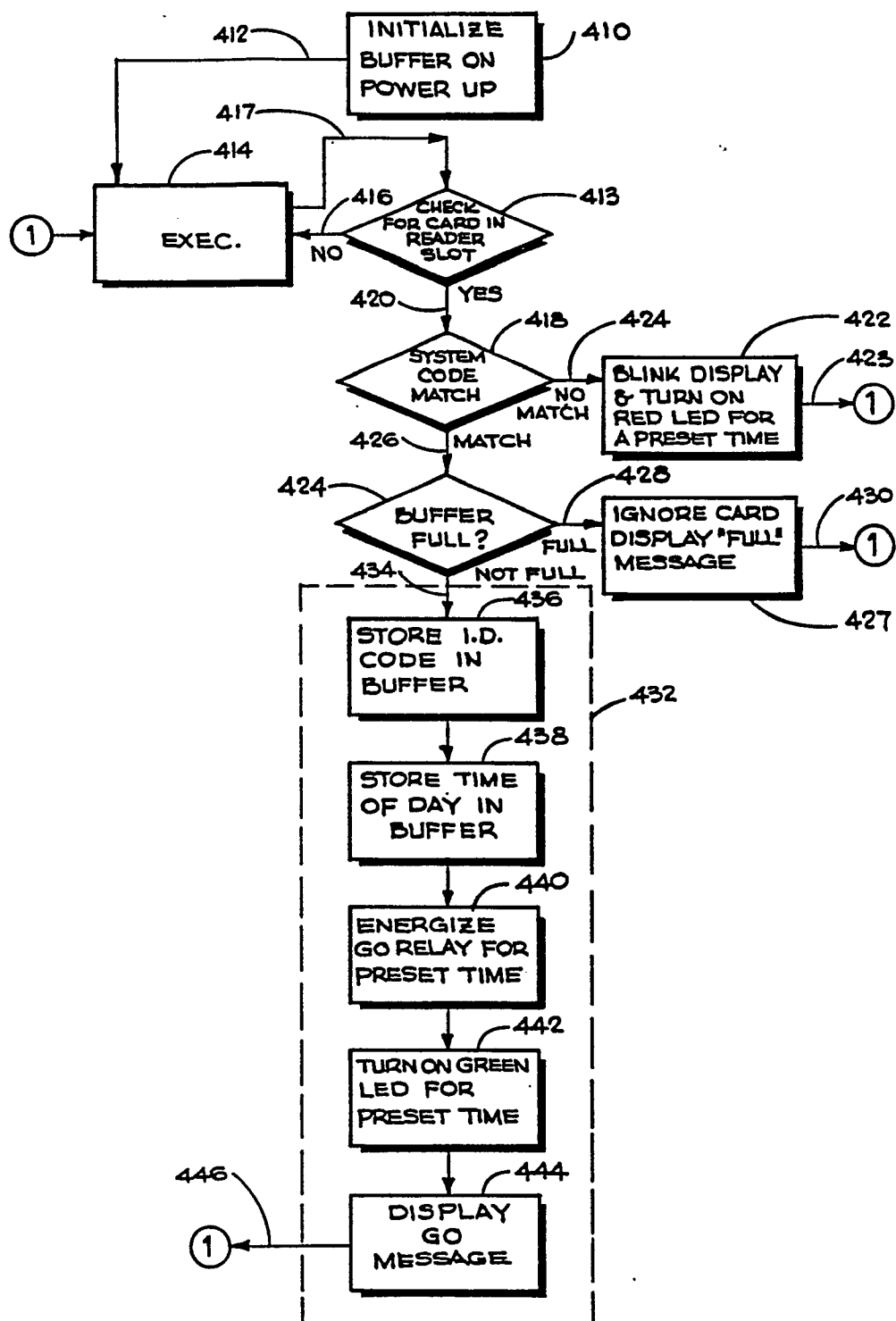


FIG. 9

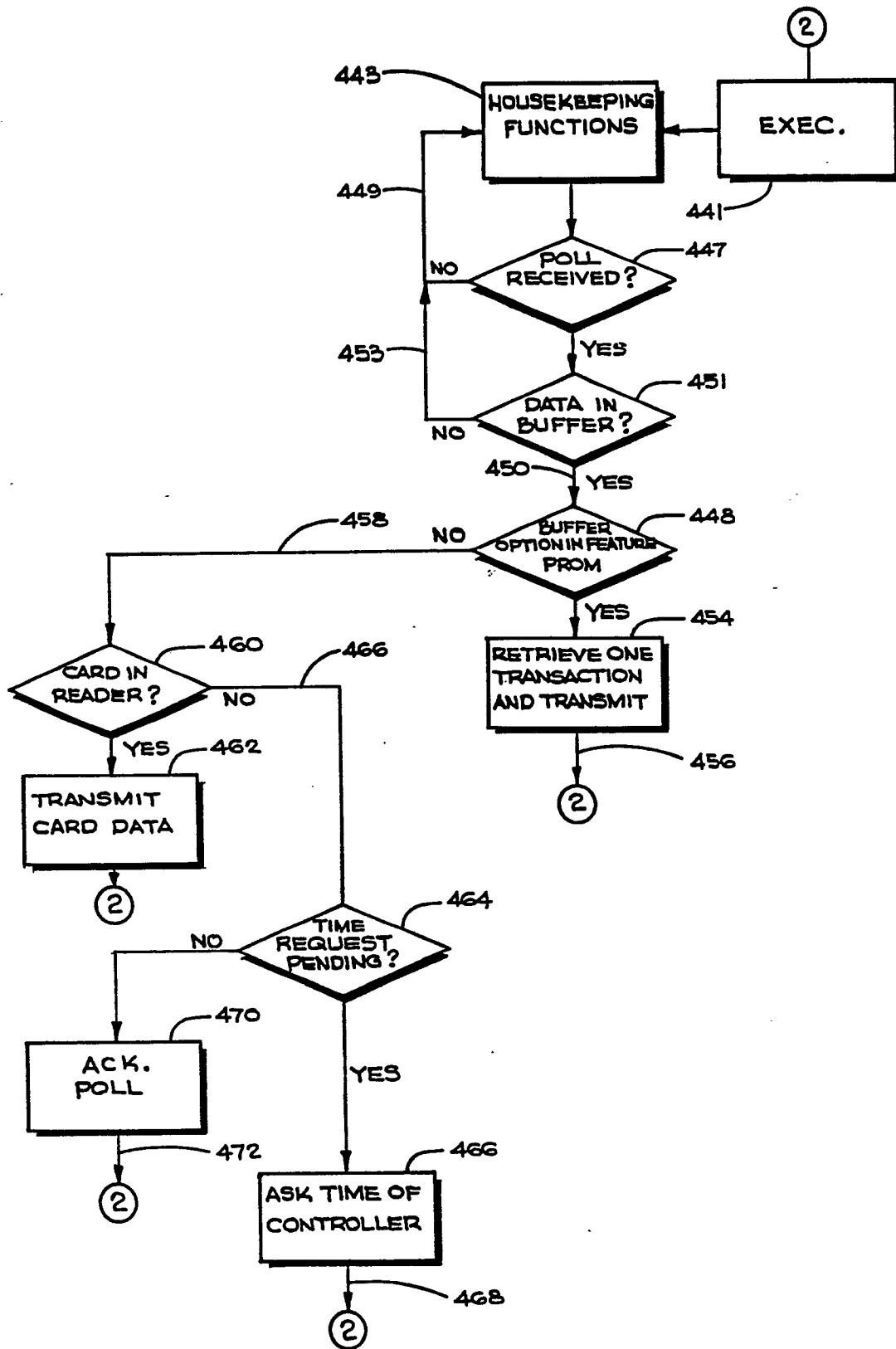


FIG. 10

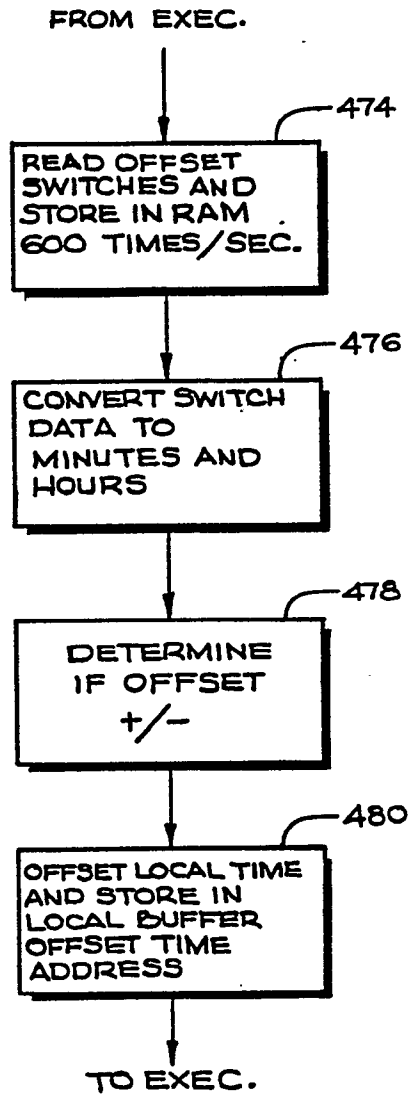


FIG. II

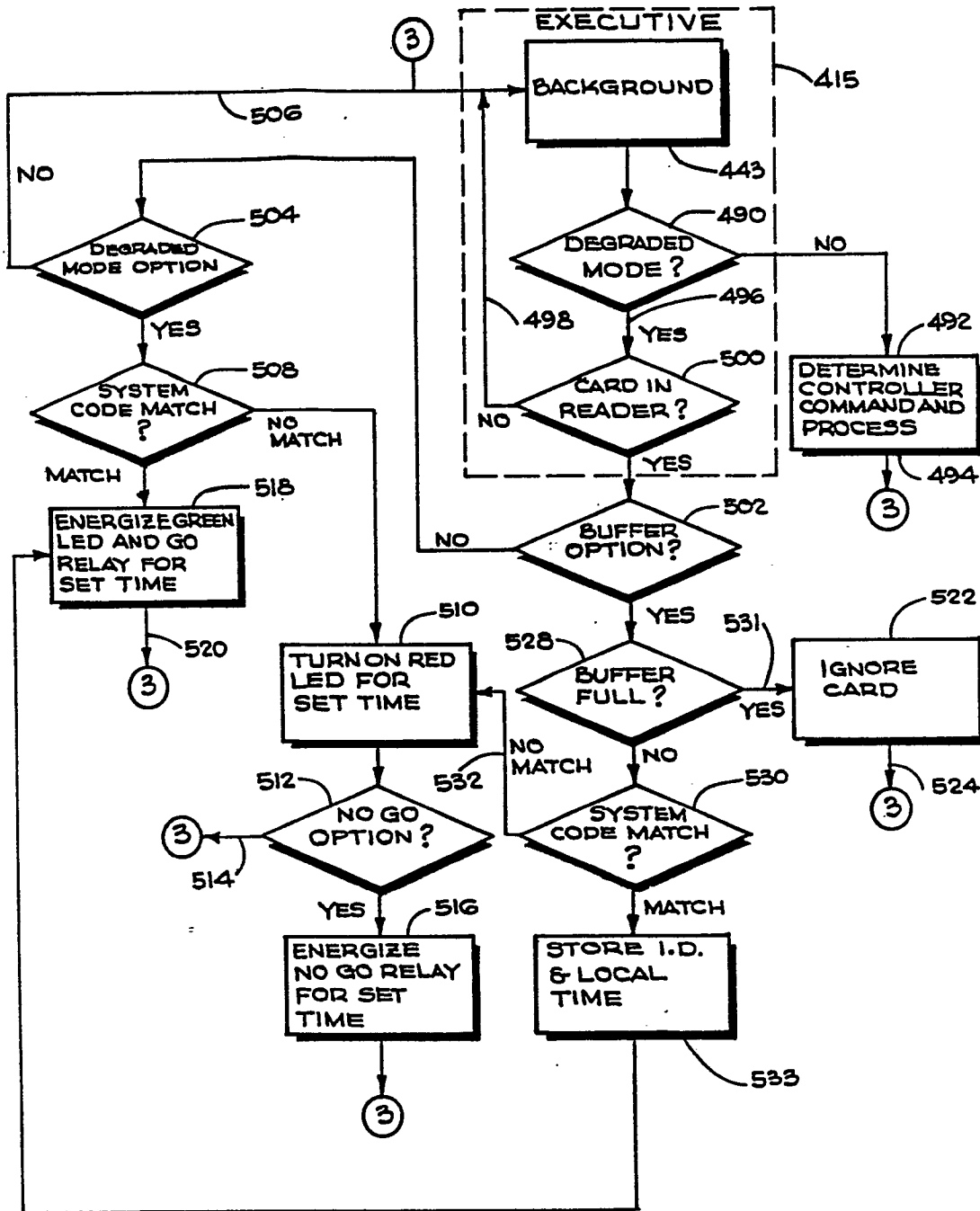


FIG. 12

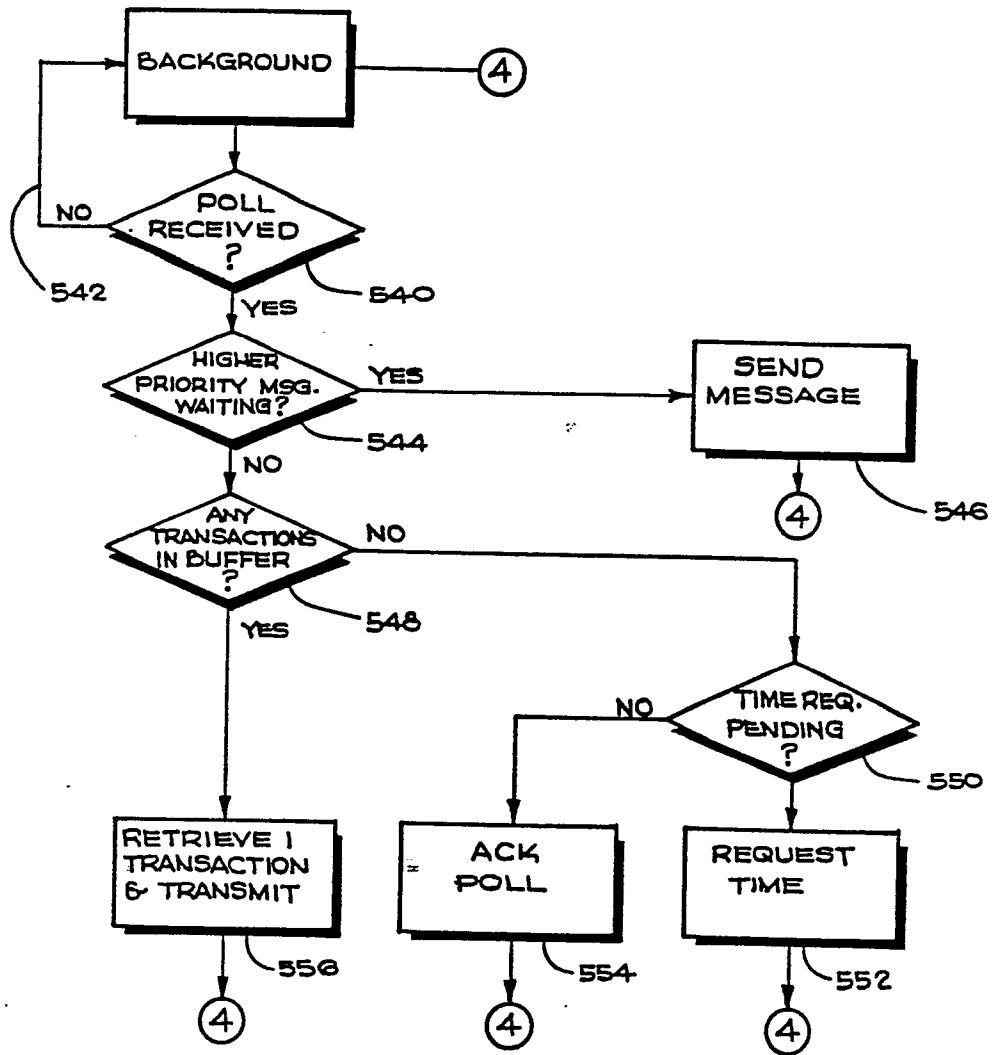


FIG. 13

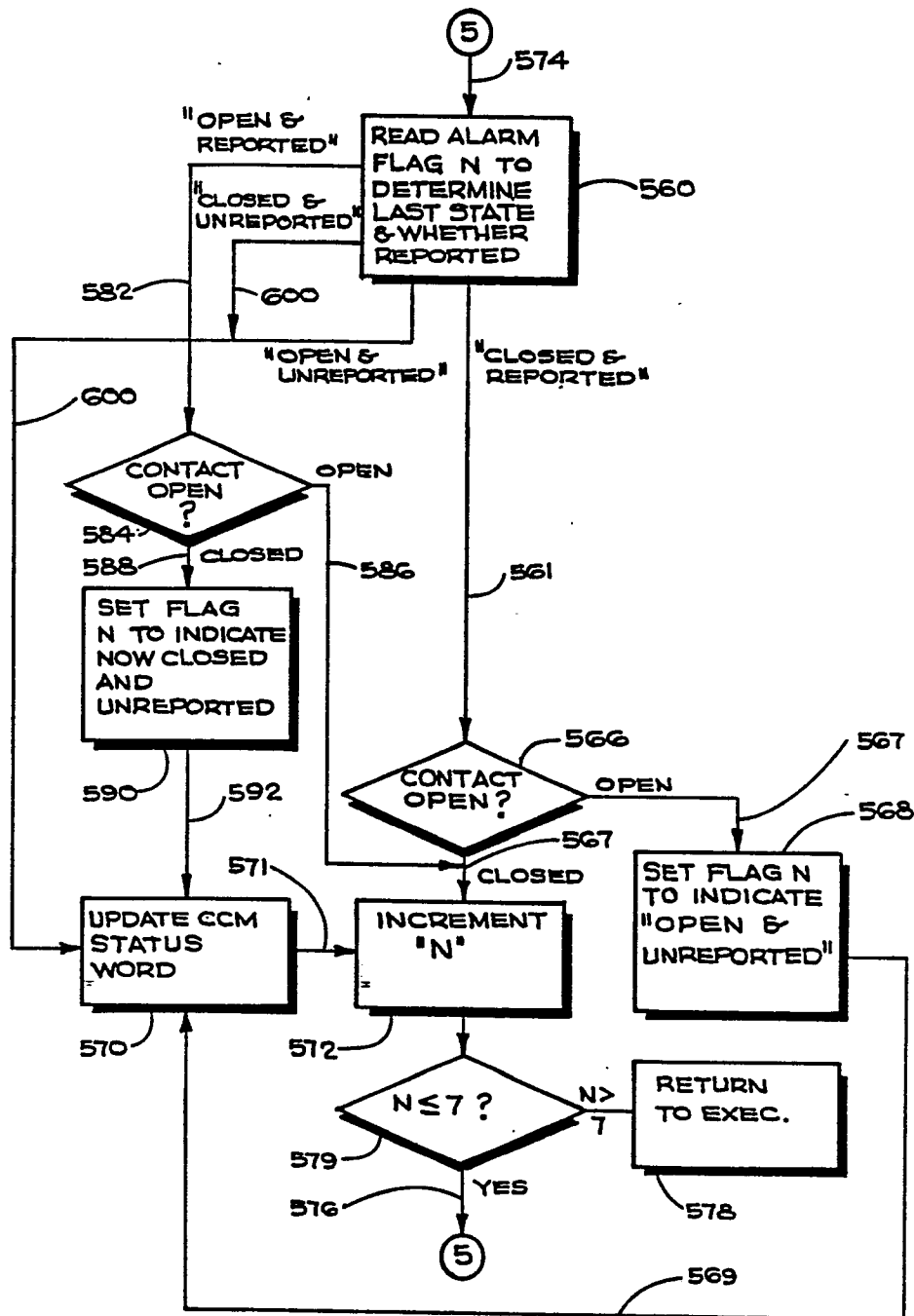


FIG. 14

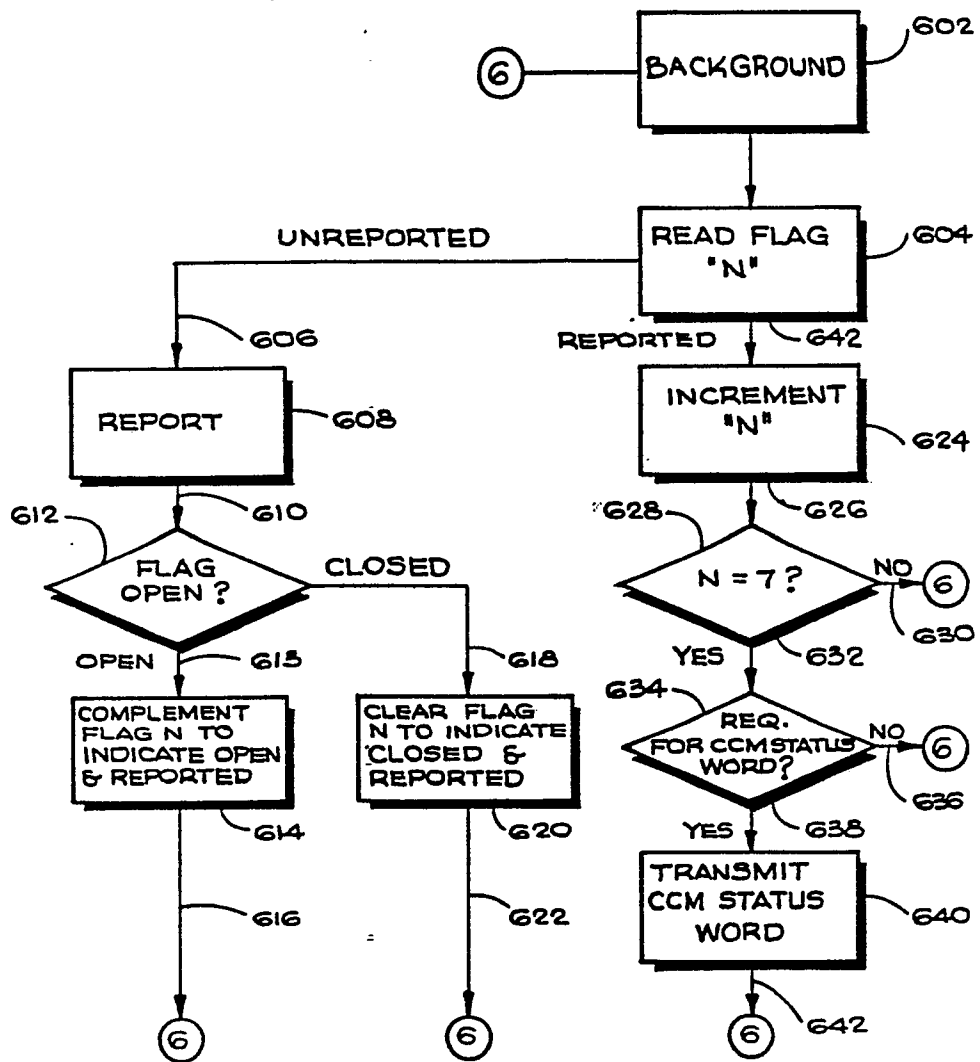


FIG. 15

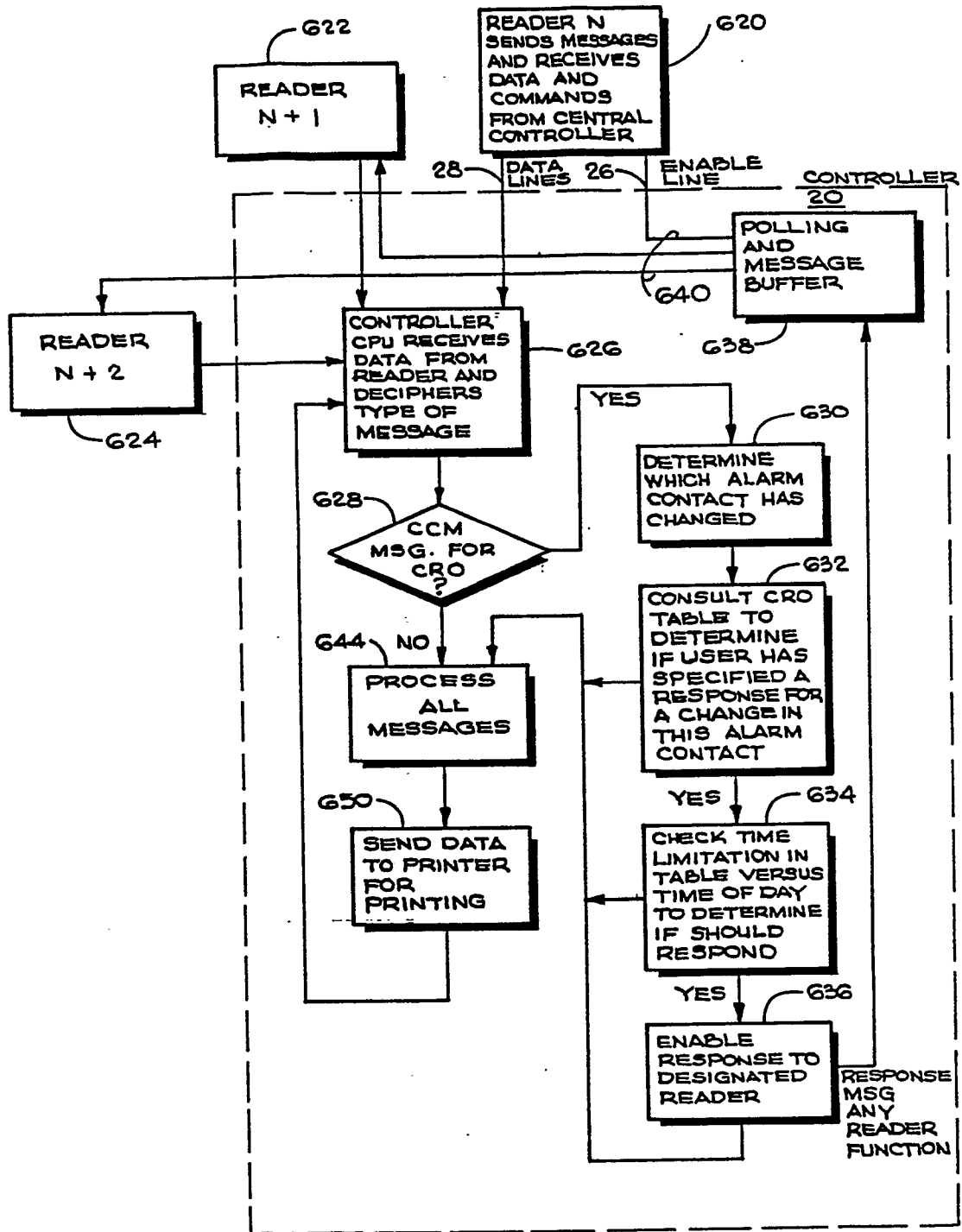


FIG. 16