United States Patent [19]

Dukes et al.

[11] **3,790,957**

[45] **Feb. 5, 1974**

[54] **KEY AUTOMATED DATA COLLECTION, CONTROL AND SOURCE INFORMATION SYSTEM**

[76] Inventors: **Lee R. Dukes,** 2828 Bammel Ln., Houston, 77006; **William W. Witt,** Richmond, both of Tex.

[22] Filed: **Nov. 24, 1972**

[21] Appl. No.: **309,469**

Related U.S. Application Data

[63] Continuation-in-part of Ser. No. 167,112, July 29, 1971, abandoned.

[52] **U.S. Cl.** ..... **340/149 R**

[51] **Int. Cl.** **G06k 7/06,** H04q 3/02

[58] **Field of Search** ..... 340/147 MD, 149 R, 149 A

[56] **References Cited**

UNITED STATES PATENTS

3,582,890	6/1971	Rivers	340/149 R
3,622,991	11/1971	Lehrer	340/147 R
3,639,906	1/1972	Tritsch	340/149 A
3,651,310	3/1972	Link	235/61.7 B
3,673,569	6/1972	Hedin et al.	340/147 R
3,688,269	8/1972	Miller	340/149 R
3,694,810	9/1972	Mullens et al.	340/149 R

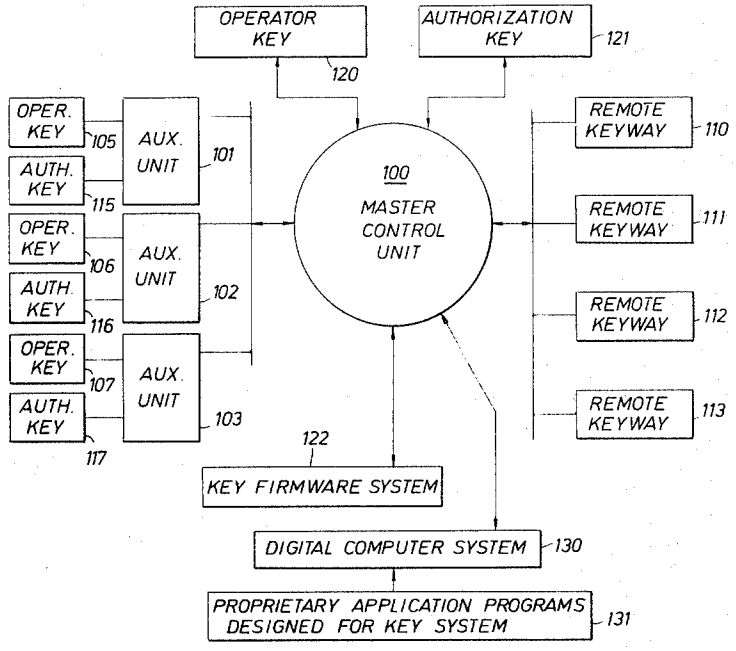
Primary Examiner—Donald J. Yusko

Attorney, Agent, or Firm—Torres and Berryhill

[57] **ABSTRACT**

Key automated data collection, control and source information system comprising a key operated locking device, a message encoding unit, and connected to a master control. The key operated device includes a conventional lock type receptacle for receiving a key, having a unique digital code associated therewith. A secondary security locking device may be engageable with the key to prevent removal from the lock's key receptacle. The message encoding unit senses the unique digital code and provides electrical signals representative thereof to a master control system. The master control system may be made responsive to the digital key code for recording and verification of the code, selective activation of the key operated device, and release of the key.

10 Claims, 9 Drawing Figures



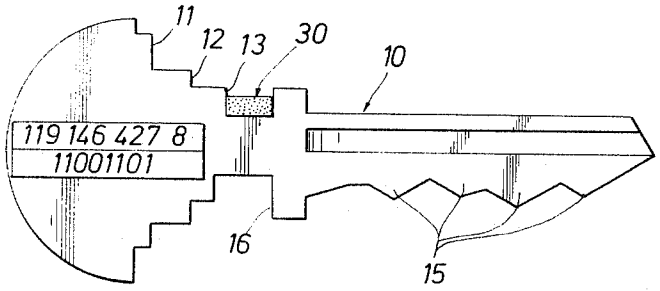


FIG. 1

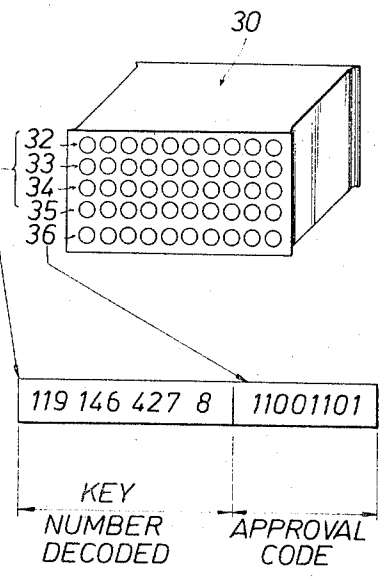
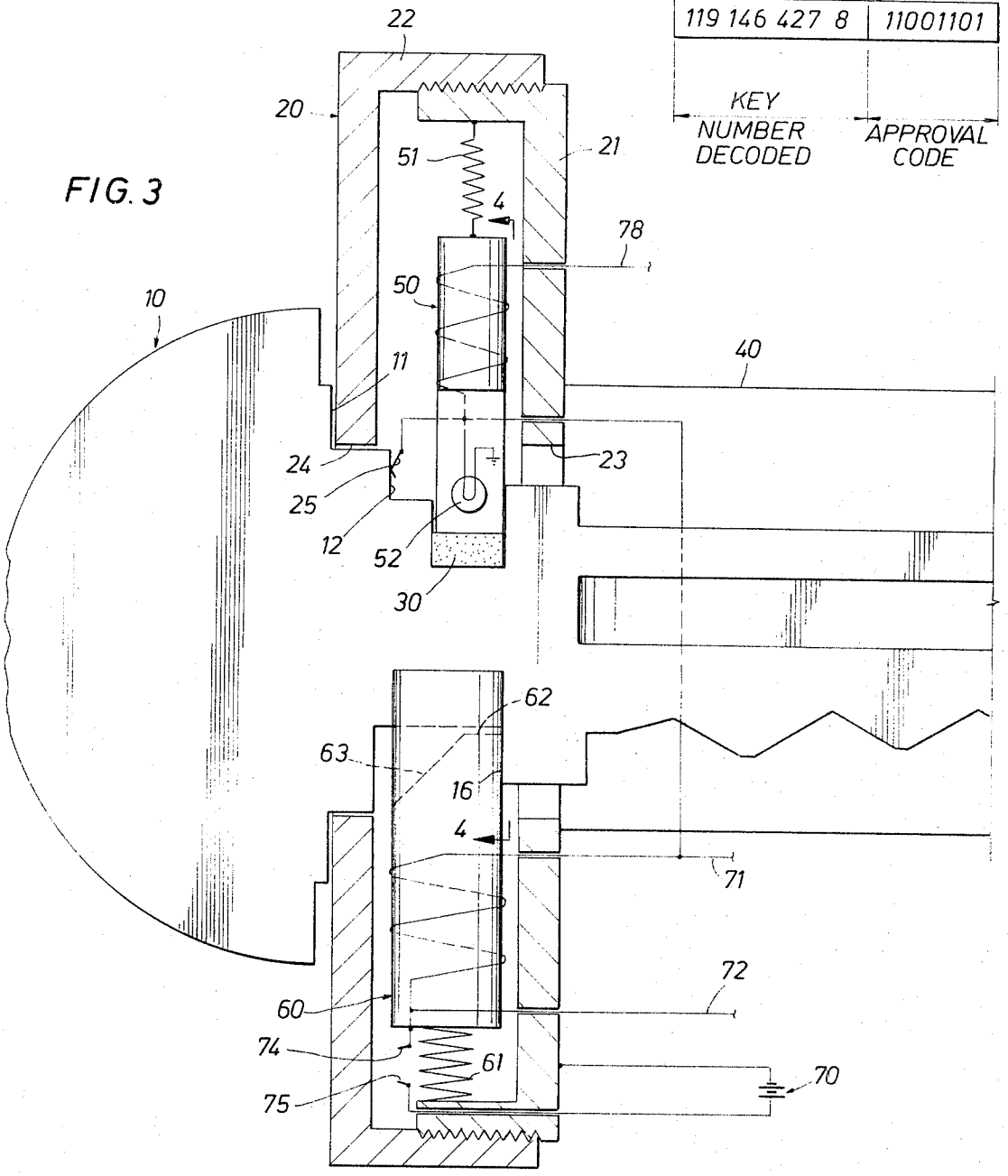


FIG. 2

FIG. 3



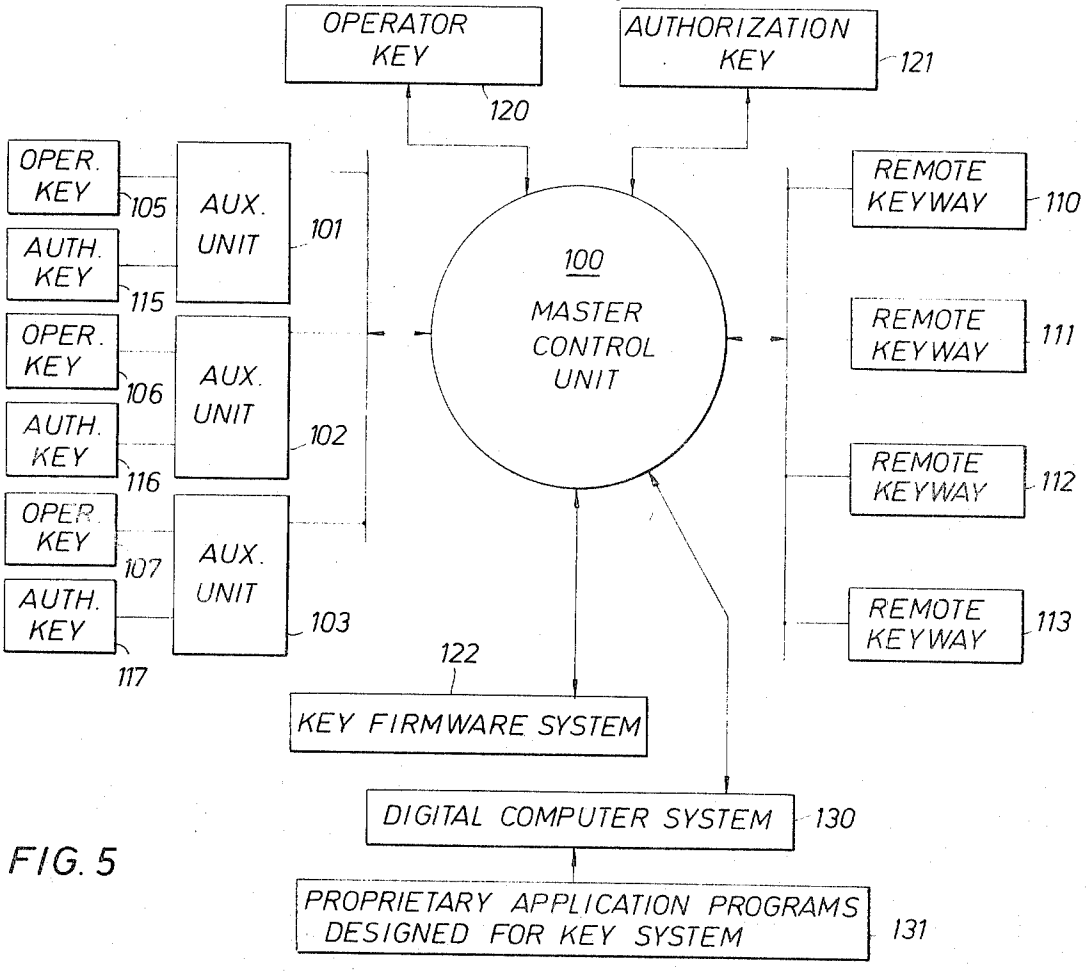

OPERATOR KEY
120
AUTHORIZATION KEY
121
OPER. KEY
105
AUTH. KEY
115
AUX. UNIT
101
OPER. KEY
106
AUTH. KEY
116
AUX. UNIT
102
OPER. KEY
107
AUTH. KEY
117
AUX. UNIT
103
100
MASTER CONTROL UNIT
REMOTE KEYWAY
110
REMOTE KEYWAY
111
REMOTE KEYWAY
112
REMOTE KEYWAY
113
122
KEY FIRMWARE SYSTEM
DIGITAL COMPUTER SYSTEM
130
PROPRIETARY APPLICATION PROGRAMS DESIGNED FOR KEY SYSTEM
131

FIG. 5

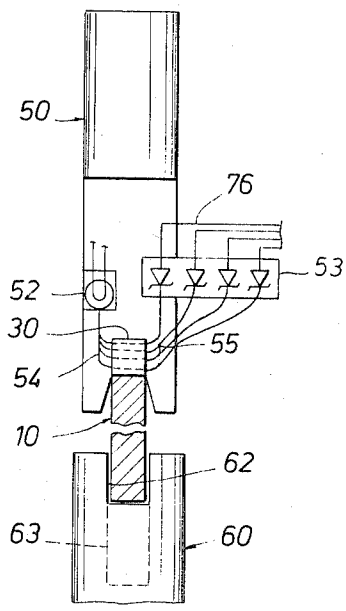

50
76
53
52
30
55
54
10
62
63
60

FIG. 4

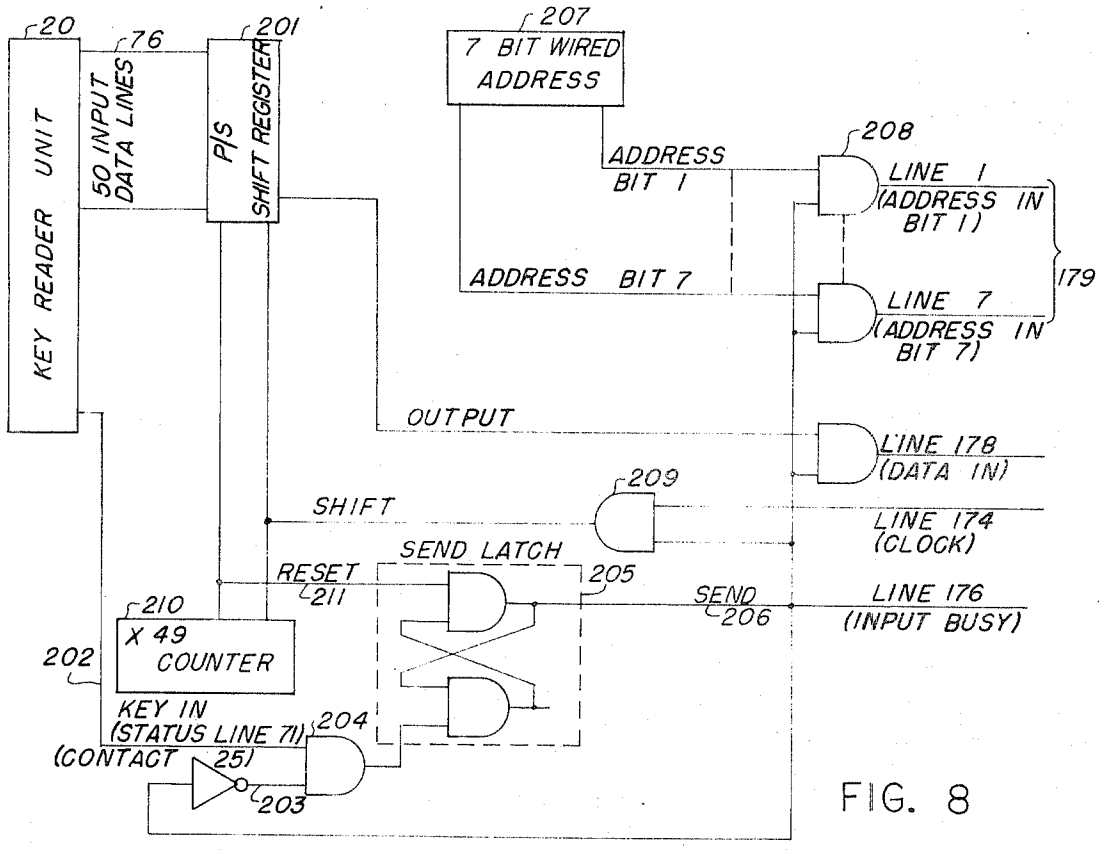

20
KEY READER UNIT
76
50 INPUT DATA LINES
201
P/S SHIFT REGISTER
207
7 BIT WIRED ADDRESS
ADDRESS BIT 1
ADDRESS BIT 7
208
LINE 1 (ADDRESS IN BIT 1)
LINE 7 (ADDRESS IN BIT 7)
179
OUTPUT
LINE 178 (DATA IN)
209
SHIFT
LINE 174 (CLOCK)
SEND LATCH
RESET
211
205
SEND
206
LINE 176 (INPUT BUSY)
210
X 49 COUNTER
202
KEY IN (STATUS LINE 71) (CONTACT 25)
204
203

FIG. 8

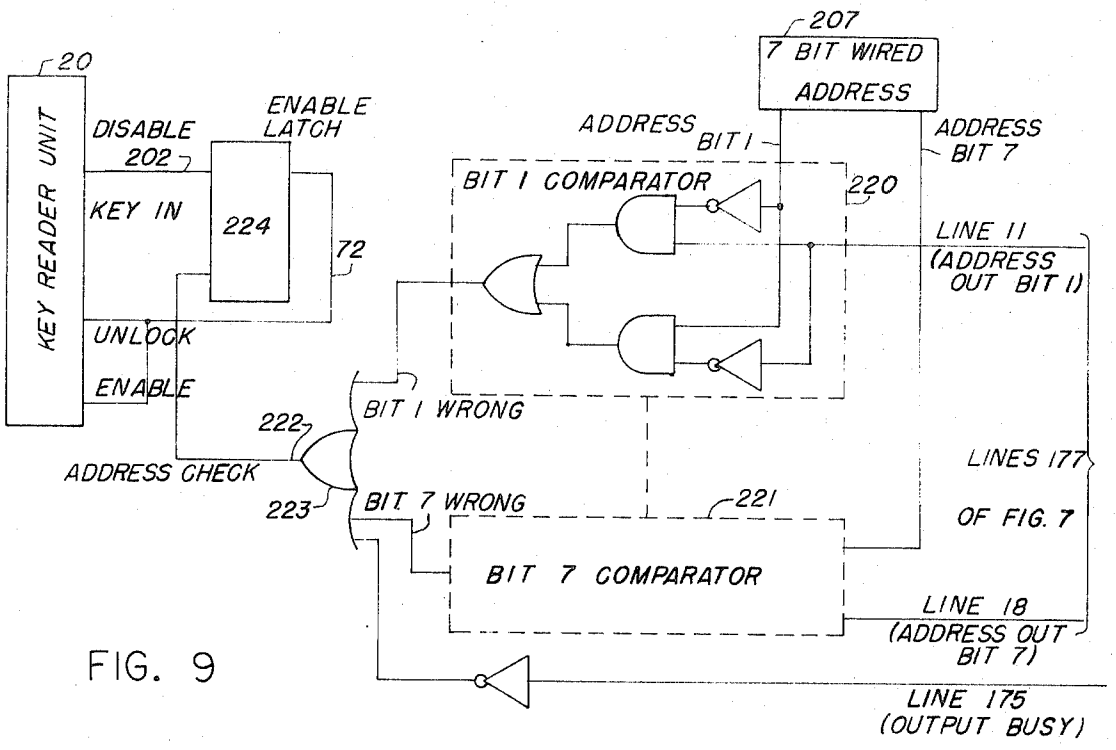

20
KEY READER UNIT
DISABLE
202
KEY IN
ENABLE
UNLOCK
ENABLE
ENABLE LATCH
224
72
207
7 BIT WIRED ADDRESS
ADDRESS BIT 1
ADDRESS BIT 7
BIT 1 COMPARATOR
220
LINE 11 (ADDRESS OUT BIT 1)
BIT 1 WRONG
222
ADDRESS CHECK
223
BIT 7 WRONG
221
BIT 7 COMPARATOR
LINES 177 OF FIG. 7
LINE 18 (ADDRESS OUT BIT 7)
LINE 175 (OUTPUT BUSY)

FIG. 9

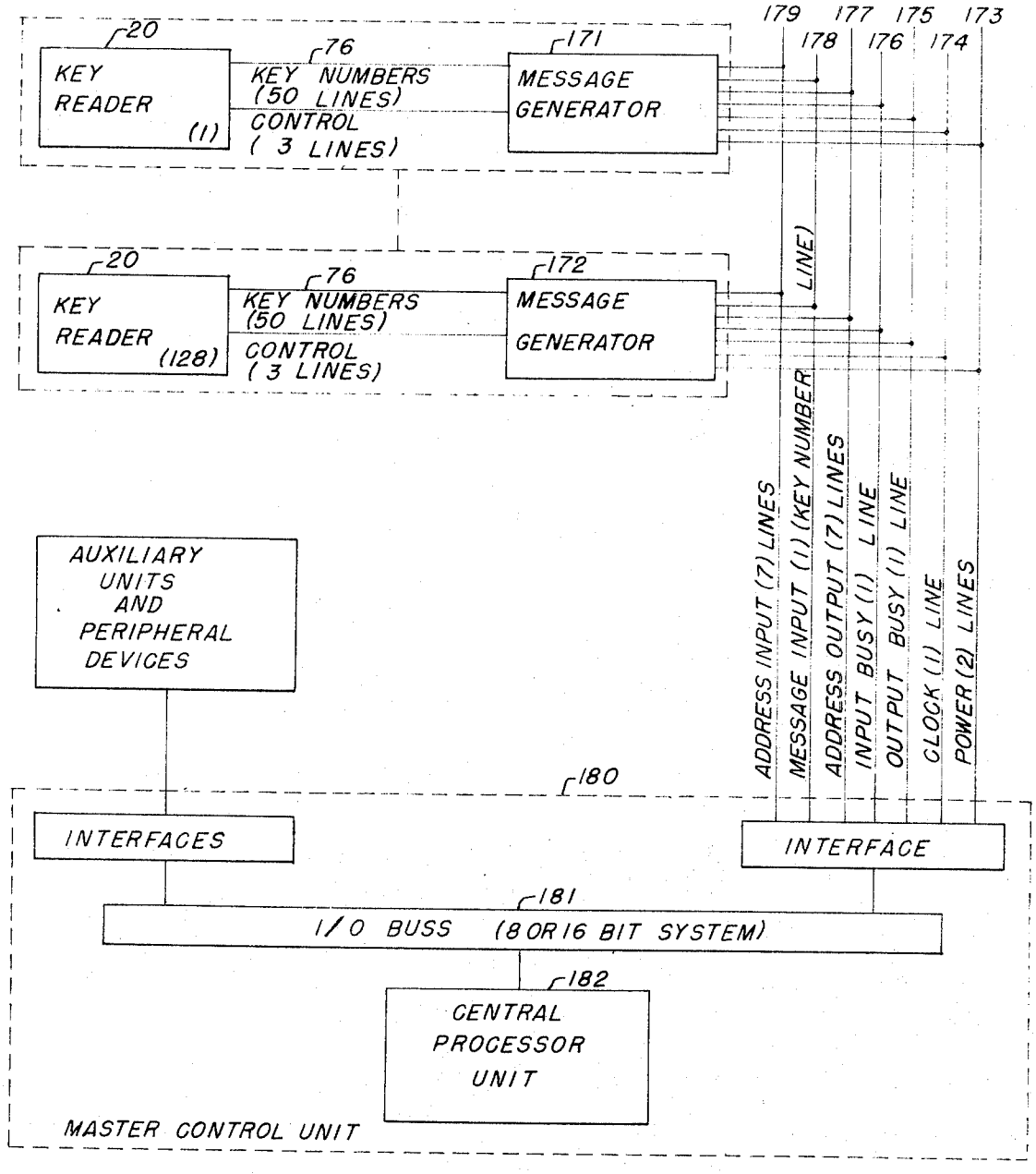

20
KEY READER (1)
76
KEY NUMBERS (50 LINES)
CONTROL (3 LINES)
171
MESSAGE GENERATOR
179
178
177
176
175
174
173
20
KEY READER (128)
76
KEY NUMBERS (50 LINES)
CONTROL (3 LINES)
172
MESSAGE GENERATOR
LINE)
ADDRESS INPUT (7) LINES
MESSAGE INPUT (1) (KEY NUMBER
ADDRESS OUTPUT (7) LINES
INPUT BUSY (1) LINE
OUTPUT BUSY (1) LINE
CLOCK (1) LINE
POWER (2) LINES
AUXILIARY UNITS AND PERIPHERAL DEVICES
180
INTERFACES
INTERFACE
181
I/O BUSS (8 OR 16 BIT SYSTEM)
182
CENTRAL PROCESSOR UNIT
MASTER CONTROL UNIT

FIG. 7

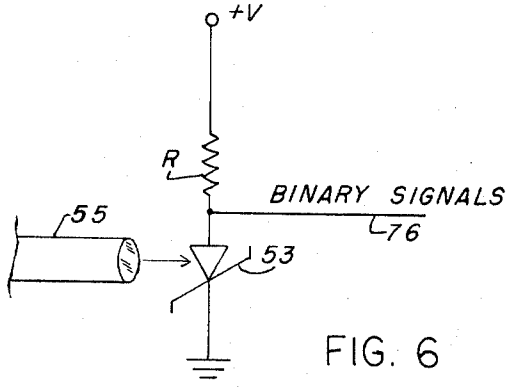

+V
R
BINARY SIGNALS
76
55
53

FIG. 6

KEY AUTOMATED DATA COLLECTION, CONTROL AND SOURCE INFORMATION SYSTEM

CROSS REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of application Ser. No. 167,112 filed July 29, 1971 which is now abandoned.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to automated data collection, control and source information systems. In particular, it concerns such systems requiring actuation by certain authorization devices such as cards, keys and the like. It also relates to a specific type of key authorization device.

2. Description of the Prior Art

In the past, various systems have been devised to selectively permit access to and operation of certain devices. Of course, the ordinary key is an example of such. However, when it is desired to permit access by a large number of people, ordinary keys become impractical. If a large number of keys are issued, some are frequently lost, stolen or duplicated, resulting in a breakdown of the system. In recent years, special keys have been designed to cooperate with various electrical circuits to permit access or operation of associated devices by a number of people. Such keys and related systems attempt to provide tamperproof methods of operation. In addition, many of the systems provide additional functions such as recording data to indicate the operator of the device and the time at which such device is operated. Examples of such keys and related systems may be seen in the following U. S. patents:

U.S. Pat. No. 2,905,926—Aid
U.S. Pat. No. 3,093,994—Richard
U.S. Pat. No. 3,438,051—Devines
U.S. Pat. No. 3,415,087—Kramasz, Jr., et al
U.S. Pat. No. 3,444,711—Sedley
U.S. Pat. No. RE 27,013—Hedin, et al

Although many of these devices work satisfactorily, some of them are extremely complex, have little flexibility and are directed to specific narrow applications. Most of them also require a specially made key incapable of any other unlocking functions.

In another, though not completely unrelated area, that of data collection, control and information, there are also many recent developments. With the advanced technology of computer software and hardware systems, business and industrial applications have expanded rapidly. For example, many credit card systems have been developed which transfer identification data from individual credit cards, along with a related transaction, to a coded card which is sent to a central location for processing by computer. Such systems still require a large amount of human handling and are somewhat susceptible to unauthorized use. Thousands of credit cards are stolen each year and used by unauthorized holders, resulting in great losses to business and industry. Furthermore, although there have been attempts to consolidate many of these systems, the average person must carry with him several credit cards for the various goods and services which he may require.

Although some attempts have been made to combine a reliable authorization or identification method with an efficient data collection, control and information system, e.g., see the aforementioned U. S. Pat. No. 2,905,926, a practical system with the desired flexibility has apparently not been developed.

SUMMARY OF THE INVENTION

In the present invention, a unique digital key identification code supplies input signals to an automated data collection, control and source information system as the means of operating a controlled device and providing source identification data to a master control system. The resulting system is a unique approach to administrative management systems and solves the identification data input problem in a new and novel fashion for a highly controlled yet flexible information system.

The unique key apparatus of the present invention comprises a key, digitally encoded with light transmission elements for reading by a message generator apparatus. This apparatus includes a light source and photodiode detecting circuits. This design permits the digital encoding of an existing key by affixing the optical encoding element thereto and attachment of the message generator to an existing conventional lock receptacle. The message generator apparatus may be connected to a recording device, which is programmed to operate in accordance with the concepts of a master control or information management system. The recording device may be provided with immediate access to stored data either in a computer or previously created on magnetic tape by a computer. The recording device may record source identification data from the key apparatus and other related components. The master control system may then be programmed to check this data for both validity and authorization for use of the key.

With the uniquely encoded key of the present invention, a new and simple method of sensing through the use of the light source and photodiode circuits is provided. With this method, one key (i.e., mechanically the same key) can be used individually in a number of key receptcles with unique approval codes for each. In addition, a special method of retaining the coded key in its receptacle is disclosed. The key is locked up on its insertion and cannot be turned or released until proper verification is received from the master control components of the system. The authorization of a release is therefore rendered flexible and is established by each controlling authority.

The invention is particularly suitable for basic data collection control and information management problems of service type businesses. This is accomplished by the proper combination of the key apparatus with suitable computer hardware and software in an unobvious manner resulting in a significant technological advance of information systems. An extremely flexible numbering system is provided through the use of standard binary coding systems. Large amounts of information can be retrieved, searched and compared according to specific and programmable sequencing of the system.

The present invention is a significant improvement over existing credit card methods. The numbering capacity, capability and flexibility of the system is sufficient to enable one organization to handle the manufacture and issue of all keys and the decoding device. This provides a significant advantage for the customer user in that he has one key for multi-credit authorizations. This approach is highly unlikely with the existing credit card procedures. The key systems permits each

company to handle its own processing as it desires while providing a new convenience for the customer. Most credit systems depend upon centralized methods which are time consuming and expensive. This is eliminated with the present key system which checks each encoded key for proper authorization by searching the properly established files stored in the data processing components of the master control. Furthermore, the procedures and methods of the system operate in a closed loop fashion removing the decision for approval by a local attendant.

Further objects, features and advantages of the invention will appear hereinafter. The invention may best be understood by reference to the accompanying drawings and detailed descriptions thereof.

BRIEF DESCRIPTION OF THE DRAWINGS

In the detailed description which follows, reference will be made to the drawings in which:

FIG. **1** is a side view of a key to which a coded identification block has been attached according to a preferred embodiment of the invention;

FIG. **2** is an enlarged perspective view of the identification block attached to the key in FIG. **1** showing one arrangement of light transmission fibres therein;

FIG. **3** is an elevation view, partly in section, showing the encoded key of FIG. **1** inserted into a key receptacle with which is associated a sensing device according to a preferred embodiment of the invention;

FIG. **4** is a sectional view of FIG. **3** taken along line **4—4** thereof showing a portion of the key and decoding apparatus including a light source and photodiode detector;

FIG. **5** is a schematic representation of the major components of a key automated data collection, control and source information system according to a preferred embodiment of the invention;

FIG. **6** is an enlargement of one portion of the binary encoding circuitry shown schematically as **53** in FIG. **3**;

FIG. **7** is a more detailed, but still schematic, diagram showing a key automated data collection, control and information system as shown in FIG. **5**;

FIG. **8** is a more detailed circuit block diagram showing the input section of a message generator for use in a system such as shown in FIG. **7**; and

FIG. **9** is a more detailed circuit block diagram showing the output section of a message generator for use in a system such as shown in FIG. **7**.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring first to FIGS. **1–4**, a digitally encoded key designated generally by the numeral **10**, will be described for use with a detecting device, designated generally by the numeral **20**, for use with a key automated data collection, control and source information system to be fully described hereafter. The key **10** may be specially manufactured or it may be machined from an existing key to establish reference surfaces **11** and **12**, notch **16** and a notch **13** for receiving an identification block **30**. Special key blanks with extra long shafts may be manufactured to specifications and the serrations **15** matched to an existing key where a large encoded number system is concerned.

The identification block **30**, as more clearly seen in FIG. **2**, may be mitered for attachment in the key notch **13**. The identification block may be manufactured of any of a number of suitable opaque materials with light transmission fibres arranged in various schemes, rows **32–36** in this case, for registration with corresponding light transmission fibres located in the sensing mechanism **20**. These light transmission fibres carried on the key may be arranged in a predetermined binary coded fashion to reflect particular identification data. For example, four vertically arranged fibres in rows **32–35** in the identification block shown may represent one digit of a key number. Similarly other groups of four vertically arranged fibres may represent subsequent digits which, when decoded, reflect the arabic numberals 1191464278 (as shown in FIG. **1**). The lower row of light fibre **36** may represent the binary number 11001101 in the present case, for an approval code number or matrix. The key number and approval code may be stamped on the key head as shown in FIG. **1**. These could represent credit card or social security numbers if desired.

In operation, the key **10** is inserted into a receptacle **40**, to which the sensing mechanism **20** (to be described subsequently) is attached. The receptacle **40** may be an existing lock mechanism or one which is specially installed to activate a related device as programmed by the computer components of the system to be described hereafter. In fact, it may not be a lock at all, serving only as a receptacle for a key **10** or a credit card type device (not shown) if desired. The decoding mechanism **20** may take many forms and may be attached to the receptacle **40** in any suitable manner. In the exemplary embodiment, shown in FIG. **1**, it comprises a cylindrical body **21** threadingly connected to cylindrical cover **22** having apertures **23** and **24** for entry of the key **10**. The decoding mechanism **20** also comprises a reader solenoid **50** and a seizure solenoid **60**. The reader solenoid **50** is biased by spring **51** away from key **10** while seizure solenoid **60** is biased toward key **10** by spring **61**. The reader solenoid **50** houses a light source **52** on one side of the encoding block **30** and photodiode logic circuits **53** on the other side (see FIG. **4**). Light transmission fibres **54** and **55** are also housed in solenoid **50** for registration with the light fibres in identification block **30** so as to provide light transmission circuits between the light source **52** and photodiode logic circuits **53**. Contrary to other key authorization devices, the present invention requires no contact between the code carrying apparatus, block **30**, and the decoding mechanism **20**.

When inserted completely against the reference stop **11**, contact is made between reference surface **12** and electrical contact **25** to energize the sensing mechanism by completing an electrical circuit to turn on the light source **52** and to activate the photodiode logic circuits **53**. When inserted into this position, the key **10** cannot turn until further steps are completed and it cannot be removed because the seizure solenoid **60** has been engaged. The end of the seizure solenoid **60** which contacts the key **10** is constructed with a slot **62** which straddles a portion of the key **10**. The slot **62** has a beveled or angled portion **62** which permits easy insertion of the key into the receptacle **40** forcing it downwardly against spring **61** until it engages the locking notch **16** of the key.

When the electrical contact **25** is engaged by the key, power is supplied from power source **70** through line **78** to energize solenoid **50**, lowering the light transmission fibres **54** and **55** into registration with the identifi-

cation block 30 and indicating through the signal or status line 71 to an external control device (master control unit) that the code lines 76 from the photodiode logic circuits 53 are ready to be read. The photodiode logic circuits 53 detect light transmitted through identification block 30 according to the binary code arrangement therein and transform this to electrical signals which are transmitted via lines 76 to a message generator (171, 172 of FIG. 7).

Each of the light transmission fibers 55 of FIG. 4 are connected as illustrated schematically in FIG. 6 to a light sensitive diode 53. The cathode side of photodiodes 53 are grounded and the base sides thereof are connected via load resistor R to a source of voltage +V. When the fibres 55 illuminate photodiodes 53, the diode conducts, thereby effectively presenting a zero voltage (binary 0) or short to ground on its corresponding line 76. When no light is emitted from fibres 55, the bias voltage +V (binary one) appears on line 76 as the diode is non-conducting, thereby effectively appearing as an open circuit to voltage +V. With one photodiode 53 thus associated with each light fibre 55 in the 5 × 10 array of the identification block, then 50 output lines 76 are supplied in parallel with binary electrical output signals corresponding to the key number and approval code as shown in FIG. 2.

The status line 71 indicates which receptacle 40 is initiating the information and when the code information can be read. If the code is acceptable for the particular receptacle 40, the seizure solenoid 60 may be energized through line 72 and retracted out of engagement with key 10 to allow turning and removal of the key. When the seizure solenoid is energized, the reader solenoid 50 is deenergized through line 78 and returns to its nonregister position. Once energized, the seizure solenoid 60 is electrically latched into place through contacts 74, 75 and 25. When the key 10 is removed, breaking contact with electrical contact 25, this latching is released. The seizure solenoid 60 may be eliminated and activation of the associated device could be done electrically through a signal such as the one transmitted through line 72.

The 50 parallel binary bits supplied along the 50 lines 76 (FIG. 7) from key readers 20 as just described are input to message generators 171,172 etc. of FIG. 7. The message generator 171, in a manner to be described, converts these to a 50 bit serial message for transmission to a master control unit 180 via a single message input line 178. While a serial message is present on message input line 178 from a particular key unit 20 the message generator 171 of FIG. 7 supplies a signal on an "input busy" line 176 to inhibit the presentation of other input data from other message generators 172 to the master control unit 180.

Other conductors used in the system include a clock line 174 which is supplied with reference clock pulses from a standard clock (not shown) and used for synchronization purposes as will be described, two power lines 173 which supply power to all system components, and an "output busy" line 175 which is used to inhibit the output of data from the interface electronics of the master control unit 180 to the message generator 171, 172 etc. and key readers 20 until they are in condition to accept such data. Seven address input lines 179 and seven address output lines 177 complete the closed loop control system linking the master control unit 180 to the message generators 171, 172 etc. and key readers 20 of the system. These lines supply, in parallel, seven binary bits of address information to identify the (up to 128) particular unit being contacted by or from which data is being accepted by the master control unit 180.

The input/output bias 181 of the master control unit 180 may comprise, typically, an input buffer in an eight or 16 bit mini-computer having a central processing unit 182. Such a computer could be, for example, a PDP-6 computer manufactured by the Digital Equipment Corp. of Cambridge, Mass. if desired. Of course other small general purpose computers could be used for this purpose and the selection of a particular model is not critical to the operation of the system of the invention.

Referring now to FIG. 8 the operation of one of the message generator units 171, 172 etc. may be examined in more detail. This figure shows the input section of the message generator (i.e., input with reference to the key reader units 20). It will be recalled that when a key is inserted into the unit 20 a contact 25 (FIG. 3) is closed. The resulting signal is supplied via a "key in" line 202 of FIG. 8 (corresponding to line 71 of FIG. 3). If no signal is present on line 176 (input busy) then "send latch" 205 is conditioned for operation via AND gate 204. This latch 205 places a signal on "send line" 206 which remains until the latch 205 is reset and allows the 7 bit wired address register 207 to present the address bits to "address in" lines 179 in parallel fashion via gates 208.

Simultaneously the parallel input data from the reader 20 is supplied on the 50 parallel input lines 76 to a parallel to serial shift register 201. When a signal is present on "send line" 206, the receipt of each new clock pulse (via clock line 174 and gate 209) causes shift register 201 to shift one bit of its contents out serially onto line 178 ("data in" line). When this process has been repeated 49 additional times, the "X49 counter" 210 stops the "send" process by turning off the "send latch" 205 by supplying a reset signal on reset line 211. This reset signal is also supplied to shift register 201, allowing the 50 parallel inputs to change as applicable.

Referring now to FIG. 9 the output section (with respect to key reader unit 20) of one of the message generator units 171 of FIG. 7 is shown in more detail. When the master control unit 180 has (for example, by software program determination) determined that a key inserted in a particular key reader unit 20 should be allowed access to open its lock, the master control unit interface electronics presents the 7 bit address of that particular key reader unit 20 on lines 177 (address output lines). The "output busy" line 175 is also signaled. When this occurs the senser address bits on lines 177 are compared in bit comparators 220, 221 with the seven address bits from the wired address register 207. If each bit of the addresses correspond correctly then OR gate 223 produces an "address check" output on line 222. This "address check" signal on line 222 together with the "key in" signal on line 202 (produced by contact 25 of FIG. 3 when a key is inserted in a key reader unit 20) then set an "enable latch" 224. The "enable latch" 224 produces the aforementioned "unlock enable" signal on line 72 to allow seizure solenoid 60 (FIG. 3) to be energized to allow the key to be turned and withdrawn from the lock receptacle in the key reader unit 20. Thus the message generator units

171, 172 etc. exert control via the master control unit 180 on all of the units which are accessed by the key reader units 20.

Referring now to FIG. 5, the major components of a key automated data collection, control and source information system, with which the foregoing key design may be employed will be described. The system may comprise a master control unit 100 (corresponding to master control unit 180 of FIG. 7) connected to a plurality of remote keyways 110–113 hardwired or interfaced with the master control unit.

The control unit may comprise a standard two unit (station 1 and station 2) magnetic cassette device interfaced with a mini-computer as previously described. These two devices form the master control unit 100. The unit is activated by the use of an operator key 120 and an authorization key 121, both of which may be of the type described with reference to the previous figures. The magnetic tape cassette unit has read, write and search capabilities thus facilitating data storage and retrieval. The master control unit may be configured to meet the specific demands of a proposed key system. Items such as memory size, memory word length, clarity check, memory protect, the central processing capabilities, arithmetic operation, input/output methods, peripheral device availability and mainframe software are part of the unit selection. The master control unit accomplishes the necessary functions of monitoring, searching, input/output printing and sequencing programs in accordance with the request of the operator display board which operates the key system program.

The master control unit may contain a supervisor key locked cassette receptacle for security. Only the key encoded for this lock unit will unlock the unit thus permitting removal of the master cassetts (station 2). This transaction may also be recorded by the master control unit.

The auxiliary units 101, 102, 103 are the type which contain a single cassette tape. This type unit is designed to record in a specified format sequence. A cassette must be prepared by the master control unit 100 in order to operate on the auxiliary units 101, 102 and 103 and for this reason, the auxiliary units may be considered computer components also. Such units are available from Sykes Datatronics of Rochester, New York and Cypher Data Products of San Diego, California. A supervisor locking receptacle for the single cassette may be included for security and control. The auxiliary units are provided with operating buttons identified according to their use. Insertion of an operator key 105, 106, 107 activates its respective auxiliary unit and insertion of an authorization key 115, 116, 117 activates the operator buttons. Upon completion of a particular function, these keys are released and another transaction can start. The auxiliary unit operating buttons can be wired to operate in several ways. Some of the buttons can be set up to operate without involving the authorization key holder. The auxiliary units 101–103 record any transaction conducted through the use of the respective operator keys 105–107 or authorization keys 115–117.

The remote keyways 110, 111, 112, 113 which function like authorization key 121, are hardwired or interfaced to the master control unit 100. In this manner, a significantly large amount of keyways can be checked, recorded and approved for entry by the same control unit 100. This is very useful in multiple receptacle or lock installations or vending machine operations. The same thing could be done with auxiliary units 102–103.

The automated data collection, control and source information system of the present invention has many uses. One use contemplated is for completely automating a self-service station having vending machines for dispensing of food, car accessories, and other products in addition to the usual gasoline. Each vending device would have a keyway for the insertion of a customer authorization key. Upon insertion, the key locks into a receptacle and the central master control unit initiates a search of the identification files for the key number. If the number is found, the master control unit notifies the attendant by the ringing of a buzzer or some other form of acknowledgement. The attendant takes proper action according to company policy. An approved transaction releases the customer key after recording the data and activating the vending unit for the items.

In the self-service station, the master control unit prints a hard copy log of each operation. In addition, the customer may obtain the hard copy receipt. Gasoline sales may require a signature even though the key system is in use. Each pump is hardwired to the master control unit, so that product, volume, price per unit and total sales are available to the master unit. At completion, the authorization key is released and the unit may produce a receipt in duplicate. The customer signs the document, which is similar to those in use in most service stations today.

A single key can be encoded for the authorization of several credit systems. The key system in the case of a service station may permit the customer to be selective in the use of his credit in accordance with those systems honored by the company. In each instance, the key system makes an automatic check of the customer's credit by searching the identification files for the customer number. A service station may use the two key concept described with reference to FIG. 5. Under this concept, each employee would have an encoded key (operator key). In a typical sale of premium gasoline, where the device is not attached to the station pump, the station attendant inserts his operator key and the customer authorization key. The attendant presses buttons on the keyboard for premium gasoline, the volume and amount. He then pushes an enter button which completes the transaction. The master control unit records data on each operation such as: station number, key unit number, attendant number, authorization number (customer), sale, time, product, volume, price per unit and total price. This detail permits a descriptive invoice procedure other than the existing "country club" billing where documents are returned to the customer along with a card invoice.

Under the master control concept, the central office of the controlling firm issues the identification files on the cassette units. For security, both cassettes (station 1 and station 2) are secured by a locking mechanism controlled by an encoded key. This permits the station to practice the type security specified by the firm. Transaction cassettes (station 1) are predetermined by the local area management of the company and the master cassette (station 2) will normally be approved by this responsible management.

The system of the present invention could also be used for the automation of an administrative system for the medical or health care profession. The system

might involve a two-key operator and authorization concept which permits the installation of a responsibility management system at the individual level of medical employee-patient. It defines by a definite accountability procedure how efficient the installation is relative to patient care. An exemplary system would cover the major functional area of a hospital. These include admissions, nurse station, service area, patient rooms and business office.

The hospital's system would consist of master control units in each of the major functional areas hardwired from the nurse station to each service area and the business office. Auxiliary units would be installed in each patient's room. The auxiliary units could be stand along units or they may be on-line, or hardwired, to the nurse's station master control units which they serve. The concept of the system is to capture the detailed data at the source, on a time frame basis, by the operator with the associated authorization. The data is collected in such a manner that the data is directly accessible and processable by the local operator on the master control unit yet can be directly input to a large computer system for a detailed management information and processing. Source information is captured only once and used thereafter by operators of the system. This minimizes errors in creating the original data. The original source is normally the most informed on the problem. This system places the responsibility at the originator.

On admission to a health care facility, admissions personnel would place a magnetic tape cassette into station 1 of the admissions master control unit, obtain an encoded patient key from storage and insert the key into the master control unit. The operator would then insert his encoded key into the master control unit. The unit would check identification of the operator and be ready to proceed with admitting of the patient. Pertinent information such as key number, patient number, doctor's name, admission date, age of patient, room number, bed number and nursing station would be placed on the cassette tape. During these operations, the same information would also be recorded in the master magnetic tape of station 2.

After admissions, the patient, with his patient key and patient transaction cassette, would be escorted to the proper nurse station. At the nurse atation, an operator would insert the patient cassette into station 1 of the nurse station master control unit to enter the proper transaction for admission to the designated room. This master control unit would transfer the information on the patient cassette into the master cassette of station 2 for storage. The master control unit would also place a unique code onto the patient cassette as did the admissions master control unit. The patient cassette would then be removed from the nurse station control unit and carried to the patient's room. Here it would be inserted into an auxiliary tape unit. An attendant key would be used to unlock the receptacle which stores the patient cassette. This would then trigger the initial transaction on the tape and permit removal of the attendant key. The patient's key would be inserted into the unit where it would be locked up. As services are provided to the room, the individual performing the services would use his key to operate the unit thus designating the function accomplished. The transaction on the patient's cassette would be recorded for processing by the business office. These transactions would normally be processed each night. When the patient is dismissed, the nurse station would make the dismissal transaction on its master control unit and send the patient cassette for the last day's transactions to the business office. The business office would then price these entries and complete the necessary dismissal forms on the master control unit located in this department.

A great number of hospitals now have an administrative accounting system. These may include such reports as admissions census, report of changes, cash receipts, cash disbursements, discharge transaction journal, accounts receivable, income summary, in-patient trial balance, aged account analysis, in-patient statements, out-patient statements, guarantor reports and statements, general ledger and general ledger trial balance. The key system interfaces with these and provides for the first time a method and procedure which collects basic data at the source which can be used to assist in better and more efficient operation relative to its effect on the patient and the management of the institution.

The key system of the present invention is extremely flexible. Although only two applications have been described herein, there are many others for hotels, motels, security systems, apartments, retail stores, communication firms and in general all types of service oriented businesses.

The authorization key device could be used alone simply as a lock security system without the other functions described. Furthermore, the type of key used for actuating and providing source and identification data described herein could be varied. For example, a magnetic key could be used. The key would have a registration area along a shaft which would contain small hidden magnetic bars to activate the recording device of the system which causes data to be imprinted on magnetic tape contained in the cassettes. The magnetic bar arrangement would be converted into electrical impulses recorded on a magnetic tape for use in associated primary arithmetic computer. The registration area of the key is called a "field." Each field is divided into equally spaced "bytes." Each byte represents one numeric number. Each byte is divided into four equally spaced parts called "slots." Four slots contain one numeric number from 0–9 represented by a binary system. The small magnetic bars embedded within the key shaft in a binary code arrangement would be sensed by suitable reading device. Such a coding scheme is readily recognizable by present day computers.

Although several embodiments of the invention have been illustrated and described herein, it is obvious that many other modifications and changes can be made by those skilled in the art without departing from the spirit of the invention. It is therefore intended that the scope of the invention be limited only by the claims which follow.

We claim:

1. Key operable identification and authorization apparatus comprising:

a. key operable authorization means having a key receptacle and capable of being mounted with said key receptacle in alignment with the key receptacle of a conventional lock without impairing the ordinary function of said lock, said key operable means being capable of existing in deactivated and activated states;

b. key means insertable through said receptacle of said authorization means and into the key recepta-

cle of said lock for transferring said key operable authorization means between its deactivated and activated states;

c. digitally coded means mounted on the part of said key means which does not function to operate said lock;

d. sensing means carried by said authorization means for non-contacting registration with said coded means; and

e. control means connected to said key operable authorization means and to said sensing means and responsive to a signal from said sensing means to activate said key operable authorization means.

2. Key identification and authorization apparatus as set forth in claim **1** comprising retainer means biased toward a first position engaging said key means for preventing removal of said key means from said authorization means, said retainer means being connected to a power source operable in response to a signal from said sensing means to overcome said biasing means and move said retainer means to a second position out of engagement with said key means.

3. Key identification and authorization apparatus as set forth in claim **2** in which said retainer means comprises an electrical solenoid activated by said power source to move said retainer means to said second position, said solenoid being deactivated on the removal of said key means from said receptacle means to resume said first position.

4. Key identification and authorization apparatus as set forth in claim **1** characterized in that said digitally coded means comprises a plurality of identification elements embedded in said non-operable part key means in a predetermined binary coded fashion to reflect particular identification data, said sensing means having detecting means responsive to said identification elements on said registration to transmit said identification data to said control means.

5. Key identification and authorization apparatus as set forth in claim **4** characterized in that said identification elements comprise a plurality of light transmission fibres arranged in said binary code arrangement, said sensing means comprising a light source and light sensitive logic circuitry, said light fibres providing a circuit through which light is transmitted from said light source to said logic circuitry according to the binary code arrangement thereof.

6. Key identification and authorization apparatus as set forth in claim **5** and further including an electrical solenoid biased away from said registration position but activated by said key means on engagement with said authorization means to move said light source and said logic circuitry into registration with said light fibres.

7. Key identification and authorization apparatus as set forth in claim **4** in which said detecting means is connected to said control means through message generator means by which said identification data converted to information suitable for use by said control means.

8. Key identification and authorization apparatus as set forth in claim **7** in which said message generator means is connected to said sensing means via a status line for indicating the insertion of said key means into said receptacle means.

9. Key identification and authorization apparatus as set forth in claim **5** in which said logic circuitry is connected to said control means through message generator means by which said identification data is converted to information suitable for use by said control means.

10. Key identification and authorization apparatus as set forth in claim **7** in which said logic circuitry is connected to said message generator by a plurality of parallel lines, each line supplying a binary bit of said identification data, said message generator means comprising circuitry for converting said identification data to a plural bit serial message for transmission to said control means via a single input line.

* * * * *