T235/382
X235/381

United Stat

Stark et al.

[11] 3,857,018
[45] Dec. 24, 1974

[54] **CONTROLLED ACCESS SYSTEMS**

[75] Inventors: **Richard M. Stark,** Long Lake; **Ronald G. Beachem,** Mound, both of Minn.

[73] Assignee: **Business Electronics, Inc.,** Minneapolis, Minn.

[22] Filed: **Dec. 7, 1973**

[21] Appl. No.: **422,753**

[52] **U.S. Cl.** ..... **235/61.7 B,** 340/149 A
[51] **Int. Cl.** **G06k 5/00,** H04q 3/00
[58] **Field of Search** ..... 235/61.7 B, 61.7 R; 340/149 A, 149 R

[56] **References Cited**

UNITED STATES PATENTS

3,593,291	7/1971	Carter	235/61.7 B
3,655,947	4/1972	Yamamoto et al.	235/61.7 B
3,761,682	9/1973	Barnes	235/61.7 B

Primary Examiner—Daryl W. Cook
Attorney, Agent, or Firm—Dorsey, Marquart, Windhorst, West & Halladay

[57] **ABSTRACT**

A security system for use either as a means for establishing credit or for limiting access to restricted areas. The system operates with a card having a variable 20 by 20 row and column matrix as its internal configuration. The system may be programmed to read any number of digits in the matrix, in any combination and in any sequence. This feature allows the owner of the system to create unique card codes and to change these codes at any time. Programming is accomplished simply by closing a key switch and positioning the proper sequence of numbers on an input keyboard. The authorized holder of an identification card is assigned a unique keyboard number for his card depending on the owner's program. Each cardholder must then use his input number which is based on his card's internal configuration. In addition, further programming of this system provides eight levels of control. This feature allows a single installation to have up to eight increasing levels of security with no change in the card's unique configuration. Cards may be coded for entry to one area only, to all eight areas or to any intermediate number of areas. Similarly, credit ranges can be established in the same manner. Provision is also made to selectively lock out individual cardholders.

15 Claims, 7 Drawing Figures

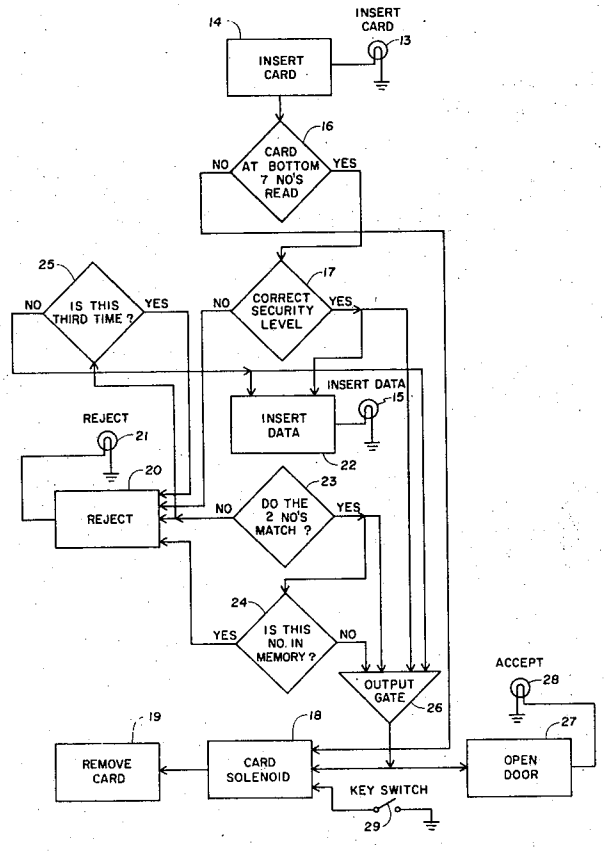


Fig. 1

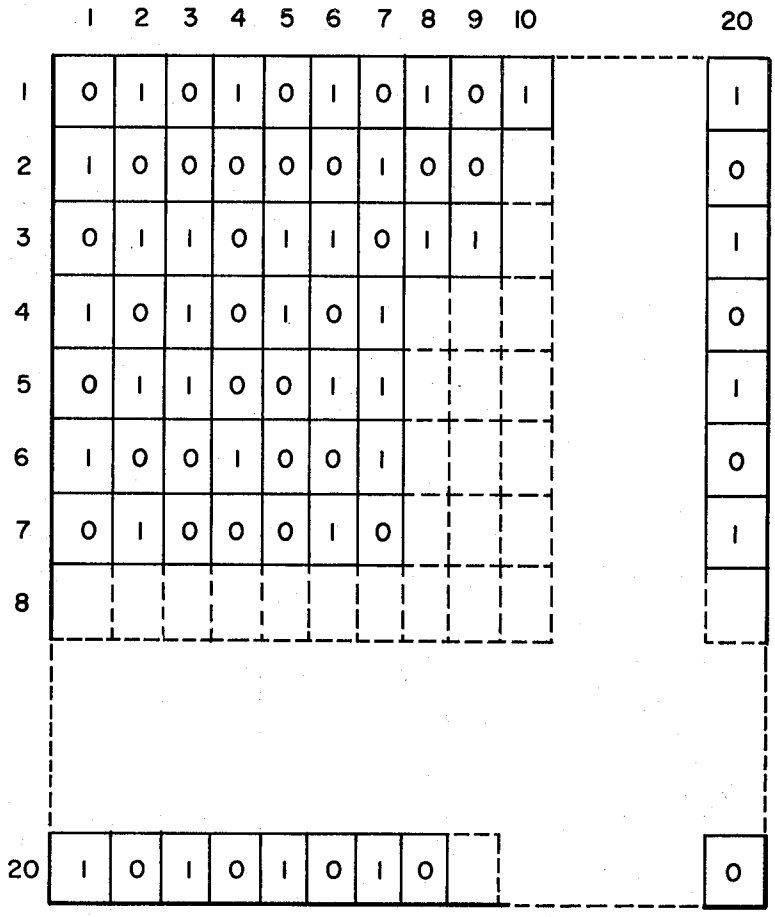
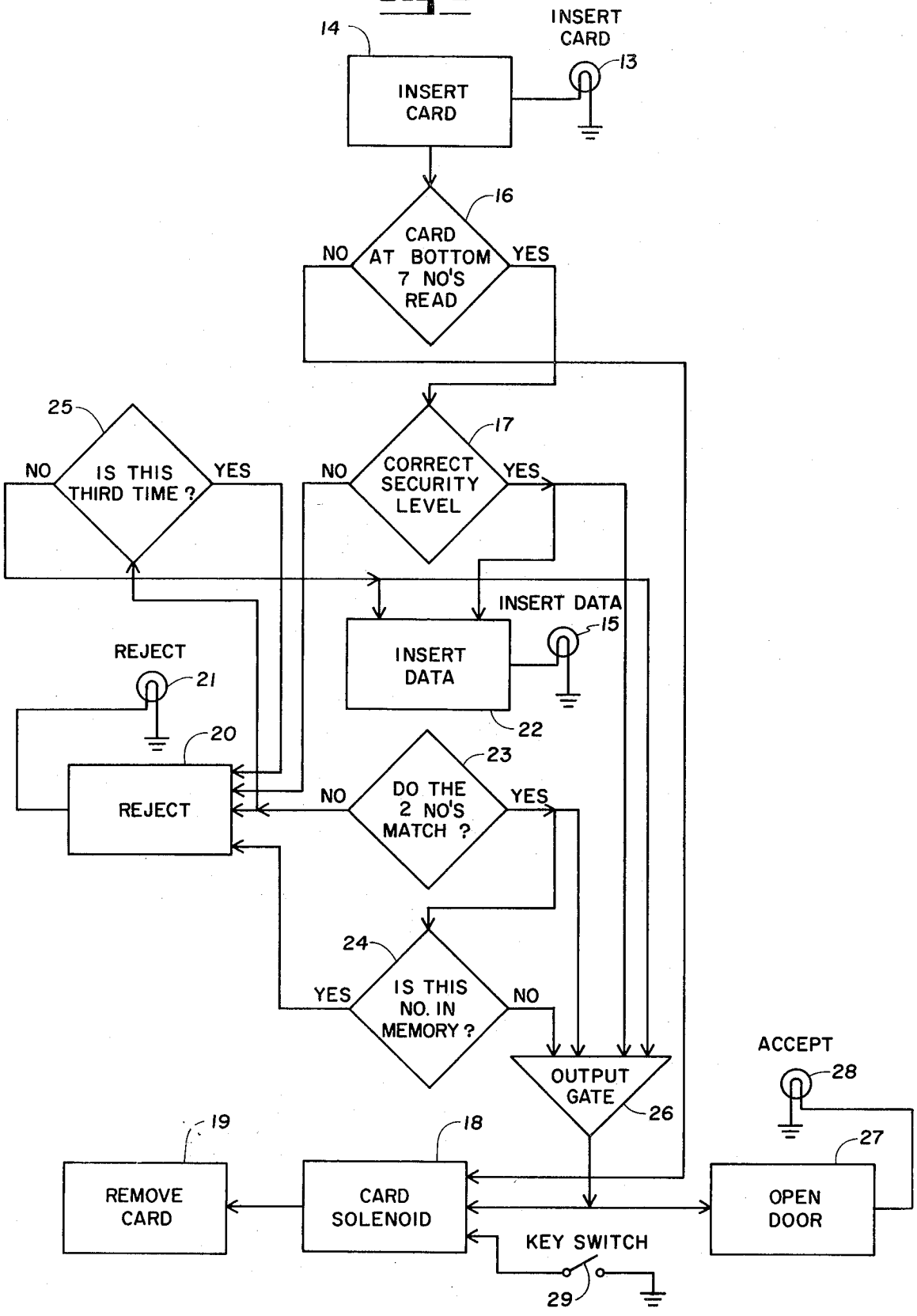


Fig. 3

Fig. 3a
Fig. 3b
Fig. 3c
Fig. 3d

Fig. 2


14
INSERT CARD
INSERT CARD
13
16
CARD AT BOTTOM 7 NO'S READ
NO
YES
25
IS THIS THIRD TIME ?
NO
YES
17
CORRECT SECURITY LEVEL
NO
YES
INSERT DATA
15
INSERT DATA
22
REJECT
21
20
REJECT
23
DO THE 2 NO'S MATCH ?
NO
YES
24
IS THIS NO. IN MEMORY ?
YES
NO
OUTPUT GATE
26
ACCEPT
28
27
19
REMOVE CARD
18
CARD SOLENOID
OPEN DOOR
KEY SWITCH
29

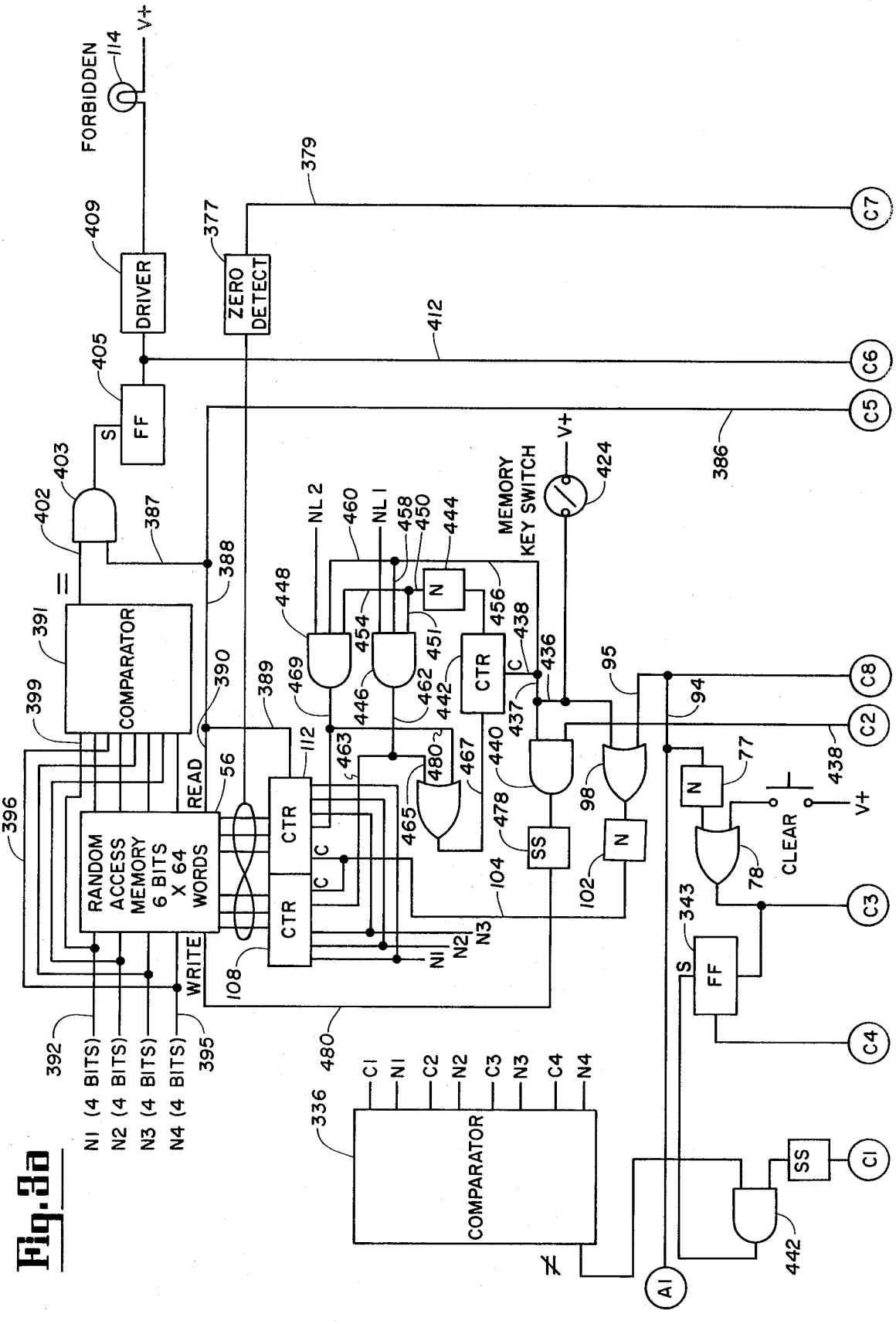
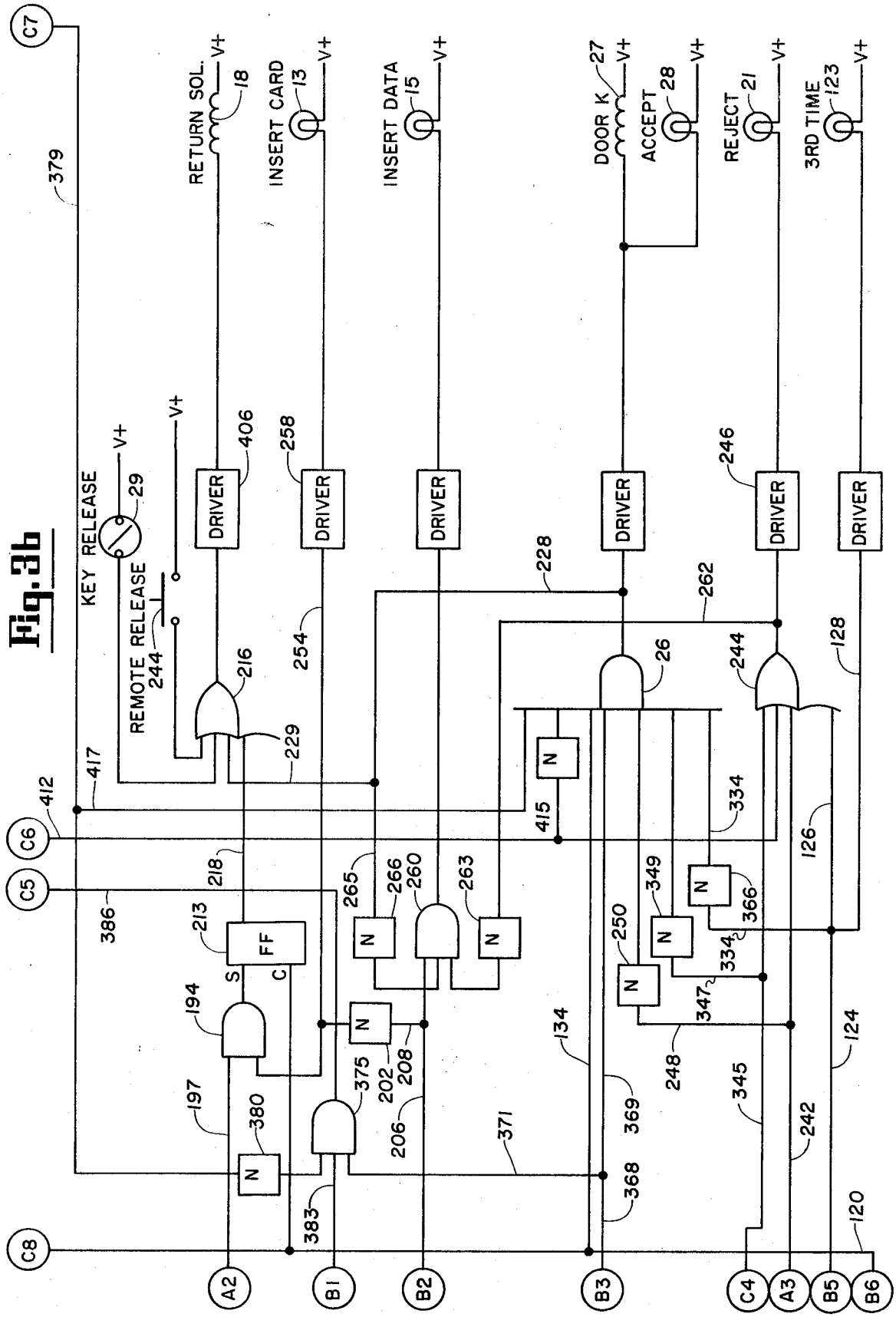

FORBIDDEN
114
V+
409
DRIVER
405
FF
S
403
402
387
388
391
COMPARATOR
399
396
RANDOM ACCESS MEMORY 6 BITS X 64 WORDS
READ
WRITE
56
390
389
112
CTR
C
108
392
395
N1 (4 BITS)
N2 (4 BITS)
N3 (4 BITS)
N4 (4 BITS)
377
ZERO DETECT
379
412
386
C7
C6
C5
C8
C2
C3
C4
C1
A1
MEMORY KEY SWITCH
424
NL 2
NL 1
460
458
450
444
448
454
451
456
438
436
446
462
442
469
463
480
467
465
440
437
478
SS
104
102
98
95
94
77
78
CLEAR
343
336
480
C1
N1
C2
N2
C3
N3
C4
N4
442

Fig. 3a

Fig. 3b


C7
379
RETURN SOL.
18
INSERT CARD
13
INSERT DATA
15
DOOR K
27
ACCEPT
28
REJECT
21
3RD TIME
123
V+
KEY RELEASE
29
REMOTE RELEASE
244
DRIVER
406
258
246
216
229
254
228
262
26
244
128
417
412
C6
C5
386
218
213
FF
S
C
194
197
380
N
375
202
208
206
371
265
266
260
263
415
334
126
349
366
250
347
248
345
242
124
134
369
368
383
C8
120
A2
B1
B2
B3
C4
A3
B5
B6

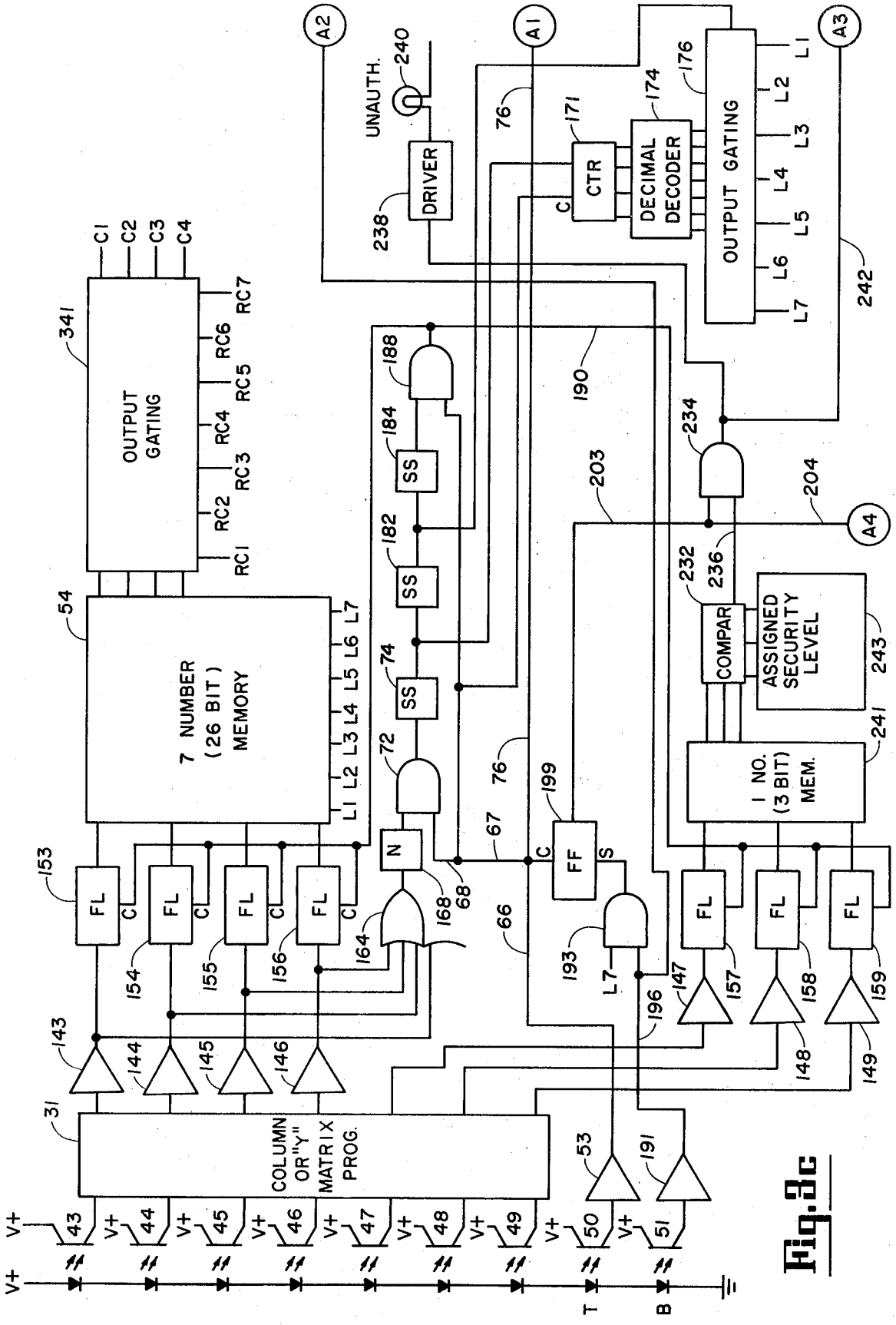

A2
A1
A3
A4
UNAUTH.
240
DRIVER
238
76
CTR
171
DECIMAL DECODER
174
176
OUTPUT GATING
L1
L2
L3
L4
L5
L6
L7
242
C1
C2
C3
C4
341
OUTPUT GATING
RC7
RC6
RC5
RC4
RC3
RC2
RC1
188
184
SS
182
SS
74
SS
72
190
234
203
204
54
7 NUMBER (26 BIT) MEMORY
232
236
COMPAR
ASSIGNED SECURITY LEVEL
243
241
I NO. (3 BIT) MEM.
153
FL
154
155
156
N
164
168
68
67
199
FF
66
193
L7
196
147
157
158
159
143
144
145
146
31
COLUMN OR "Y" MATRIX PROG.
53
191
V+
43
44
45
46
47
48
49
50
51
T
B

Fig. 3c

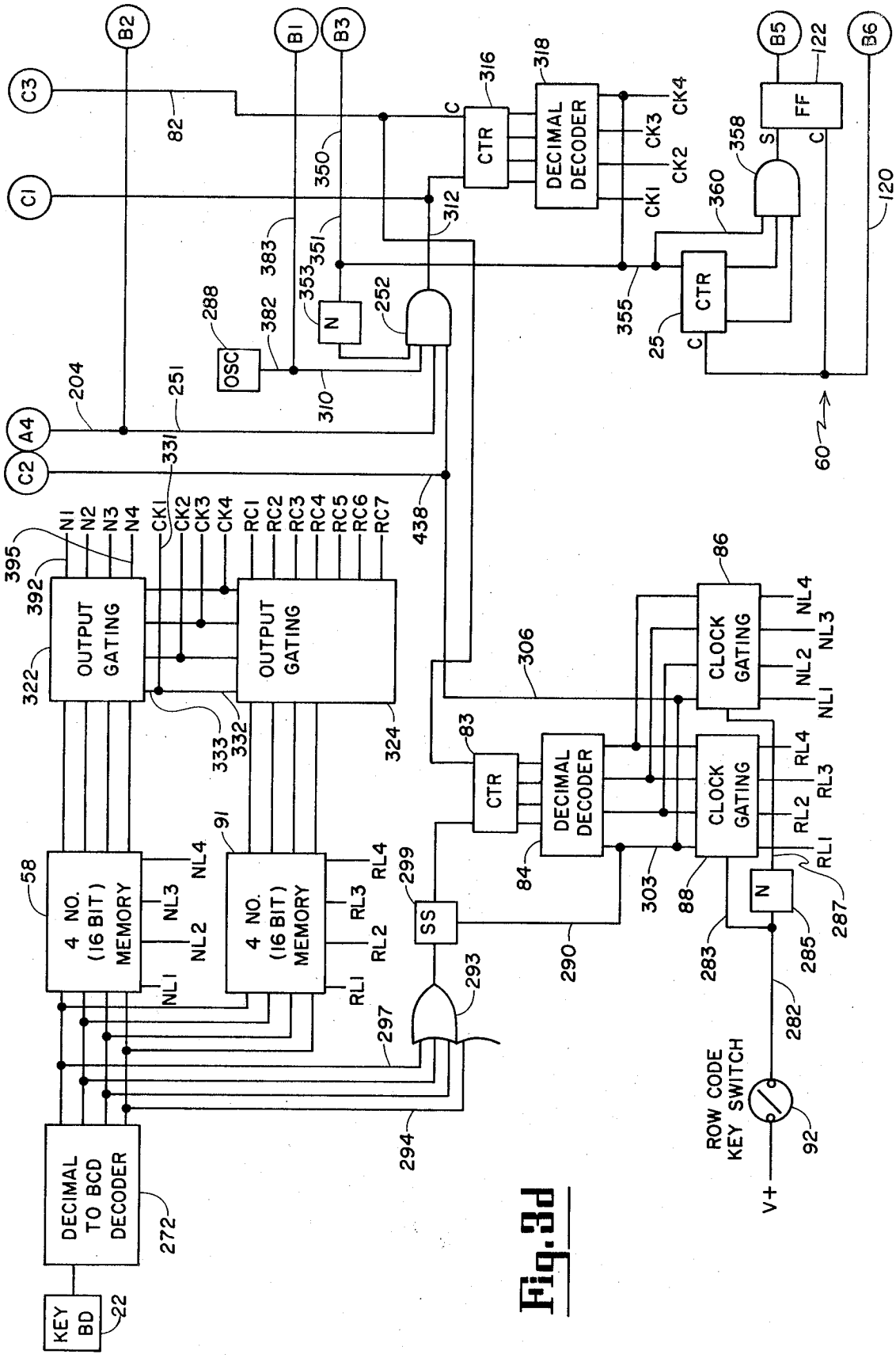

B2
B1
B3
B5
B6
C3
C1
C2
A4
82
350
312
316
CTR
318
DECIMAL DECODER
CK4
CK3
CK2
CK1
358
FF
122
120
360
383
351
353
N
252
288
OSC
382
355
25
CTR
204
251
310
331
60
438
N1
N2
N3
N4
CK1
CK2
CK3
CK4
RC1
RC2
RC3
RC4
RC5
RC6
RC7
395
392
322
OUTPUT GATING
OUTPUT GATING
333
332
324
306
86
CLOCK GATING
NL4
NL3
NL2
NL1
83
CTR
DECIMAL DECODER
CLOCK GATING
RL4
RL3
RL2
RL1
84
303
88
58
4 NO. (16 BIT) MEMORY
NL4
NL3
NL2
NL1
91
4 NO. (16 BIT) MEMORY
RL4
RL3
RL2
RL1
299
SS
290
293
297
294
283
285
287
N
282
ROW CODE KEY SWITCH
92
V+
DECIMAL TO BCD DECODER
272
KEY BD
22

Fig. 3d

CONTROLLED ACCESS SYSTEMS

BACKGROUND OF THE INVENTION

Due to the advent of a cashless society and increased necessity for security controls, plastic and metallic numbered cards are being used ever increasingly for purposes of identification. It is also an actively changing field of art in that owners of card systems are attempting to use more and more sophisticated type apparatus to prevent fraud or unauthorized entry while others, either through contests or for illegal purposes, are increasingly more active in attempts to break the codes or systems used on credit cards and the like.

Initially cards used only embossed numbers on the surface of the card which were mechanically reproduced on a document or were read with mechanical linkages. It is believed that the art then moved to magnetically sensitive strips of tape which, although they cannot be readily duplicated with the naked eye, were read and reproduced with suitable electronic equipment. Other efforts in the field have used apertures in the card or apertures hidden in the card, again sensitive and susceptible to reproduction with the use of X-ray or other suitable equipment. Most recent advances have combined numbers on the card with code numbers memorized by the user, said user numbers being directly related to the number on the card, related to a random combination of the numbers on the card or variably related to a random combination of the numbers on the card depending on a key number which repositions the digits in different combinations.

In these systems, however, each card uses one fixed card number and the card number is a limiting factor for security. For example, with a six digit number and a three digit secret number there are only eighteen three number groupings with six arrangements of each three number grouping or a total or maximum of 108 possibilities which may be utilized for each card number.

SUMMARY OF THE INVENTION

The invention disclosed herein represents the very latest in electronic security control. It has been designed to eliminate the shortcomings of existing systems, and provide maximum security at minimum cost. All components and circuitry are contained in the single wall mounted control unit, with a sturdy, tamperproof chassis.

Access or credit is restricted to those persons with a properly encoded identification card and knowledge of a unique keyboard number for their card. Identification cards may be laminated plastic with an internal encoding pattern which is not vulnerable to heat, chemicals or electromagnetic force.

The invention is available with eight levels of control. This feature allows a single installation to have up to eight increasing levels of security with no change in the card's unique configuration. Cards may be coded for entry to one area only, to all eight areas, or to any intermediate number of areas. Should a user attempt to enter a secure area beyond his authorized level, a remote alarm is sounded, and the card is retained. Similarly, credit ranges can be established in the same manner.

The invention may be programmmed by the system owner to read any number of digits of a multiple row and column matrix, in any combination and in any sequence. This feature allows the owner to create unique codes for the users and to change these codes at any time. Programming is accomplished simply by closing a key switch and pushing a sequence of numbers on the input keyboard.

Each cardholder is then assigned and must use an input number which is based on his card's internal configuration. it is not possible to decipher the number by opening a card since the user never knows what all the digits are, which digits are being read, nor the order of reading. The encoding technique allows for a total of several thousand possible number combinations per card.

Provision is also made to selectively lock out individual cardholders. This feature provides a convenient means to locate and retain stolen credit cards or to deny access to discharged employees still holding a valid identification card. The employee's number is entered by the system owner into a location in the memory bank. This memory bank is scanned each timme a card is inserted. When a number entered by an unauthorized user of the system matches a number in memory, the card is retained, and a remote alarm is activated. Unauthorized members are entered into memory by a simple key-in procedure similar to the programming method. Turning the proper key enables the credit manager or personnel director or other authorized operator to enter the unauthorized number using the same input keyboard. That number remains in memory until it is removed or replaced.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is an exemplary matrix showing a possible internal configuration of an identification card;

FIG. **2** is a simplified flow diagram of the operational steps of the invention; and

FIG. **3** consisting of FIGS. **3***a* – **3***d*, is a schematic diagram showing the logical techniques which are utilized to accomplish the purposes of the invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

As explained in more detail below, operation of the invention is accomplished with three codes. The three codes utilized are: (1) a column code; (2) a row code; and (3) a user's code number.

As sketched in FIG. **1** a 20 by 20 matrix is provided which is read by the system to create a distinct number to be associated with a card. One embodiment which may be utilized employs an opaque insert implanted in the card which is cut or slotted to provide translucent areas which may be read with infrared readers. It should be understood that there is no limit in the size of the matrix, its extent being a choice of design. The infrared reader registers either the opaque or translucent portions of the interior of the card which can be converted into an on or off representation to be read in binary.

Which vertical rows on the card are to be read can be randomly selected and locked in with either a keyboard or by internal wiring (e.g., vertical rows **4, 5, 1** and **2**). This is referred to as the "column program."

The horizontal rows are also selected by the system owner in any order or in any sequence on the keyboard and locked in (e.g., **2, 5, 7** and **3**). Thereafter a programmed number must be punched in by the card-

holder in the order selected before the machine will operate to accept the card.

In other words, suppose the column code is as indicated above, **4, 5, 1** and **2,** and the system owner selects a row code of **2, 5, 7** and **3.** Also assume that the binary representation cut into the interior of the card is as shown in FIG. **1.** Each card utilized will be coded differently, thus providing distinct information. However, since each card will be coded for the entire matrix the information contained on the card will be nondiscrete without the use of the system. A user or cardholder would have to enter the number **2, 1, 1, 5** before the system would accept him as the cardholder. A sketch of the matrix as shown in FIG. **1** shows why.

The cardholder's program number is obtained as follows:

Row **2,** Column **4** has a **0** Column **5** has a **0** Column **1** has a **1** Column **2** has a **0**

Binary No. **0010** is decimal **2**

Row **5,** Column **4** has a **0** Column **5** has a **0** Column **1** has a **0** Column **2** has a **1**

Binary No. **0001** is a decimal **1**

Row **7,** Column **4** has a **0** Column **5** has a **0** Column **1** has a **0** Column **2** has a **1**

Binary No. **0001** is decimal **1**

Row **3,** Column **4** has a **0** Column **5** has a **1** Column **1** has a **0** Column **2** has a **1**

Binary No. **0101** is decimal **5**

Thus, the cardholder's number is **2115.**

A variation can be made in either the column code or the row code, or the cardholder's code number or any combination thereof. Also, if the card is lost or stolen, it can't be used since whoever has it will not know the programmed number.

While an infrared reader is currently utilized to read an insert impregnated in a plastic card it should be obvious that the same type matrix can be impressed on a magnetic tape strip.

FIG. **2** is a simplified flow diagram of the operational steps of the invention. As the user approaches the control unit, an insert card light **13** is energized indicating the unit is in the ready condition. When a card is inserted properly at **14,** the insert card light **13** is deenergized and the key code number lamp **15** is energized. Improper card insertion results in card rejection. As the card is being inserted optical readers **16** determine whether or not the card has been fully inserted and whether or not a specified number of digits have been read, for example, seven digits. In addition, logical programming **17** determines from other information obtained from the card a security or credit level to determine whether the cardholder is in the correct area.

If less than seven numbers were read, a card solenoid **18** is energized to enable the cardholder to remove the card **19** for reinsertion. If the cardholder is not in an authorized security area the card is rejected **20** and the reject lamp **21** is energized.

If the card has been properly utilized the cardholder may now insert data on an input keyboard **22.** Logical gating and a comparator **23** initially match the cardholder's memorized key number with a programmed, unfixed and random number read from the card and then compares the number with unauthorized numbers in a random access memory **24.** If the cardholders's memorized number and the programmed card number do not match or if the cardholder's key number is unauthorized, the card is rejected at **20** and the reject lamp **21** is energized.

It the cardholder enters the proper code and the code is not retained as an unauthorized code in the memory **24,** all inputs to master AND gate **26** are enabled, the door **27** releases, the accept indicator **28** is energized and the card is ejected by the card solenoid **18.** In the event an improper code is entered, the cardholder has two additional chances to key in the proper number. Should he fail, this is noted by a counter **25,** the card is retained and a remote alarm is sounded. At this point, the card can only be removed by a security guard or other authorized persons holding a key to release the card with key switch **29.**

The above operations are accomplished electronically in the following manner. As shown in FIG. **3,** the system is programmed to read from a 20 by 20 matrix impregnated in a card, seven digits in four bit binary and one three bit digit for the security code. The column program **31** is shown as internally wired. It should be understood, however, that the column program **31** may be constructed in the same manner as the row code program described below and that variations can be made in the matrix configuration or the number of digits read and still be within the intention and scope of the invention as claimed.

Referring to the schematic diagram shown in FIG. **3,** information in the interior of the card is read with the utilization of light sensitive transistors **43** through **51.** On each of seven passes these transistors **43** through **49** are capable of detecting four binary bits which represent a decimal number plus three binary bits which represent a security code. In addition, transistors **50** and **51** detect insertion of the card and the bottom of the card.

When the card is inserted, top optical reader **50** is activated. The signal is amplified with amplifier **53** and is utilized to enable the card storage memory **54,** the lock out memory **56,** the keyboard storage memory **58,** the third time counting circuit **60,** to partially enable the door relay gate **26** and to serve as a master clear for other circuits as explained more fully below.

The card storage memory **54** is enabled through amplifier **53,** lines **66, 67** and **68,** which is the initial high signal on AND gate **72..** As explained below, as each additional four bit number is read the second input signal to AND gate **72** goes high activating the one shot **74** to load the data into the card storage memory **54.**

The keyboard storage memory **58** is enabled through amplifier **53,** lines **66, 76** through inverter **77** and OR gate **78,** the output of which is fed by line **82** to counter **83.** The normally low signal from amplifier **53** clears the counter **83.** When the signal goes high it is inverted with inverter **77,** disabling the OR gate **78** and this enabling the counter **83.** As shown in FIG. **3** the output of counter **83** is decoded by decimal decoder **84** and controls the clock gating **86** and **88,** respectively. The clock gating output is then in condition to receive either code numbers through the keyboard **22** or row codes to be stored in memory **91,** respectively, depending on whether or not row code key switch **92** is in an open or closed position.

Similarly, the lock-out memory **56** is enabled through amplifier **53,** lines **66, 76, 94, 95,** OR gate **98,** inverter **102,** the output of which is fed through line **104** to clear counters **108** and **112.** The output of counters **108** and

112 are utilized to sequentially step through the lockout memory 56 so that if a number located in the random access memory 56 compares equally with a number entered on the keyboard 22, the forbiddden light 114 is energized and the number is rejected.

The third time counting circuit is enabled by clearing counter 25 through amplifier 53, lines 66, 76, 94, 120 to counter 25. This clear signal also clears flip-flop 122, the output of which is fed through an OR gate to both the reject light 21 and the third time light 123 through lines 124, 126 and 128, respectively. As shown, the door relay gate 27 is partially enabled through amplifier 53, lines 66, 76, 94, 120 and 134 which is one of the seven inputs to AND gate 26, the output of which, when the other conditions are met, energizes door relay 27.

As the card is inserted, optical readers 43 through 49 read seven columns. The columns read in the twenty by twenty matrix which makes up the interior of the card are determined by the column or Y matrix program 31 which is variable to read any seven of the twenty columns of the matrix. The output pulses from the seven columns are amplified with amplifiers 143 through 149 with the amplified signal being stored in latches 153 through 159. The output of the latches 153 through 156 are then gated into the scratch pad memory 54 as explained below.

When the card is between rows there are not bit signals, thus each of the inputs to OR gate 164 will be low. The low output of OR gate 164 is then inverted with inverter 168 creating the second high input signal to the AND gate 72. The output from AND gate 72 energizes one shot 74 which increments counter 171. The output of counter 171 is decoded by decimal decoder 174 and sets up output gates 176 so that the immediately preceding number is stored in the correct position in the card number storage memory 54. The output of one shot 74 is also fed to a second one shot 182 which serves as a delay to clock output gates 176. When the output of one shot 182 goes high the number is then stored in a correct location in the seven number memory 54. The output of one shot 182 is also fed to one shot 184, the output of which is ANDed with the output of the top optical reader which when it goes high, clears each of latches 153 through 159 to enable them to read the next number.

The bottom optical reader 51 turns off when the card is fully inserted. The output of bottom optical reader 51 is amplified by amplifier 191 and fed to AND gate 193 along line 196 and AND gate 194 along lines 196 and 197, respectively. If there were not seven card numbers read, a flip-flop 213 is set and the card release solenoid 18 is energized. This is accomplished as follows.

The output of the bottom optical reader is fed into an AND gate 193, the other input to which is the L-7 or last output from output gates 176 from counter 171. Thus, if the counter 171 has counted seven numbers and the bottom has been reached, the output of AND gate 193 will be high which sets flip-flop 199. The output of flip-flop 199 is connected to inverter 202 by lines 203, 204, 206 and 208 and the inverted or low input is fed into AND gate 194 along with the high input from the bottom optical reader. Thus, the output of the AND gate 194 remains low, flip-flop 213 is not set, and the card return solenoid 18 is not energized. If, however, seven numbers have not been counted, L-7 will remain low, thus the output of AND gate 193 will remain low and flip-flop 199 will not be set. Its output will therefore remain low. The output of inverter 202 will then be high and when it is combined with the output of the bottom optical reader at AND gate 194, it will set flip-flop 213, the output of which is fed to OR gate 216 by line 218. This will activate the card return solenoid 18 to return the card. It should be noted that the card return solenoid 18 is activated by each of the inputs to the OR gate 216 which comprise a key release switch 29, a remote release button 224, as well as the output of AND gate 26 which will return the card after the card has been accepted and the door relay 27 has been energized.

The accepted card signal 28 is connected to OR gate 216 from the output of AND gate 26 by lines 228 and 229. If seven numbers were read the security level comparator 232 is checked and if the security level is greater than the number assigned to the cardholder, an unauthorized light 240 is energized at the guard station, the door relay 27 is disabled and the reject light 21 is energized. This is accomplished in the following manner.

Optical readers 47 through 49 read bits corresponding to the security level of the cardholder. Only one row is read and by electrical connection this can be any row L-1 through L-7, that row being selected by connection of the one number memory 241 to one of the outputs L-1 through L-7 of output gates 176. The output of the security code memory 241 is compared with an assigned security level 243 having eight levels of security designated 0 through 7. The security level 243 and the number in memory 241 is compared with comparator 232 and the output of the comparator 232 is fed to an AND gate 234. The comparator 232 is set so that if the cardholder's security code entered into the memory 241 indicating the highest security level he can enter is less than the assigned security level setting 243 the output of the comparator 232 will go high. This output is fed to an AND gate 234 through line 236. The other input to the AND gate 234 is the output of the flip-flop 199 which is set when seven numbers have been read and the card has tripped the bottom optical reader 51. If both inputs are high the output of the AND gate 234 is fed through a driver 238 to a circuit which energizes an unauthorized light 240. In addition, the output of the AND gate 234 is fed through line 242 to an OR gate 244. The output of the OR gate is fed through a driver 246 to the reject lighting circuit and the reject light 21 is energized. The output of the AND gate 234 is also fed through lines 242 and 248 to an inverter 250 and the inverted signal, being a low signal, is then inputted to AND gate 26 which prevents all inputs signals from being high, thus disabling the output of AND gate 26, thereby preventing the door relay 27 from being energized.

In addition to the foregoing, if there is a positive indication that seven numbers were read, the clock circuit is partially enabled, the insert card light 13 is deenergized and the insert data light 15 is energized providing there was no reject or accept signal. The clock circuit is partially enabled from the output of flip-flop 199 through lines 203, 204, and 251 which is fed to AND gate 252, discussed below. The insert card light 13 is deenergized due to the signal fed from the output of flip-flop 199 through lines 203, 204, 206, 208 through inverter 202, the low output from inverter 202 being fed through line 254 through driver 258 to extinguish

the insert card light **13.** Finally, the insert data light **15** is energized due to the signal from flip-flop **199** being fed to AND gate **260** through lines **203, 204** and **206.** The other two inputs to AND gate **260** are inverted signals from the reject light **21** and the reenergization circuit for the door relay **27** and accept light **28.** From the reject light **21** the output of OR gate **244** is fed through lines **262,** inverter **263** to the input of AND gate **260.** Similarly, the accept light **28** energization circuit is connected by lines **228, 265,** inverter **266** to the input of AND gate **260.** Thus, when the output of both inverters are high it is an indication that neither the accept light **28** has been energized nor the reject light **21** and thus the third signal through line **206** indicating that the bottom has been reached and seven numbers were read, energizes the insert data light **15.**

After the insert data light **15** has been lit, information can be fed into the circuit through the keyboard **22.** The keyboard **22** is utilized for three purposes. By a cardholder, to enter the cardholder's memorized code number, and by the owner of the apparatus, to change the row code numbers and to enter forbidden numbers in the random access memory **56** which will prevent certain persons with a card from gaining access through the system. As noted above, modification of the circuit in the manner of the row code program may be made to enable the system owner to program the column matrix **31** as well. The keyboard **22** is keyed with a four digit decimal number which is decoded with a decimal to binary decoder **272** and stored in memory **58.** It will be entered in either the code number memory **58,** or the row code number memory **91.** As indicated on the drawing and explained below, numbers may be keyed into the random access forbidden number memory **56** through the code number memory **58.** If the row code key switch **92** is on, the row code memory **91** is enabled and the code number memory **58** is disabled. This is accomplished by feeding a positive signal through the row code key switch **92** into clock gating circuit **88** through lines **282, 283.** The code number memory **58** is then disabled due to inverter **285** which disables the clock gating **86** through line **287.** Conversely, if the row code switch **92** is off, the number memory **58** is enabled and the row code number memory **91** is disabled in the same manner.

At the end of the fourth number keyed into the keyboard **22,** the keyboard **22** is disabled and the internal oscillator **288** is enabled. The keyboard **22** is disabled with the use of inhibit line **290.** As each number is entered into the keyboard **22** the output of the decimal to binary decoder **272** is fed to OR gate **293** through lines **294** through **297.** The output of the OR gate **293** fires a one shot **299,** the output of which is fed to counter **83.** The output of counter **83** is decoded by decimal decoder **84** and when the fourth digit has been entered, the signal on line **303** is fed back with line **290** to the one shot **299** to inhibit further counting. The internal oscillator **288** is enabled in a similar manner. As line **303** registers the entry of the fourth digit through keyboard **22,** the signal is fed on line **306** to AND gate **252.** Since all other inputs are now high, including the varying output of oscillator **288** which is fed to the AND gate **252** through line **310,** the output of the AND gate **252** varies as the oscillator **288** varies. The output of the AND gate **252** is connected through line **312** to counter **316.** The oscillator pulses are counted, decoded with decimal decoder **318** and used as clock signals, CK-1 through CK-4, to gate in the card number and keyboard number through output gating circuits **322** and **324.** To assure that only four clock signals are received the fourth clock pulse is fed directly back to the AND gate along line **351** through inverter **353.** The low output from the inverter disables the AND gate and thus no further oscillations are counted or decoded.

To obtain the random row code the numbers retained in the seven number memory **54** are not directly gated by the clock. Note also that each number of the user's secret number is compared individually with the number in the seven number memory **54** according to the four number program contained in the row code memory **91.**

The first clock signal clocks output gating circuits **322** and **324** through lines **331, 332** and **333.** The four bits which constitute the first of the user's four numbers from the code number memory **58** appear at the input of the comparator **336.** The output of output gating **324** is dependent on the first number in the row code memory **91.** That number determines which of row code one (RC-1) through row code seven (RC-7) will be enabled. The particular row code enable is then fed to the output gating **341** associated with the seven number memory **54.** The four binary bits of that number are then gated to comparator **336.** If the two numbers are not equal the output of comparator **336** goes high which sets a flip-flop **343,** the output of which disables the door relay **27** and energizes the reject light **21.** This is accomplished with line **345** which feeds the output of the flip-flop **343** to OR gate **244** to energize the reject light **21.** In addition, the high output on line **345** is fed with line **347** to inverter **349** which creates a low input to AND gate **26,** thereby disabling the AND gate **26** to prevent door relay **27** from being energized. Each of the four digits in the code number memory **58** are compared to the selected four numbers in the seven number memory **54** according to the row code contained in memory **91.** If any of the four digits are unequal, the door relay **27** is disabled and the reject light **21** is energized in the manner described.

As explained above, the keyboard **22** may only be used three times. Each of the first two uses of the keyboard **22** are stored in the two place counter **25** by registering each of the first two occurences of the fourth clock pulse, the output of the counter being connected to AND gate **358.** The fourth clock pulse is also fed directly over lines **350, 368** and **369** to partially enable AND gate **26** and is connected to AND gate **358** through lines **355** and **360.** Therefore, the third time clock four occurs, the AND gate **358** is enabled and the high output then sets flip-flop **122** which is fed over lines **124, 126** to OR gate **244** to energize the reject light **21.** In addition, the high output of flip-flop **122** is fed over lines **124, 128** to the third time light **123** and is fed over lines **124** and **334** to inverter **366** which disables AND gate **26** so that the door relay **27** cannot be energized.

Finally, a fourth clock pulse without a reject indicates that the two numbers are equal and enables the random access counting and gating circuit to begin the check for unauthorized numbers. This is accomplished through lines **368, 371** to AND gate **375.** A second input to the AND gate **375** is from the zero detect circuit **377** which reads the counter **108, 112** outputs. Although the counters **108, 112** initially are cleared thus indicating a zero state, the zero detect circuit **377** is in-

ternally latched and is not enabled until a digit appears in the counters **108, 112.** The low output of the zero detection circuit is inverted with line **379** and inverter **380** to enable AND **375.**

The third input to the AND gate **375** is the oscillator **288** output which is fed to the AND gate **375** along lines **382** and **383.** Since the output of the AND gate **375** will oscillate this output is fed along lines **386, 387, 388, 389, 390.** Therefore, AND gate **375** gates in the internal oscillator **288** along line **386** to increment the counters **108, 112** with line **389.** The oscillator pulses are also utilized to commmand the random access memory **56** to read with inputs along line **390.** Thus each of the **64** sixteen bit words are clocked into the comparator **391.** Since the contents of the four four bit code numbers are retained in memory **58** and are also inputted to the comparator along lines **392** through **399,** the comparator **391** sequentially compares the user's code number with each of the forbidden numbers contained in the random access memory **56.**

If the user's code number is contained in the random access memory **58,** the comparator **391** output will go high and is fed with line **402** to AND gate **403** which sets a flip-flop **405.** The output of the flip-flop **405** energizes the forbidden light **114** with driver **409.** In addition, the reject light **21** is energized, the output of the flip-flop **405** being connected to OR gate **244** with line **412,** and the door relay **27** is disabled with inverter **415,** yielding a low signal and thus disabling AND gate **26.**

If no equal condition is detected between the user's code number and the numbers contained in the random access memory **56,** the address counters again read zero after the 64th word is read. When it reaches zero the zero detect **377** output goes high, this signal being inverted with inverter **380** which disables gate **375.** This signal is also fed along lines **379, 417** to AND gate **26** which is the last enabling signal for the AND gate **26** and the door would now open if all other signals were true. The accept light **28** would be energized. In addition, the card return solenoid **18** would be energized. This is accomplished by the output of AND gate **26** being fed to OR gate **216** along lines **228** and **229,** the output of OR gate **216** being utilized to energize card return solenoid **18** with driver **406.**

To put a number into the random access memory **56,** the memory key switch **424** is closed which enables the memory address counters **108, 112.** The high output through memory key switch **424** is fed through lines **436, 437, 438** to clear two time counter **442.** The counter initially has a low output which is inverted by inverter **444** and fed to the input of AND gates **446, 448** along lines **450** and **451, 454,** respectively. The second enabling inputs to AND gates **446** and **448** from the memory key switch is fed along lines **436, 437, 456** to the input of AND gates **446, 448** along lines **458** and **460,** respectively.

The desired address for random access memory **26** is then keyed into the keyboard **22.**

The first address digit is entered into address counter **108** as follows. The decimal number is converted to four bit binary by decimal to binary decoder **272** and loaded into four number memory **58.** At the time the entry of the first number is fed along line **297** to OR gate **293** which fires a one shot **299.** The output of the one shot is counted by counter **83** and decoded by decimal decoder **84** which creates a clocking signal NL-1 from clock gating circuit **86.** The clocking signal NL-1 causes the four binary digits contained in the first number location in memory **58** to be read on the four outputs N-1 through N-4 of output gating circuit **322.** Since there are only 64 locations in random access memory **56,** only the first three binary digits or N-1 through N-3 are fed to the input of counter **108.** The NL-1 clock signal is also fed to the input of AND gate **446** which is the last enable for that AND gate. Consequently, the output of AND gate **446** is fed along lines **462** and **463** and used as the command signal to enter the three bit binary number into the counter **108.** In addition, the output is fed along lines **462** and **465** to OR gate **467** to counter **442** indicating the first number has been entered.

In the same manner the second number entered into the keyboard **22** is clocked into counter **112** through AND gate **448** with the use of output NL-2 from clock gating circuit **86.** The output of AND gate **448** is also fed to the counter **442** along lines **469** and **480** to OR gate **467** to the two bit counter **442.** Since counter **442** is only a two bit counter with the entry of the second number, the output goes high, is inverted with inverter **444,** and disables AND gates **446** and **448** through lines **450** and **451** and **454,** respectively.

The keyboard **22** is then cleared with a clear button on the keyboard **22** and the desired four digit number is keyed in. The four bits are stored in four number memory **58,** the contents of which is fed to the input of the random access memory **56,** along lines **392** through **395,** N-1 through N-4. At the completion of the fourth number, a one shot **478** is enabled from the decimal decoder **84** along lines **303, 306, 438** to AND gate **440,** the second input to which is the closed memory key switch **424.** The output of the one shot is fed along line **480** to command the random access memory **56** to write and retain the four digit sixteen bit word in the address location indicated by the address memory counters **108, 112** in the random access memory **56.**

In general, while we have described a specific embodiment of our invention, it is to be understood that this is for purposes of illustration only and that various modifications can be made within the scope of the invention.

We claim as our invention:

1. A system for security control of a desired operation comprising:

a series of identification cards having individually distinct but nondiscrete information as a part of each card;

means for programming said system with a system program to read a random selection of information from the cards;

input means for entering the system program and for enabling a user to enter memorized information into the system;

information sensing means to read the random selection of information in accordance with the system program;

means for comparing the memorized information to the randomly selected information obtained from the cards to determine whether or not they are identical; and

means for implementing the desired operation if the memorized information and the randomly selected information are identical.

2. The system of claim 1 wherein the nondiscrete information associated with the identification cards is impregnated in the identification cards.

3. The system of claim 1 wherein the nondiscrete information associated with the identification cards is affixed to the surface of the identification cards.

4. The system of claim 1 wherein the nondiscrete information associated with the identification cards is arranged in a matrix configuration.

5. The system of claim 4 wherein the system can be programmed to read selected rows of the matrix in any order to establish a number to identify a user of the card.

6. The system of claim 4 wherein the system can be programmed to read selected columns of the matrix in any order to establish a number to identify a user of the card.

7. The system of claim 4 wherein the system can be programmed to read selected rows and columns of the matrix in any order to establish a number to identify a user of the card.

8. The system of claim 1 wherein the desired operation is to identify the user of the card for the purpose of providing credit thereto.

9. The system of claim 1 wherein the desired operation is to identify the user of the card for the purposes of controlling access to secured areas.

10. The system of claim 1 further comprising security level means for establishing various levels of security for the desired operation and wherein a portion of the nondiscrete information associated with the identification cards is related to the maximum level of security that the user may be permitted to obtain.

11. The system of claim 1 wherein the memorized information are numbers used to identify the user and further comprising storage means for storing numbers identifying users who will not be permitted to perform the desired operation;

means for comparing the memorized number with the stored numbers to determine whether or not they are identical; and

means for preventing the desired operation if the memorized number and the stored number are identical.

12. The system of claim 1 wherein the memorized information is a number and each digit of the user's memorized number is sequentially compared with each digit of a number selected by the system program from information associated with the identification card.

13. The system of claim 10 wherein the system may be programmed to obtain a multiple digit number having an identification component and a security level component from the nondiscrete information impregnated in each identification card.

14. The system of claim 10 wherein the desired operation can be accomplished at various levels of security and wherein the system may be programmed to obtain a multiple decimal digit number for identification of the user and a multiple octal digit number to determine at which security level the user may perform the desired operation.

15. The system of claim 14 wherein the system may be programmed to ignore all but one octal digit of the multiple octal digit number, the octal digit number being used to establish the maximum of eight levels of security that the user will be permitted to perform the desired operation.

* * * * *