(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 April 2005 (28.04.2005)

PCT

(10) International Publication Number
WO 2005/038729 A1

(51) International Patent Classification[7]: G07C 9/00

(21) International Application Number:
PCT/US2004/033926

(22) International Filing Date: 15 October 2004 (15.10.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/512,461	16 October 2003 (16.10.2003)	US
10/870,475	16 June 2004 (16.06.2004)	US

(71) Applicant *(for all designated States except US)*: **SCM MICROSYSTEMS, INC.** [US/US]; 47211 Bayside Parkway, Fremont, CA 94538 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **MERKERT, Robert, J., Sr.** [US/US]; 21 Chippenham Drive, Voorhees, NJ 08043 (US).

(74) Agent: **GARRETT, ARTHUR, S.**; Finnegan, Henderson, Farabow, Garrett, & DunneR, L.L.P., 901 New York Avenue, NW, Washington, D.C. 20001-4413 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ACCESS CONTROL SYSTEM

(57) Abstract: An access system is disclosed that provides secured access to a security area. In some embodiments of the present invention, the access system includes an input device that is accessible to a user and capable of reading an authentication and/or identification information provided by the user; a standard signal control panel coupled to the input device for evaluation of the information provided by the user, the control panel being located in a secure area remote from the input device; and a signal processor coupled between the input device and the standard signal control panel, the signal processor being located in the secure area, wherein the input device provides data in a secured communication channel to the signal processor and the signal processor, in response to the data provided by the input device, provides the data to the standard signal control panel utilizing a standard signal. In some embodiments, the standard signal control panel may be a Wiegand or Magnetic-strip control panel. In some embodiments, the secured communications channel may be an RS422, RS485 or a TCP/IP protocol channel.

WO 2005/038729 A1

ACCESS CONTROL SYSTEM

DESCRIPTION

Related Applications

[001] This application claims priority to U.S. Provisional Application No. 60/512,461 filed Oct. 16, 2003, entitled "Access System" and U.S. Application No.10/870,475 filed June 16, 2004, entitled "Access System," which claims priority to Germany Application DE 20309254.6, filed on June 16, 2003 in Germany, all of which are herein incorporated by reference in their entirety.

Field of the Invention

[002] The present invention is related to access devices to provide physical access to a secured area and, in particular, to access devices compatible with current access control systems while providing higher levels of security.

Background of the Invention

[003] Secured access to sensitive areas has become an important issue, especially after the events of 11 September 2001. As such, there is a current focus on technological systems for controlling access to security areas in both the private and public arenas. Such systems must be made highly impervious to attack by those wishing to gain unauthorized access to the secured area.

[004] Security systems using, for example, Wiegand readers and control panels adapted to evaluate the data read from a Wiegand card are well known and widely employed in various applications like systems for unlocking doors or parking garage gates, etc. Usually, the Wiegand reader is located to be accessible to the user (Wiegand card holder) while the control panel, which after a positive evaluation of the

data, performs a security relevant operation (e.g. unlocking a door) is located in an area which is not accessible to the user, e.g. in a secure room, to guarantee a certain level of security.

[005] U.S. Patent 5,679,945 discloses an access system that provides an "intelligent" card reader in order to replace existing magnetic stripe readers, bar code readers and Wiegand readers without the need for retrofitting of existing computer systems, which are coupled to the existing readers. However, readers that utilize a standard signal for communication into a secured area are easily attacked by those seeking unauthorized access to the secured area. Therefore, access systems utilizing readers that provide standard signals (e.g., Wiegand, Mag Stripe, or bar-code standard signals) do not provide a high level of security because those signals are more susceptible to, for example, replay attacks. Replay attacks in a conventional access control system can be accomplished by an intruder gaining access to the communication wires. By capturing the data sent on a valid data transfer, the attacker can later replay the same data and gain unauthorized entrance.

[006] Therefore, there is a strong need, especially in a highly security conscious environment, to provide access systems with high levels of security against unauthorized access.

SUMMARY

[007] In accordance with the present invention, an access system is provided that includes an input device accessible to a user and capable of reading authentication and/or identification information provided by the user, and a standard control panel coupled to the input device for evaluation of the information provided by the user. The standard control panel can be located in a secure area remote from

the input device and can accept input signals compatible with those from standard signal readers that read traditional access cards, such as, for example, magnetic strip (Mag Stripe) cards, Wiegand cards, bar-code cards, etc. The input device can, for example, be a device that reads smart cards or memory cards, either contact or contactless. In some embodiments, the input device can also read inputted information from the user (user information) or data regarding the user (e.g., biometric data such as fingerprints).

An access system according to the present invention can include an input device that is accessible to a user and capable of reading authentication and/or identification information provided by the user; a standard signal control panel coupled to the input device for evaluation of the information provided by the user, the control panel being located in a secure area remote from the input device; and a signal processor coupled between the input device and the standard signal control panel, the signal processor being located in the secure area, wherein the input device provides data in a secured communication channel to the signal processor; and the signal processor, in response to the data provided by the input device, provides the data to the standard signal control panel utilizing a standard signal.

[008] These and other embodiments are further discussed below with respect to the following figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[009] Figure 1 shows a block diagram illustrating an access system according to the prior art.

[010] Figure 2 shows a block diagram of an embodiment of an access system according to the present invention.

[011] Figure 3 is shows a block diagram of embodiment of an access system according to the present invention.

[012] Figure 4 shows a block diagram of an embodiment of an access system according to the present invention.

[013] Figure 5 shows a block diagram of an embodiment of an access system according to the present invention that utilizes encrypted or signed, self-clocked data transmission.

[014] Figures 6A and 6B illustrate uni-directional and bi-directional data transmission, respectively.

[015] Figure 7 illustrates sample wave shapes for Wiegand signals, Mag-Stripe signals, and self-clocked di-phase signals.

[016] Figure 8 illustrates sample timing diagrams for self-clocked di-phase communication on Transmit and Receive data.

[017] Figure 9 shows a block diagram of a signal processor according to the present invention.

[018] Figure 10 shows a security system according to the present invention.

[019] Figure 11 illustrates relative security level based on combinations of various inputs requested of a user attempting to gain access.

[020] Figure 12 illustrates a three-factor card reader.

[021] Figure 13 illustrates other card readers.

[022] In the figures, elements having the same designation have the same or similar functions.

DESCRIPTION OF THE EMBODIMENTS

[023] Embodiments of the present invention provide an access system with an extremely high level of security. Embodiments of the invention include a signal processor coupled between the input device and the control device. The input devices in some embodiments can include encryption to encrypt information obtained from the user (i.e., from a memory or smart card, from input to a keypad, and/or from user data -- for example fingerprints). The signal processor, which can be placed in a secured location, can convert the encrypted information into a standard signal that can be sent to the standard control device, for example a standard Wiegand signal, magnetic strip signal, or strip-chart signal. Embodiments of the present invention, then, can be highly versatile because they can, for example, be utilized with Wiegand control panels without being restricted to Wiegand readers as input devices and without transmitting insecure Wiegand signals from the reader to a secured area.

[024] With the signal processor located in a secured location, for example at or near the control panel, the risk of interference with the data by those attempting to gain unauthorized access can be significantly reduced. A higher level of security can be guaranteed with regard to the data transfer from the input device to the control panel because it is not possible to intercept and abuse the authentication/identification information provided by the user if it is encrypted until it reaches the signal processor, especially if the signal processor and the control panel are located in a secure area which is not accessible from an unsecured area, and if a dynamic element is used in the data transfer. A second communication channel between the input device and the securely located signal processor can be provided. The input device can include a smart card reader into which a secure output can be implemented, for example an

RS422, an RS485 or a TCP/IP output protocol can be implemented in some embodiments.

[025] An access system according to some embodiments of the present invention may further include a host computer coupled to the input device and located remotely from the input device. The host computer may also be coupled to the control panel and the signal processor. Data may be transmitted between the input device and the host computer utilizing, for example, an RS485 or a TCP/IP protocol

[026] Figure 1 shows a block diagram of a prior art access system that includes a standard Wiegand reader 10 and a Wiegand control panel 12 adapted to retrieve data from standard Wiegand reader 10. The Control panel 12 is located in a secure area 14 remote from Wiegand reader 10, which is accessible to a user attempting to obtain access to a secure area. In order to gain access, the user inserts his Wiegand card (not shown), which contains authentication and, if required, identification information, into the Wiegand reader 10. The information is transmitted from the reader 10 to the control panel 12 where the information is evaluated. Depending on the result of the evaluation, the control panel 12 either performs a security relevant operation, e.g. unlocking a door or the like, to grant the user the requested access, or it denies access.

[027] The weak point in an access system such as that illustrated in Figure 1 is the link between Wiegand reader 10 and control panel 12. The Wiegand data lines are susceptible to replay attacks, i.e. data can be intercepted at the wiring going into secured area 14 and replayed to gain unauthorized entrance.

[028] Figure 2 shows an embodiment of an access system according to the present invention. A reader 16 is coupled to a signal processor 18. Signal processor

18 receives signals from reader 18 and converts these signals to standard signals that can be transmitted to control panel 12. In some embodiments, signal processor 18 and control panel 12 are physically located in a secured area 14. In some embodiments, control panel 12 can be a Wiegand control panel. It should be understood that the term "Wiegand control panel" is not restricted to a particular hardware configuration but rather includes any suitable control panel, which is capable of processing data signals in a Wiegand format by using corresponding signal processing or software. Additionally, although an embodiment utilizing a Wiegand control signal is described here, other control signal formats can also be utilized, for example magnetic strip (Mag Stripe) formats or bar-code formats.

[029] In the embodiment shown in Figure 2, the standard Wiegand reader 10 shown in Figure 1 is replaced by another input device, for example a smart card reader 16 into which a smart card (not shown) containing authentication/identification information can be inserted (for contact reading) or otherwise interfaced with (for example for contactless reading). Reader 16 can include an encryption circuit that encrypts the information read from the smart card and an output port, for example an RS422, an RS485 or a TCP/IP output port, for outputting data to signal processor 18. The embodiment of the access system shown in Figure 2 includes a signal processor 18 coupled between reader 16 and control panel 12. Signal processor 18 and control panel 12 can be co-located in secure area 14, which is remote from card reader 16.

[030] In some embodiments, card reader 16 can include a contactless reader for reading a contactless smart card. In general, embodiments of card reader 16 can include contactless smart card readers, contact smart card readers, memory card readers, a user input device such as a keypad on which a user can input

authentication/identification data, biometric devices such as a fingerprint or retinal scan reader for directly evaluating the identity of the user, and other signaling devices for communicating with the user.

[031] To begin operation of the embodiment of the access system shown in Figure 2, the user inserts a smart card into smart card reader 16, or in the case of a contactless smart card brings the smart card in close proximity to reader 16. The information on the smart card is read by reader 16. In some embodiments, the information from the smart card can be encrypted in reader 16. The information can then be transmitted to signal processor 18 using a secured, for example RS422, RS485 or TCP/IP protocol, output port. Data transfer between smart card reader 16 and signal processor 18, then, can be regarded as a "secure channel." Signal processor 18 converts the information received from reader 16 into a standard signal (e.g., a Wiegand signal, a bar code signal, or a magnetic stripe signal) that can be received by control panel 12. Control panel 12 is able to evaluate the standard signal and, based on access protocols, decides whether to allow or to deny access to the user.

[032] Figure 3 shows another embodiment of access system according to the present invention. The embodiment shown in Figure 3 includes reader 16, signal processor 18 and control panel 12 as was previously discussed with Figure 2. Further, a host computer 20 can be coupled to one or more of control panel 12, signal processor 18, and reader 16. Remote host computer 20 can be located outside secure area 14 and is coupled to reader 16 and to control panel 12. Communication between host computer 20 and reader 16 can be provided by a further secure channel, for example data can be transferred using an RS485 or a TCP/IP protocol.

[033] The operation of the embodiment of the access system of Figure 3 to gain access is similar to that described above with respect to Figure 2. However, the embodiment of access system shown in Figure 3 can easily be adapted to various requirements. For example, the secure channel between remote host computer 20 and reader 16 can be used to change the configuration of reader 16 on command from host computer 20 in a comfortable and secure manner. For example, differing levels of security can be implemented by sending commands to reader 16 and control panel 12 from host computer 20. Additionally, host computer 20 can be used to define the type of input devices from which correct identification data is obtained that are required to gain access. Suitable input devices that can be included in reader 16 include a contactless smart card reader, a contact smart card reader, PIN pads (or keypads), biometric devices (for example fingerprint or retinal readers), and combinations thereof. The input devices from which data is required in order to gain access can be changed as a function of security threat level, day of week, time of day, or other conditions. The coupling between host computer 20 and control panel 12 allows checking as to whether a control panel operation has been successfully executed. Further, host computer 20 can be used to identify a possible malfunction of control panel 12 by utilizing test signals.

[034] Additionally, reader 16 may include user-interface (for example a data screen or set of LED displays) for communicating information to a user. The LED signals may originate from control panel 12 and be transmitted through the secured channel between signal processor 18 and reader 16 as is indicated in Figure 3. Further, the secured channel between signal processor 18 and reader 16 may be bi-directional as is shown in Figure 3. In that case, control panel 12 may transmit data

and instructions to reader 16, for example regarding security levels and such, over a bi-directional secured line. Additionally, LED display data may be transmitted between control panel 12 and reader 16 over separate lines or through the bi-direction secured line. Control panel 12 may also communicate system status to reader 16 for display to a user directly without communicating through signal processor 18.

[035] Figure 4 illustrates an access system similar to that illustrated in Figure 3, except that the secured channel between reader 16 and signal processor 18 is a uni-directional line. Reader 16, then, cannot receive data from control panel 12 through the secured channel. In some embodiments, status information can be communicated between control panel 12 and reader 16 using a separate line. Status information can be displayed in reader 16 through LCD displays, LED lights, or audible tones, for example. As further shown in Figure 4, setup information can be transmitted to reader 16 separately. Setup information can include for example, which of the various input devices of reader 16 are activated in order to collect the appropriate information from the user to meet the current level of security.

[036] Figure 5 illustrates another embodiment of an access system according to the present invention. As has been discussed above, reader 16 is typically located in a non-secure area on the outside of a locked entranceway. Reader 16 can include interfaces for smart cards, contactless smart cards, biometric readers (e.g. fingerprint readers), PIN pads, and/or other user interface devices. Reader 16 transmits data which may be encrypted and/or digitally signed, extracted from a smart card or other input device to signal processor 18, which is located in secure area 14. In some embodiments, signal processor 18 can be located near or possibly in standard signal control panel 12.

[037] Digital signatures may be used to authenticate the information being sent to the control panel to ensure that it originated with the card or device that actually sent the information, and to ensure that the transmitted information was not altered after the information being transmitted was digitally signed.

[038] There exist many well-known processes for creating and validating digital signatures. One example is the Digital Signature Algorithm, which may be used by a *signatory* to generate a digital signature on data and by a *verifier* to verify the authenticity of the signature. Each signatory has a public and private key. The private key is used in the signature generation process and the public key is used in the signature verification process.

[039] To generate the correct digital signature for a signatory, knowledge of the private key of the signatory is needed. In other words, signatures cannot be forged, without knowledge of a signatory's private key. However, by using the signatory's public key, anyone can verify a correctly signed message.

[040] The Digital Signature Algorithm uses parameters denoted by p, q, g, and x, which are defined below:

p is an L-bit prime p, where $512 \leq L \geq 1024$, and L is divisible by 64;

q *is* a 160-bit prime q, such that q is a factor of p - 1, i.e. $(p - 1) = qz$, where z is any natural number;

h is chosen such that, $1 < h < p - 1$ and $g = h^z \bmod p > 1$;

x is chosen randomly such that $0 < x < q$ and $y = g^x \bmod p$.

The Public Key is y and the Private Key is x.

[041] To generate a digital signature, the algorithm also makes use of a one-way hash function, *SHA(m)*, such as, for example, the Secure Hash Algorithm,

and a randomly generated number k, where $0 < k < q$. Parameter k is regenerated for each time a signature is generated. Parameters x and k are used for signature generation and are kept secret.

[042] The Digital Signature (r,s) of a message M is the pair of numbers r and s computed according to the equations below:

$$r = (g^k \bmod p) \bmod q \qquad \text{and}$$

$$s = (k^{-1} SHA(M) + xr)) \bmod q.$$

[043] Prior to verifying the signature in a signed message, p, q, g and the sender's public key y and identity are made available to verifiers. These parameters may be publicly distributed. Additionally, the Digital Signature (r, s) is also made available along with its associated message M to potential verifiers.

[044] To verify the signature, the verifier first checks to see that $0 < r < q$ and $0 < s < q$; if either condition is violated, the signature is invalid.

[045] If these two conditions are satisfied, the verifier computes:

$$w = s^{-1} \bmod q;$$

$$u_1 = ((SHA(M)) * w) \bmod q;$$

$$u_2 = (rw) \bmod q; \text{ and}$$

$$v = ((g^{u1} * y^{u2}) \bmod p) \bmod q.$$

[046] If $v = r$, then the signature is verified. On the other hand, if $v \neq r$, then the message may have been modified and the signature should be considered invalid.

[047] In some embodiments, data sent from reader 16 to signal processor 18 can be clocked data or self-clocked data. As has been described above, signal

processor 18 converts the data received from reader 16 into a standard format signal, such as, for example, Wiegand, Mag Stripe, or bar code that is recognizable by standard signal control panel 12.

[048] In some embodiments, a host computer 20 can communicate with signal processor 18 and with reader 16 through signal processor 18. As discussed above, host computer 20 can, for example, vary the level of security or alter the action or display setup of reader 16.

[049] In some embodiments, a security module or processor is located in each of reader 16 and signal processor 18 to allow for the secure transfer of data between reader 16 and signal processor 18, either through encryption or digitally signing the data. In some embodiments, a dynamic element can be used in the data transmission process to ensure that a replay attack cannot be used to gain unauthorized access to an entrance portal through reader 16. Replay attacks in a conventional access control system can be accomplished by an intruder gaining access to the communication wires, between the output terminal of reader 10 (Figure 1) and the control panel 12. By capturing the data sent on a valid data transfer, the attacker can later replay the same data and gain unauthorized entrance. In some embodiments consistent with the present invention, the dynamic element could include date and time information corresponding to the date and time when the reader was accessed. The date and time information can be sent to the signal processor, which can then check the received information with the current date and time to ensure that the information sent is not a replay attack.

[050] In some embodiments, the secured communication channel between reader 16 and signal processor 18 can utilize the wiring that may be in place when

replacing a conventional access system, for example the Wiegand wiring. The existing two wires can be used for data and clock for one-way communication between reader 16 and signal processor 18 or bi-directional communication can be established using self-clocked data, for example non-return to zero (NRZ) or Di-phase communications. There are many advantages to using a bi-directional communication path between reader 16 and signal processor 18. Some of these include error retransmission capability, the ability to transmit status level information between control panel 12 to reader 16 via data signal processor 18, and general two-way communications for various other functions.

[051] Utilizing self-clocked NRZ or Di-phase communication between reader 16 and signal processor 18 allows for improved data detection and immunity to sporadic 'noise' signals generated by external sources on the data lines between reader 16 and signal processor 18. The technique employs the use of a sampling clock that is at a frequency of 8, 16, 32 or higher times that of the data transmission frequency. Multiple samples can be taken of the data line in each bit transmission in order to ascertain the data bit's true state. A plurality of clock signals indicating the same data status during the given bit time can be used to ascertain the state of the data bit. In some embodiments, both reader 16 and signal processor 18 can have independent sampling clocks running at the same higher frequency as that of the data bit frequency. In some embodiments, the data between reader 16 and signal processor 18 may be out of synchronization by only a few, for example one, clock cycle of the higher frequency clock.

[052] Di-phase communication can be used to further improve communication between reader 16 and signal processor 18. The state of the data is

changed on every data bit time period. If the data were in a high state it would be changed to a low state, and vice versa. A data 'one' is in the same state for the entire bit period. A data 'zero' changes state at the half-bit time. The value of the data bit is determined by comparing the state of the data bit during the first half of the data bit period and the second half of the data bit period. If the data state is the same in both half-bit times, the value of the data bit is a 'one'; if the data state is different in both halves of the bit time the data bit is a 'zero'.

[053] In some embodiments, reader 16 can change configuration on request from a host computer via a communications channel or from control panel 12 through status lines. In some embodiments, data signal processor 18 can receive configuration information from host computer 20 or from standard signal control panel 12 and can transmit the configuration data to reader 16 via the bi-directional data lines between signal processor 18 and reader 16. An example of configuration information being sent to reader 16 is a requirement for additional user inputs, such as card and PIN pad data; card, PIN pad and biometric data; or other combinations. Such security level changes may be sent as required based on time of day, day of the month, or National Security levels.

[054] Figures 6A and 6B illustrate uni-directional and self-clocked bi-directional data lines, respectively. Figure 6A shows how the Data out-0 line from the reader, such as from exemplary reader 16, is sent to the Signal Processor across the data channel interface. A signal arriving on the Data out-0 or D0 lines, at the Signal Processor is always interpreted as a "0". Figure 6B shows transmission of data using a self-clocked bi-directional line for the Data in-1 signal, across the data channel interface. Data transmitted by the Reader is buffered and sent to the Signal

Processor. Similarly, data transmitted by the Signal Processor is buffered and sent to the Reader. A signal arriving on the Data out-1, Data in-1 or D1 line at the Signal Processor is always interpreted as a "1".

[055] Figure 7 illustrates sample wave shapes for Wiegand (D0, D1), Mag Stripe (Clock and Data), and self-clocked Di-phase. The data being transmitted, shown in the Data row of Figure 7 is the 9-bit binary stream "110100101". As shown in Fig. 7, transmission of this data using Wiegand (D0, D1) depicted as W-D0 and W-D1 uses 9 clock cycles. Whenever a "0" is being transmitted during a clock cycle, the W-D0 line is asserted. If a "1" is being transmitted during a clock cycle, the W-D1 line is asserted. Thus, the W-D1 line is asserted during the first two clock cycles corresponding to the first two binary digits "11" of the 9-bit stream being transmitted. On the third clock cycle, the W-D0 line is asserted corresponding to the third digit ("0") of the binary stream. In the Mag Stripe (Clock and Data), as shown in Fig. 7, the Data line is asserted for "1's" and negated for "0's". Thus, the Data line is asserted for the first two clock cycles and then negated during the third clock cycle corresponding to the initial "110" data sequence of the 9-bit stream.

[056] In the Self-Clocked Di-phase scheme, if the line is held to a constant value over the entire clock period, then the data being transmitted is a "1". On the other hand, if the line value changes in the middle of the clock period the data being transmitted is a "0". Thus, the line is high for the entire first clock period, low for all of the second clock period, and changes in the middle of third clock period corresponding to the "110" data sequence. Figure 8 illustrates an example of self-clocked Di-phase communication, on transmit and receive data. Fig. 8 shows changes in the "Data Out" and "Data In" signals over 16 cycles of the base input clock, which

corresponds to the Bit Time or Bit Period. Changes in Data Out or Data In during the bit period indicate that a "0" is being transmitted whereas a constant value (0 or 1) for the entire period indicates that the data on the line is a "1".

[057] Figure 9 shows an embodiment of signal processor 18. The embodiment of signal processor 18 shown in Figure 9 includes a microprocessor 21 coupled to a reader communications switch 20 and a control panel data line switch 22. Further, microprocessor 21 may be coupled to a communications channel interface 23 for communications with host computer 20 and to a security access module (SAM) 24.

[058] Reader communications switch 20 can be coupled to one or more readers 16 of differing types through, for example, a bi-directional data communications channel. Further, data regarding each of the readers can be communicated to control panel 12 through control panel line switch 22. In some embodiments, data regarding the readers could include data regarding the status of the readers, such as whether they are active, inactive or malfunctioning.

[059] Conversion of data from reader 16 to a standard signal for standard signal control panel 12 can be accomplished in software operating on microprocessor 21 and stored in memory. In some embodiments, software operating on microprocessor 21 and stored in memory could implement portions of a digital signature verification and authentication algorithm. SAM 24 stores and implements encryption codes and, in some embodiments, can be removable using a "SAM lock".

[060] Figure 10 shows an example of a security system according to the present invention. A security system according to the present invention includes one or more access systems according to the present invention. Further, host computer 20

may include one or more workstations, such as an access control station, badging station, and guard workstation. As shown, control panel 12 communicates, through signal processor 18, with reader 16 and can open an appropriate door 30 once access is approved.

[061] In some embodiments of the invention, various levels of security may be programmed into control panel 12 and reader 16. For example, security levels may be classified with regard to threat level, for example low, guarded, significant, high, and severe. The level of authentication/identification required for each threat level may be different. For example, in a low threat security environment access may be gained with a contactless card. With a guarded level, the access system may be set to require both a contactless card and that the user input a personal identification number (PIN) into a keypad. With a significant threat, a contact card and a PIN may be required. In a high threat security level, a contact card and some biometric input (e.g., fingerprint) may be required to gain access. In a severe threat security level, three inputs -- a contact card, a PIN, and a biometric input -- may be requested of a user attempting to gain access. Figure 11 illustrates the relative security level with respect to various inputs and combinations of inputs requested of the user in a security system. In some embodiments, a single smart card may be configured to provide both contactless and contact connection with reader 16.

[062] Figure 12 illustrates a card reader that can be utilized in embodiments of the present invention. The embodiment of card reader shown in Figure 12 includes an LCD display, a keypad for accepting PIN information, a smart card reader, a contactless reader, and a fingerprint sensor. A series of LEDs can indicate security level. Further, an acoustic alarm may be included.

[063] Figure 13 illustrates other types of card readers that may be utilized with embodiments of the present invention.

[064] Although any standard formats may be utilized in embodiments of the present invention, in some embodiments, the contact card readers may be ISO 7816 card readers and the contactless cards may be ISO 14443, parts 1-4 with a FIPS 140-2 approved algorithm. Further, the card reader can be programmable, for example in order to extract SEIWG-12 data strings or other ID strings from a smart card.

[065] Several standards and working groups have been established in the area of access control. For example, the Security Equipment Integration Working Group has issued a specification on September 30, 2002: "Development of a specification for SEIWG-compliant Access Control Components; a study by the Security Equipment Integration Working Group," September 30, 2002, which is herein incorporated by reference in its entirety and made a part of this disclosure. Further, the Physical Access Interoperability Working Group has implemented a "Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems, Version 1.0," July 2, 2003, which is herein incorporated by reference in its entirety and made a part of this disclosure. Additionally, the Security Industry Association has issued an "Access Control Standard Protocol for the 26-Bit Wiegand Reader Interfaces," October 17, 1996, which is herein incorporated by reference in its entirety and made a part of this disclosure. The later document provides information regarding the Wiegand standard.

[066] Other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. For example, embodiments utilizing standards other than the Wiegand

standard for signaling between signal processor 18 and control panel 12 can be utilized. Additionally, other protocols may be utilized for secure transmission channels other than the RS422, RS485 or TCP/IP protocols described as examples here. It is intended that the specification and examples be considered as exemplary only, with a true scope and spirit of the invention being indicated by the following claims.

WHAT IS CLAIMED IS:

1. An access system, comprising:

an input device that is accessible to a user and capable of reading authentication and/or identification information provided by the user;

a standard signal control panel coupled to the input device for evaluation of the information provided by the user, the control panel being located in a secure area remote from the input device; and

a signal processor coupled between the input device and the standard signal control panel, the signal processor being located in the secure area,

wherein the input device provides data in a secured communication channel to the signal processor and the signal processor, in response to the data provided by the input device, provides the data to the standard signal control panel utilizing a standard signal.

2. The system of claim 1, wherein the data provided by the input device in the secured communication channel includes a dynamic element.

3. The method of claim 2, wherein the dynamic element is used to ensure that a replay attack cannot be used to gain unauthorized access to an entrance portal.

4. The system of claim 1, wherein the standard signal is chosen from a set consisting of Wiegand signals, Mag Stripe signals, and Bar Code signals.

5. The system of claim 1, wherein the signal processor is co-located with the control panel in the secure area.

6. The system of claim 1, wherein the input device includes a smart card reader.

7. The system of claim 1, wherein the input device includes a PIN pad.

8. The system of claim 1, wherein the input device includes a biometric device.

9. The system of claim 1, further including a host computer coupled to the input device and the standard signal control panel, the host computer communicating parameters to the input device and the standard signal control panel through secured channels.

10. The system of claim 1, wherein the communications channel is secured using at least one of the following methods:

encryption of the transmitted information; and/or

authentication of the transmitted information using a digital signature; and/or

the use of a dynamic element, shared by input device and the signal processor to protect against replay attacks.

11. The system of claim 1, wherein the input device communicates with the signal processor in a self-clocked non return to zero or Di-phase communication.

12. An access system comprising:

means for receiving authentication and/or identification information provided by a user;

means for securely transmitting the authentication and/or identification information provided by the user;

means for receiving the securely transmitted information; and

means for providing the received information to a standard control panel using standard signals; and

means for controlling access to a secured area based on the information received by the standard control panel.

13. The system of claim 12, wherein the authentication and/or identification information provided by a user includes at least one of smart card information, biometric information, or PIN information.

14. The system of claim 12, wherein means for receiving authentication and/or identification information provided by a user further includes means for combining additional dynamic information with the authentication and/or identification information.

15. The method of claim 14, wherein the additional dynamic information is based on temporal information generated contemporaneously with the authentication and/or identification information provided by the user.

16. The system of claim 12, wherein means for securely transmitting the authentication and/or identification information provided by the user further includes means for digitally signing and/or encrypting the information.

17. The system of claim 12, wherein means for receiving the securely transmitted information further includes means for decrypting and/or authenticating the received information.

18. The system of claim 12, wherein means for means for providing the received information to a standard control panel using standard signals further includes means for translating the received information to a format compatible with standard control panel inputs.

19. The method of claim 18, wherein the standard control panel inputs are chosen from chosen from a set consisting of Wiegand signals, Mag Stripe signals, and Bar Code signals.

20. An access method comprising:

receiving authentication and/or identification information provided by a user through an input device;

securely transmitting the authentication and/or identification information provided by the user;

receiving the securely transmitted information;

providing the received information to a standard control panel using standard signals; and

controlling access to a secured area based on the information received by the standard control panel.

21. The method of claim 20, wherein the authentication and/or identification information provided by a user through an input device includes at least one of smart card information, biometric information, or PIN information.

22. The method of claim 20, wherein receiving authentication and/or identification information provided by a user through an input device further includes combining additional dynamic information with the authentication and/or identification information.

23. The method of claim 22, wherein the additional information is generated by the input device.

24. The method of claim 22 wherein the additional dynamic information is based on temporal information generated contemporaneously with the authentication and/or identification information provided by the user.

25. The method of claim 20 wherein securely transmitting the authentication and/or identification information provided by the user further includes digitally signing and/or encrypting the information.

26. The method of claim 25, wherein the digital signing and/or encryption of the information is performed by the input device.

27. The method of claim 20, wherein the steps of receiving the securely transmitted information and providing the received information to a standard control panel using standard signals are performed by a signal processor.

28. The method of claim 20, wherein receiving the securely transmitted information further includes decrypting and/or authenticating the received information.

29. The method of claim 20 wherein providing the received information to a standard control panel using standard signals further includes translating the received information to a format compatible with standard control panel inputs.

30. The method of claim 29, wherein the standard control panel inputs are chosen from chosen from a set consisting of Wiegand signals, Mag Stripe signals, and Bar Code signals.

31. The method of claim 27, wherein the input device communicates with the signal processor using self-clocked non return to zero or Di-phase communication.

FIG. 2

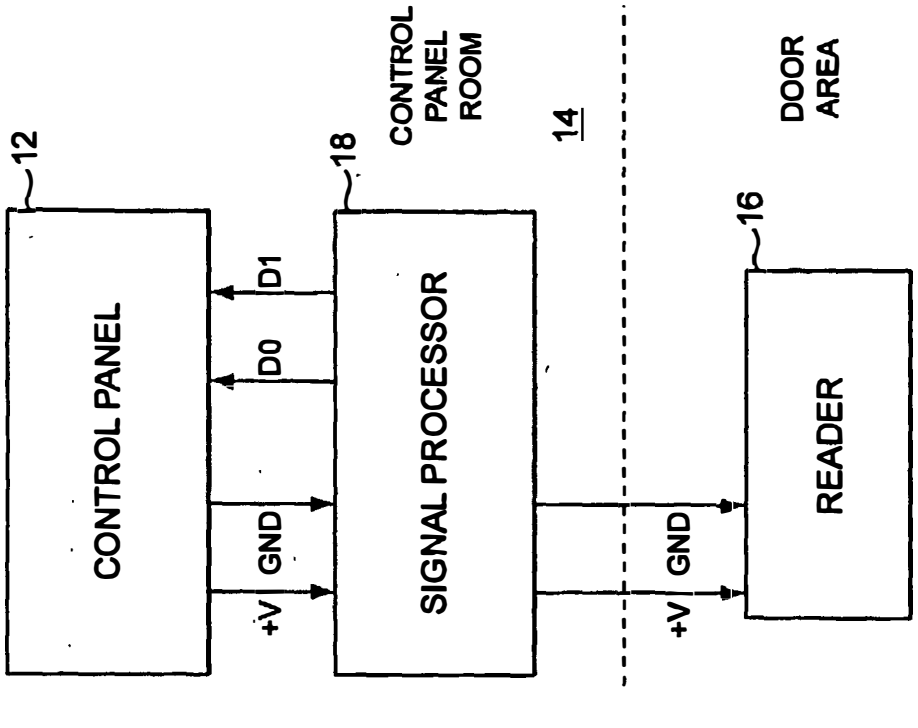
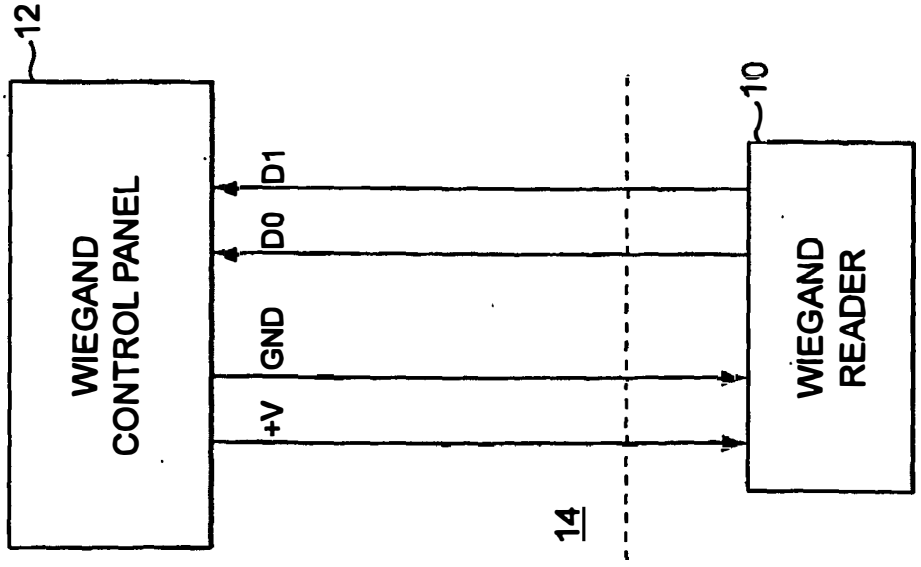


FIG. 1



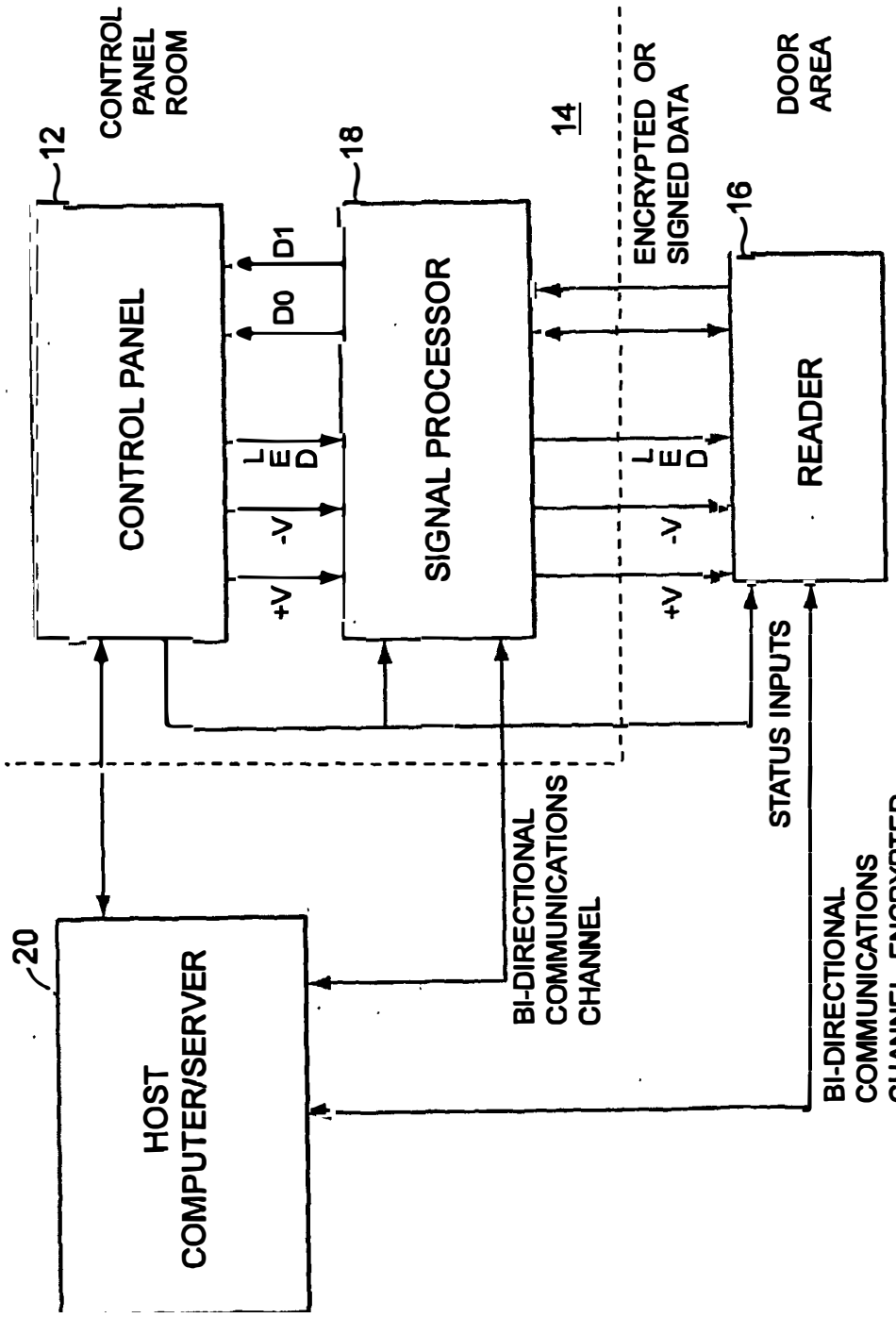


FIG. 3

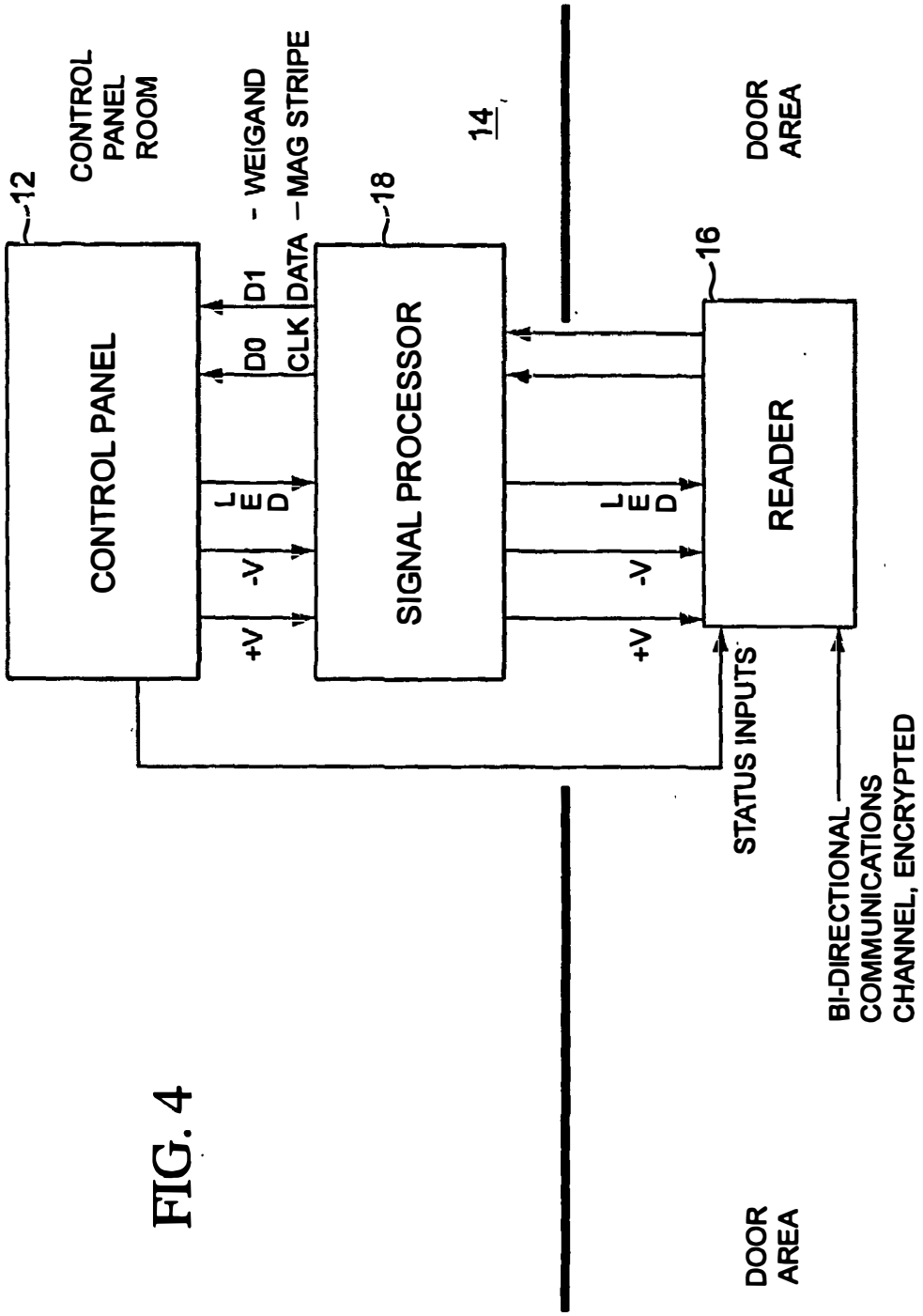


FIG. 4

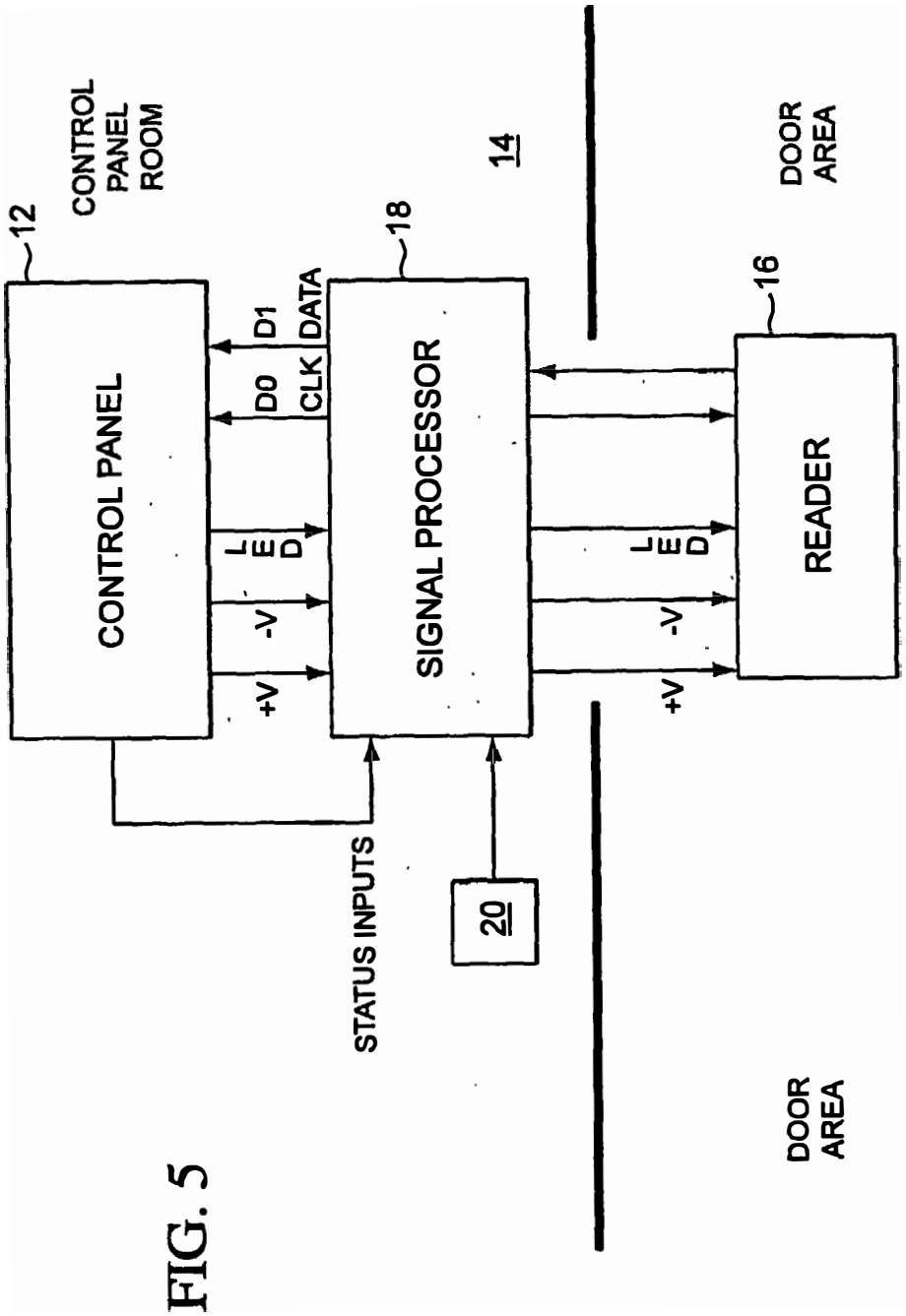


FIG. 5

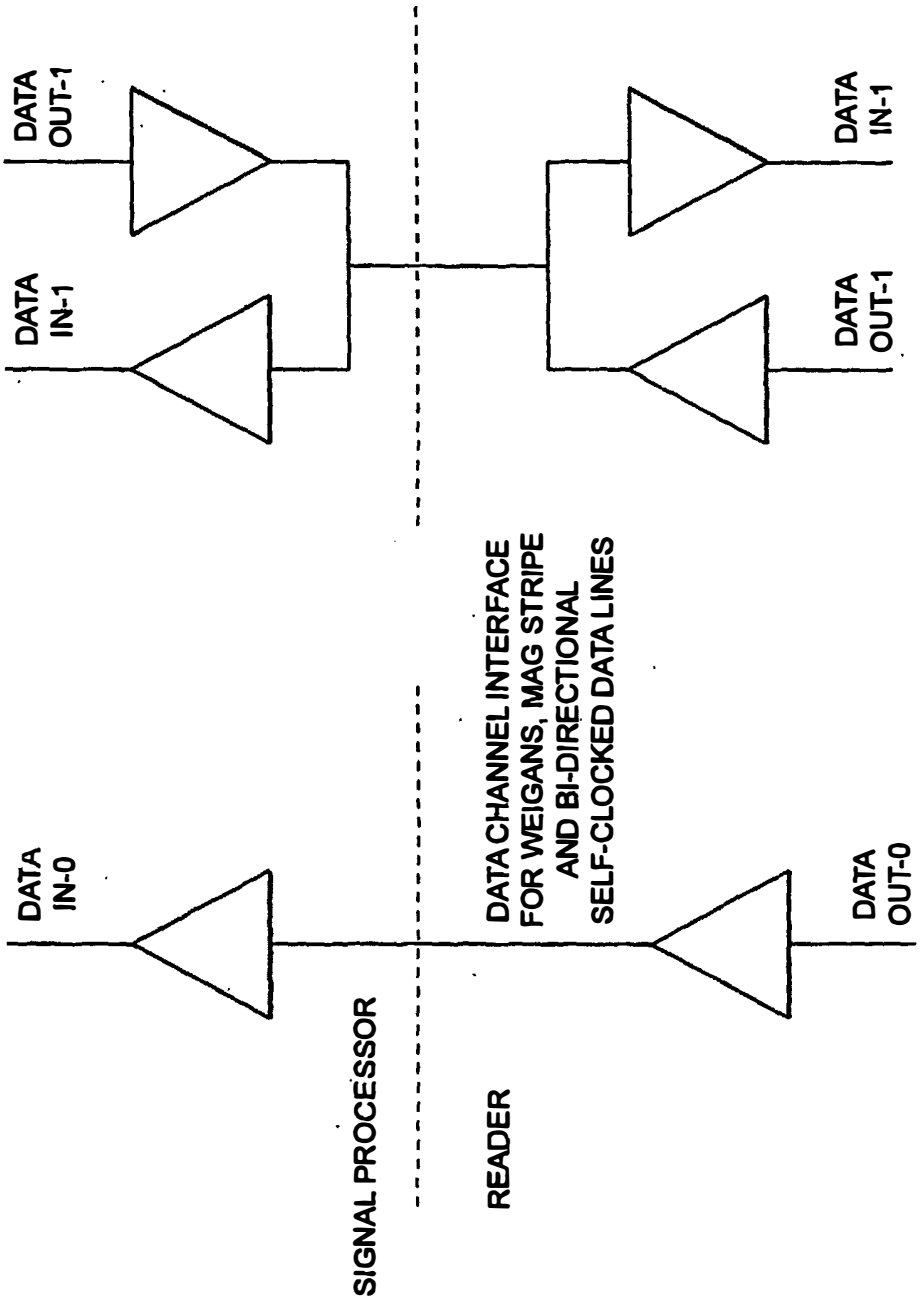


FIG. 6B

FIG. 6A

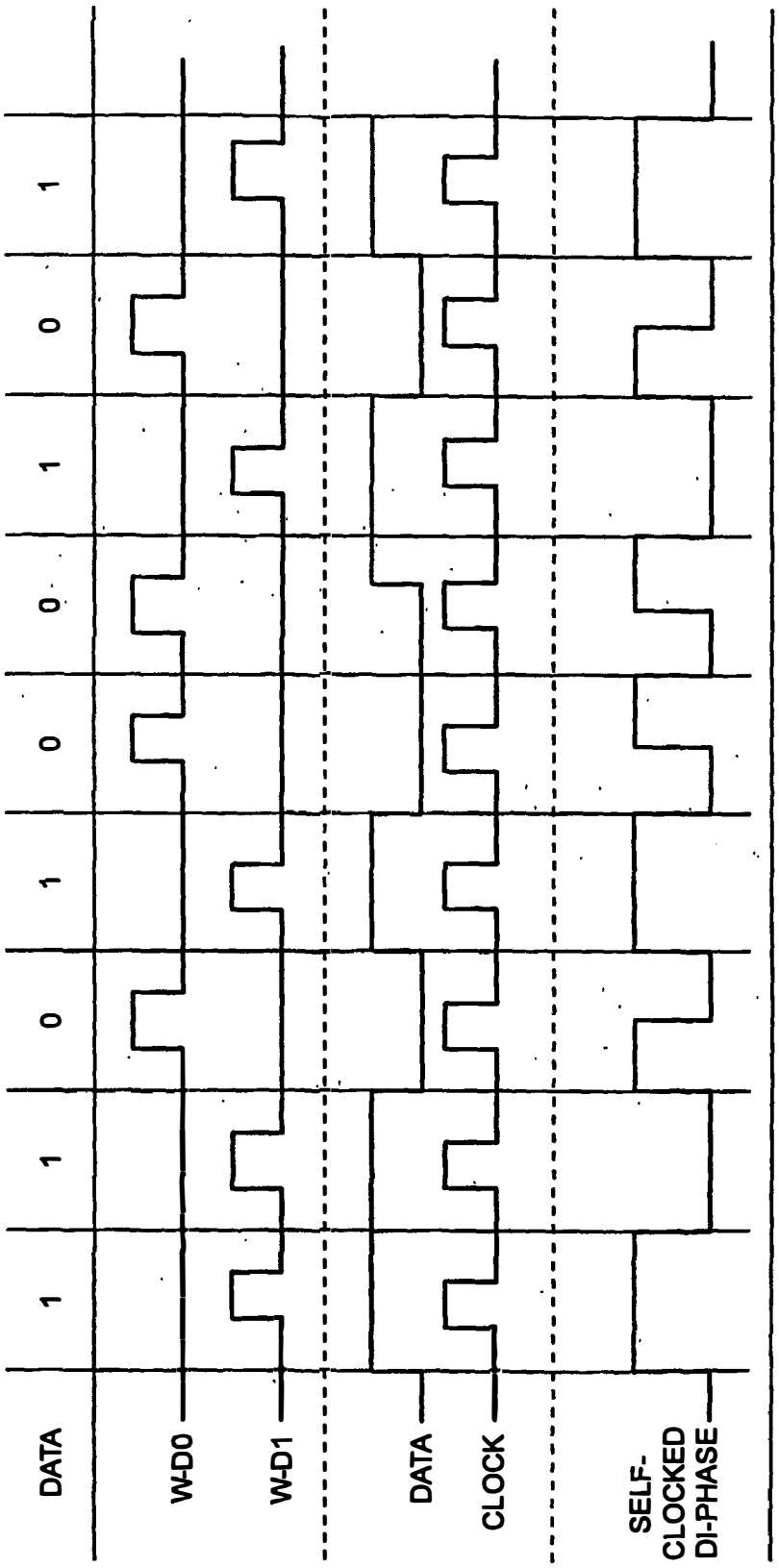
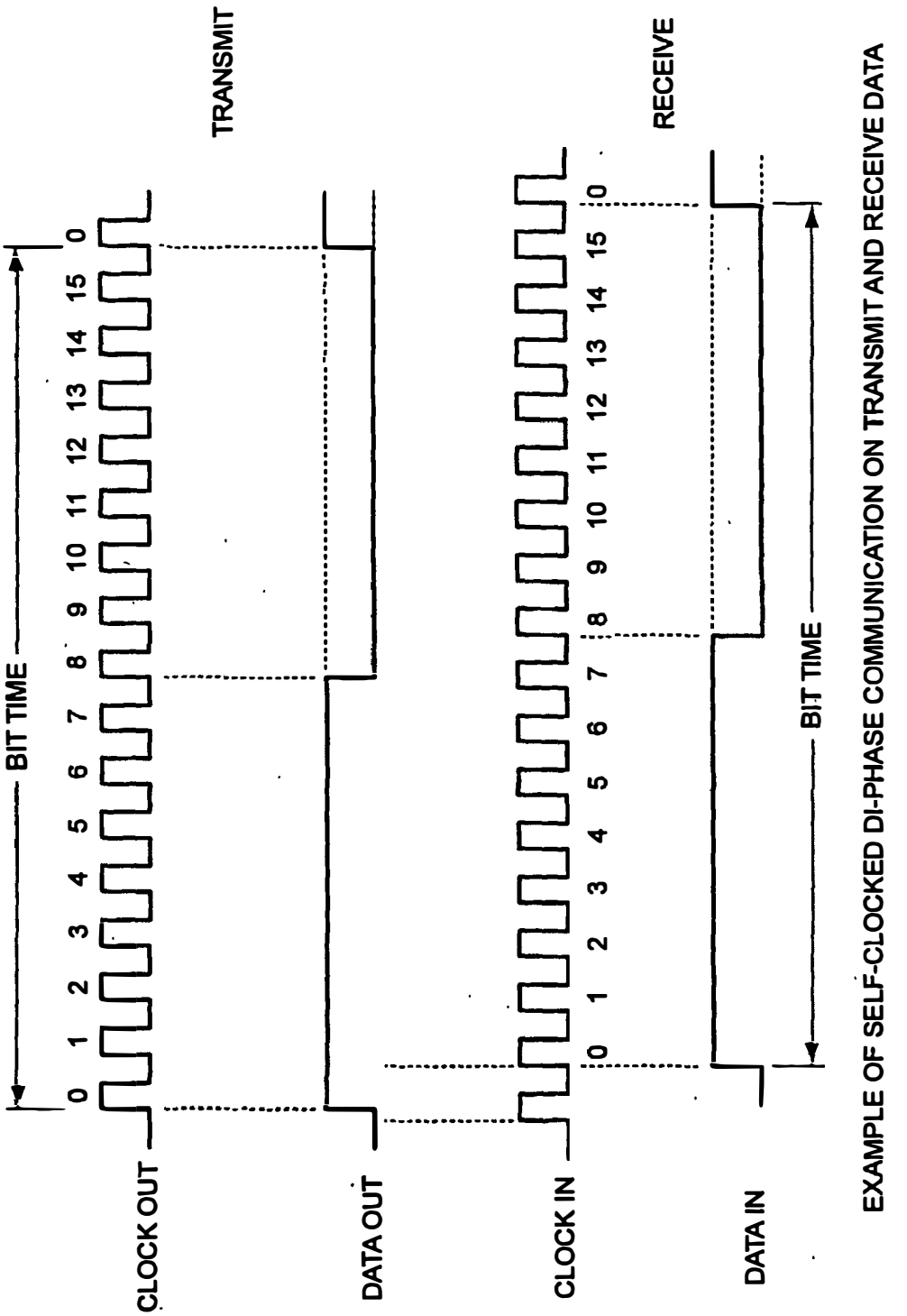


FIG. 7



EXAMPLE OF SELF-CLOCKED DI-PHASE COMMUNICATION ON TRANSMIT AND RECEIVE DATA

FIG. 8

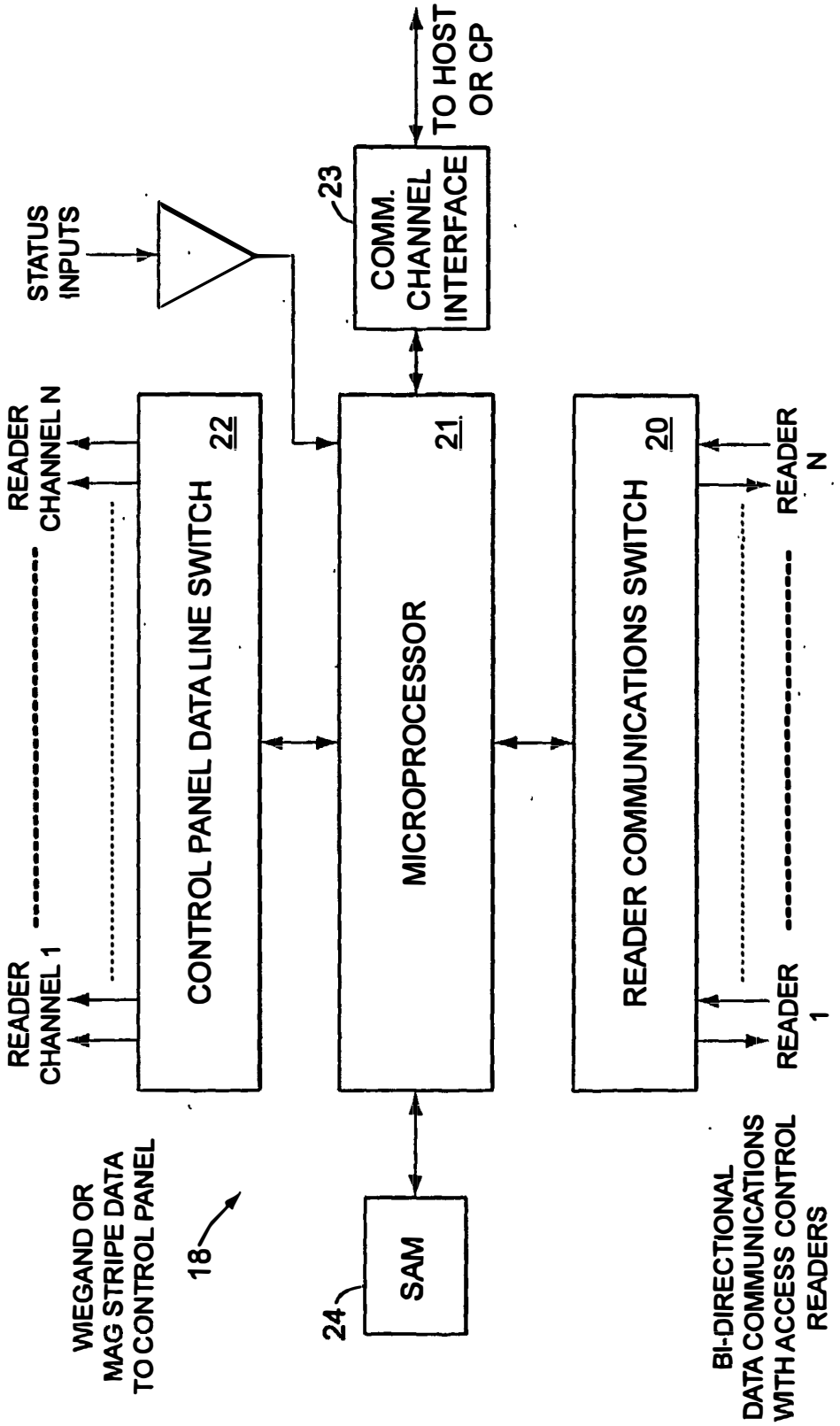


FIG. 9

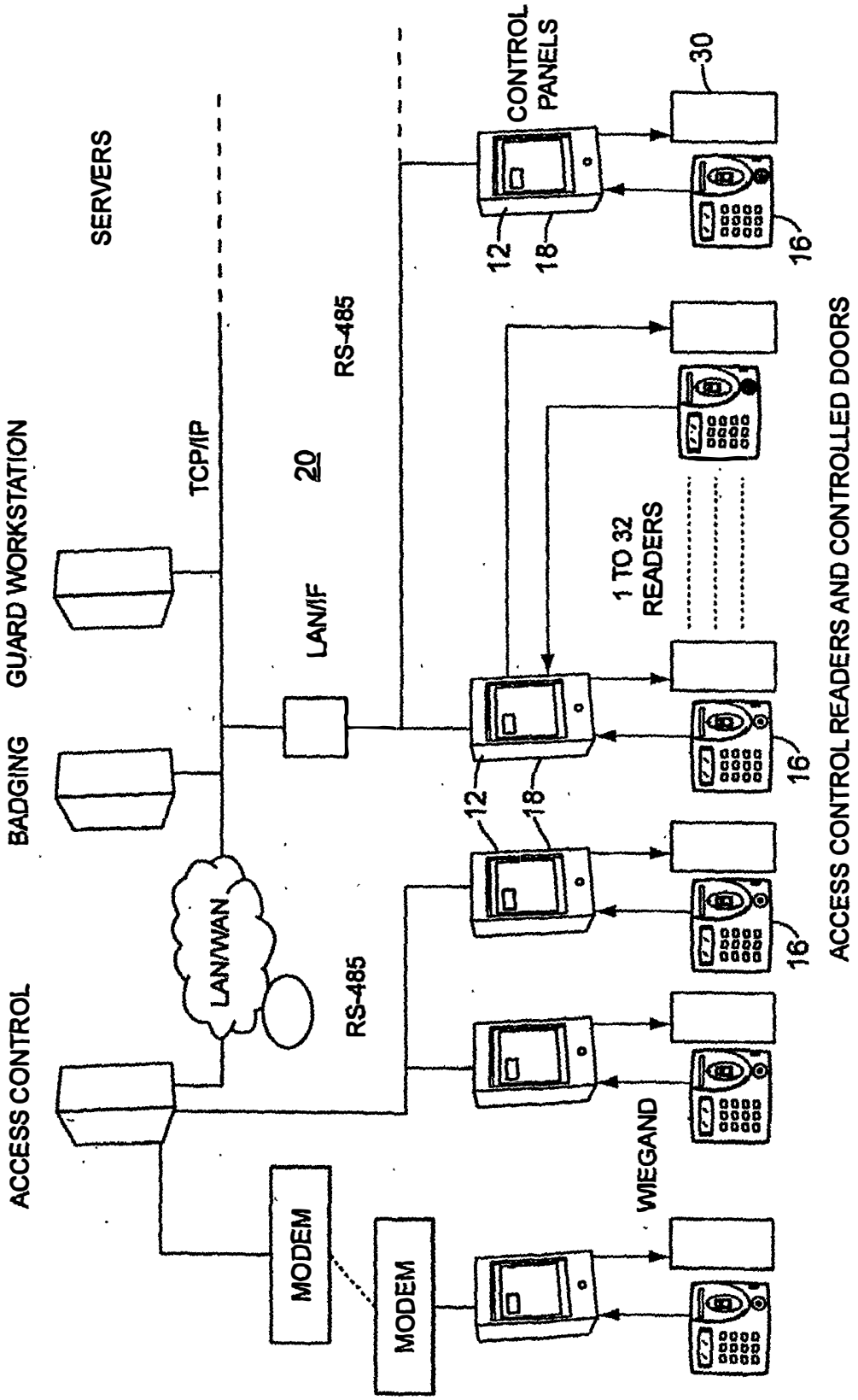


FIG. 10

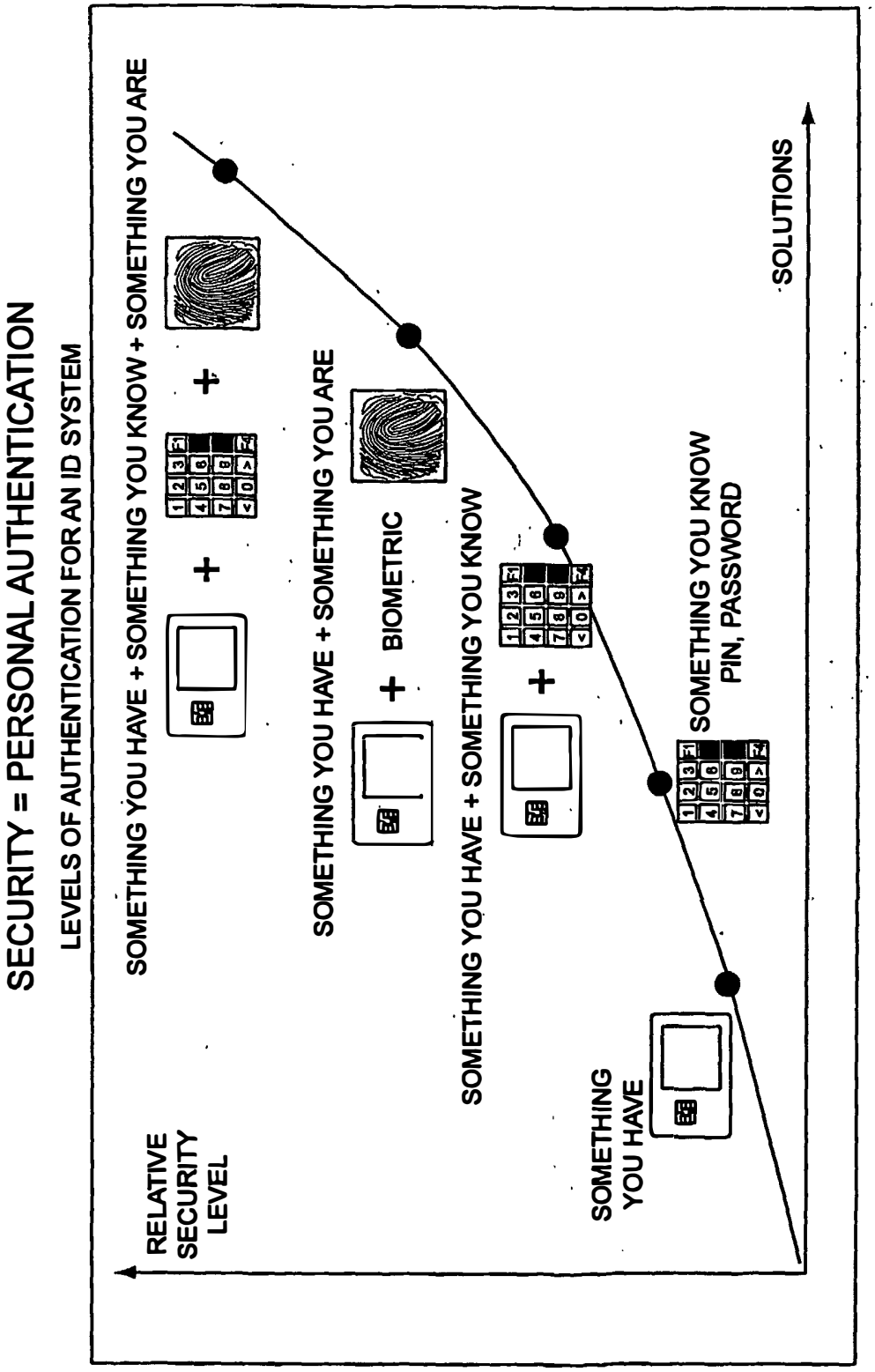


FIG. 11

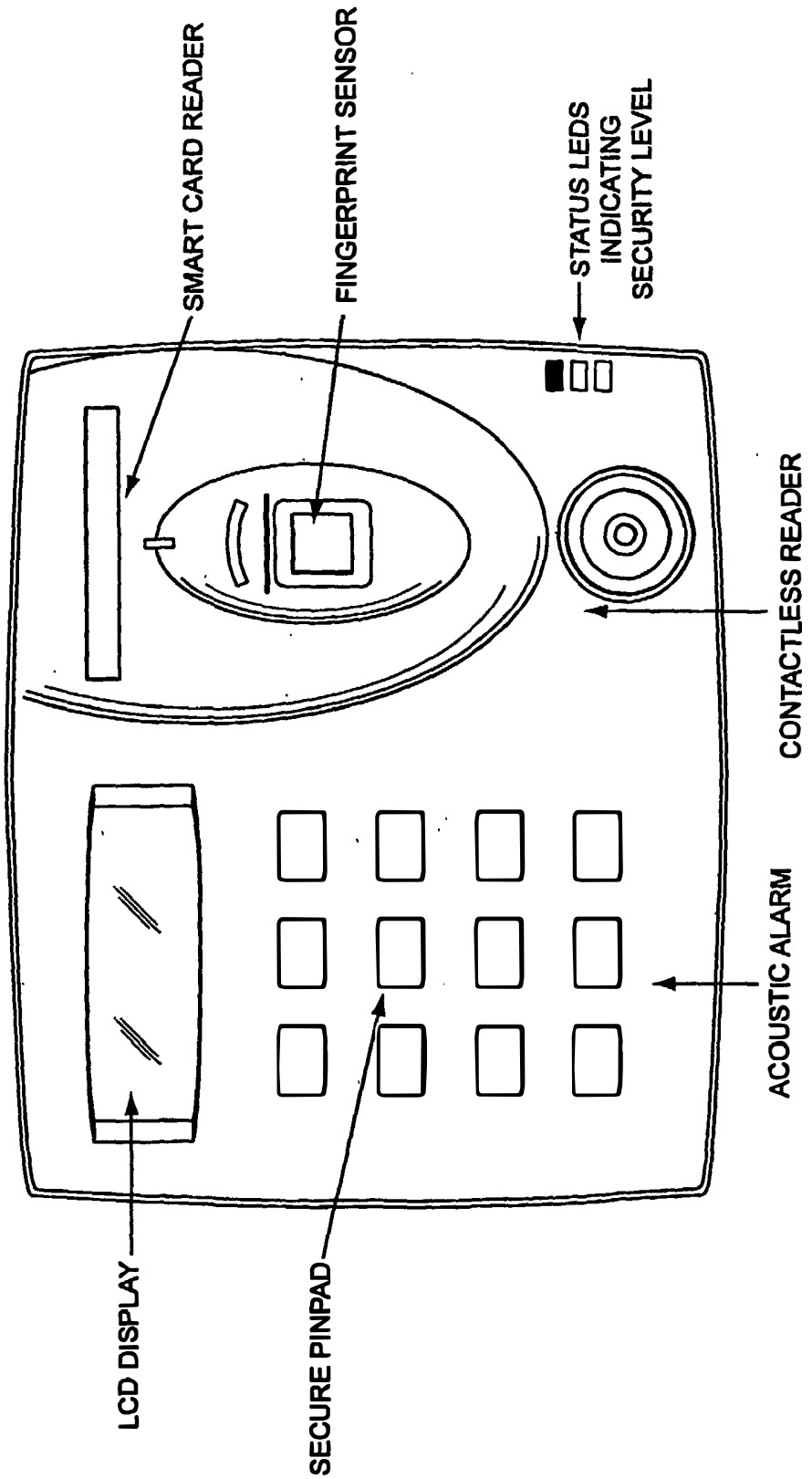


FIG. 12

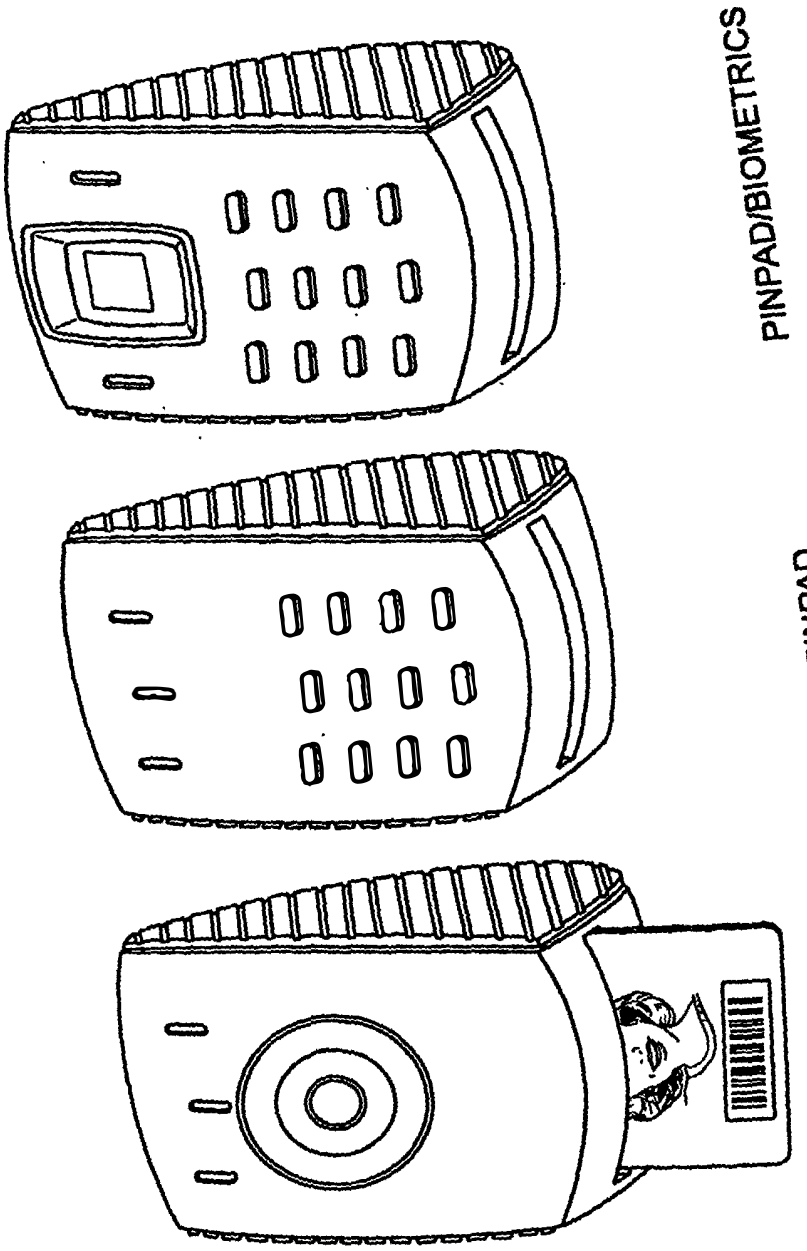


FIG. 13

INTERNATIONAL SEARCH REPORT

PCT/US2004/033926

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 679 945 A (RENNER ET AL) 21 October 1997 (1997-10-21) cited in the application figures 2,6	1-11, 20-31
A	US 2002/110242 A1 (BRUWER FREDERICK JOHANNES) 15 August 2002 (2002-08-15) paragraph '0008!	1-11, 20-31
A	US 6 532 298 B1 (CAMBIER JAMES L ET AL) 11 March 2003 (2003-03-11) column 16, line 56 - column 17, line 21	1-11, 20-31
A	US 5 995 630 A (BORZA ET AL) 30 November 1999 (1999-11-30) column 11, line 12 - line 24	1-11, 20-31

-/--

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

[X] Patent family members are listed in annex.

° Special categories of cited documents :

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

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

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 February 2005	24/02/2005

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

Form PCT/ISA/210 (second sheet) (January 2004)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2003/014642 A1 (MARTINSSON ROY ET AL) 16 January 2003 (2003-01-16) paragraph '0010!	1-11, 20-31
A	EP 1 237 091 A (FUJITSU LIMITED) 4 September 2002 (2002-09-04) paragraph '0028!	1-11, 20-31
A	WO 01/27723 A (HEWLETT-PACKARD COMPANY; VAMVAKAS, ATHANASIOS; PEARSON, SIANI; CHEN, L) 19 April 2001 (2001-04-19) page 2, line 1 - line 6 page 11, line 22 - page 12, line 26	1-11, 20-31

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5679945 A	21-10-1997	AU 5313896 A	16-10-1996
		CA 2217052 A1	03-10-1996
		WO 9630857 A1	03-10-1996
		US 6223984 B1	01-05-2001
US 2002110242 A1	15-08-2002	AU 2028602 A	01-07-2002
		EP 1354300 A2	22-10-2003
		WO 0250782 A2	27-06-2002
		ZA 200303622 A	21-06-2004
US 6532298 B1	11-03-2003	US 6483930 B1	19-11-2002
		US 6377699 B1	23-04-2002
		AU 6774200 A	17-04-2001
		WO 0120561 A1	22-03-2001
		AU 1615300 A	13-06-2000
		BR 9916864 A	21-08-2001
		CA 2350309 A1	02-06-2000
		EP 1153361 A1	14-11-2001
		JP 2002530976 T	17-09-2002
		NO 20012510 A	19-07-2001
		WO 0031679 A1	02-06-2000
		US 6424727 B1	23-07-2002
		US 2002131623 A1	19-09-2002
		ZA 200103797 A	10-05-2002
US 5995630 A	30-11-1999	WO 9838567 A1	03-09-1998
		EP 1012689 A1	28-06-2000
		CA 2198993 A1	07-09-1997
US 2003014642 A1	16-01-2003	AU 7695400 A	17-04-2001
		CN 1378667 T	06-11-2002
		EP 1228433 A1	07-08-2002
		JP 2003509771 T	11-03-2003
		WO 0120463 A1	22-03-2001
		EP 1480099 A2	24-11-2004
		SE 0001687 A	18-03-2001
EP 1237091 A	04-09-2002	WO 0142938 A1	14-06-2001
		EP 1237091 A1	04-09-2002
		US 2003005310 A1	02-01-2003
WO 0127723 A	19-04-2001	EP 1224518 A1	24-07-2002
		WO 0127723 A1	19-04-2001
		JP 2003511784 T	25-03-2003