



(43) International Publication Date
3 January 2014 (03.01.2014)

- (51) International Patent Classification:
G06F 17/30 (2006.01) *G06F 21/34* (2013.01)
- (21) International Application Number:
PCT/US2013/047679
- (22) International Filing Date:
25 June 2013 (25.06.2013)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
61/664,147 25 June 2012 (25.06.2012) US
- (71) Applicant: **XCEEDID CORPORATION** [US/US]; 500
Golden Ridge Road, Golden, CO 80401 (US).
- (72) Inventor: **CONLIN, Michael, T.**; 2907 West Yarrow
Circle, Superior, CO 80227 (US).
- (74) Agents: **ALLIE, John H.** et al.; Krieg DeVault LLP, One
Indiana Square, Suite 2800, Indianapolis, IN 46204 (US).
- (81) Designated States (*unless otherwise indicated, for every
kind of national protection available*): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,
BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,

DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR,
KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC,
SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) Designated States (*unless otherwise indicated, for every
kind of regional protection available*): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Published:

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the
claims and to be republished in the event of receipt of
amendments (Rule 48.2(h))

(54) Title: ACCESS CREDENTIAL READER CONNECTOR

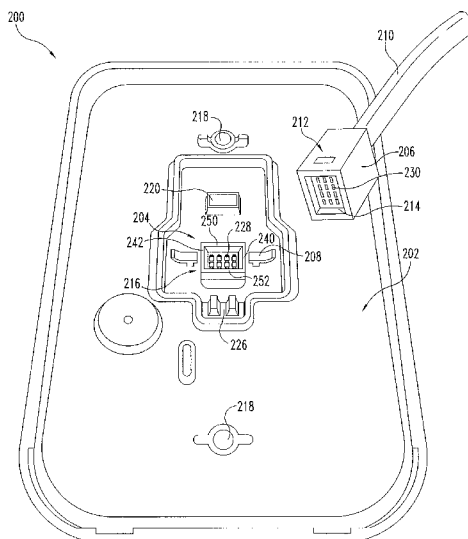


Fig. 2

(57) Abstract: An apparatus including a central access control system and an access reader. The access reader is structured to receive an access credential from the central access control system, and includes a first connector connected with a second connector with the second connector connected to a cable, and with the cable in electronic communication with the central access control system. Connection of the first connector and the second connector places the access reader in electronic communication with the central access control system.

ACCESS CREDENTIAL READER CONNECTOR

CROSS REFERENCE TO RELATED APPLICATIONS

The present application claims the benefit of U.S. Provisional Patent Application No. 61/664,147 filed June 25, 2012, the contents of which are incorporated herein by reference in their entirety.

TECHNICAL FIELD

The present invention relates to access control systems, and more particularly, but not exclusively, to the installation of a wall mounted access credential reader.

BACKGROUND

The current practice for installation of an access credential reader includes soldering a pigtail harness into the reader while leaving several bare wires exposed for connection to wiring in a structure. Typically, an installer attaches one of the bare wires to a corresponding wire from the structure, then hangs the reader from the wire while connecting the remainder of the wires to the corresponding wires from the structure. This approach is time consuming, cumbersome, and can result in loose connections and/or marring of the reader or adjacent structures. Accordingly, there remains a need for further contributions in this area of technology.

SUMMARY

One embodiment of the present invention is directed to a unique wiring connection for an access reader. Other embodiments include apparatuses, systems, devices, hardware, methods, and combinations for connecting an access reader to wiring located within a structure. Further embodiment, forms, features, aspects, benefits, and advantages of the present invention shall become apparent from the description and figures provided herewith.

DESCRIPTION OF THE DRAWINGS

Features of the invention will be better understood from the following detailed description when considered in reference to the accompanying drawings, in which:

FIG. 1 is a schematic illustration of an access control system.

FIG. 2 is a view of an embodiment of an access reader including a connector.

FIG. 3 is a view of an embodiment of an access reader including a backplate.

FIG. 4 is a view of an embodiment of an access reader assembly.

DETAILED DESCRIPTION

For purposes of promoting an understanding of the principles of the invention, reference will now be made to the embodiments illustrated in the drawings and specific language will be used to describe the same. It will nevertheless be understood that no limitation of the scope of the invention is hereby intended, any alterations and further modifications in the illustrated device, and any further applications of the principles of the invention as illustrated therein being contemplated as would normally occur to one skilled in the art to which the invention relates.

Referring to FIG. 1, shown therein is a conventional access control system 100 according to one form of the invention. System 100 includes a central access control 120 and a number of access control devices 140a, 140b. The central access control 120 is associated with an access control database 130 and a credential production system 110 that serves to generate access credentials. In a typical scenario, the central access control 120, the credential production system 110, and the access control database 130 are maintained by security personnel. The security personnel maintain the access control database 130 as a list of all persons authorized to enter various access points 150a and 150b on the premises. The access information associated with each person is gathered from the access control database 130 and is programmed into a blank access credential such as, for example, a smart card or proximity card, using access credential production system 110. Additionally or alternatively, the access production system 110 can be utilized to generate one or more access input codes, with each access input code being assigned to an individual or individuals, to be stored in the access control database 130. This programmed access

credential or input code can then be used to access one or more of access points 150a, 150b via presentation to respective access control devices 140a, 140b which can be a card reader and/or a keypad mounted proximate to an access controlled door.

In the system 100, the individual access control devices 140a, 140b are configured to read access credentials. In response to a correct credential being presented to the access control devices 140a, 140b, an actuator (not shown) can be activated which is associated with the respective access points 150a, 150b. To make the determination to activate an actuator and thereby grant access, the access control device 140a, 140b reads the access credential and then transmits the credential or information derived from the credential to the central access control 120 where a look up function is performed. The lookup function can include accessing the access control database 130 to determine whether a credential presented at a given access control device 140 is authorized for accessing the access point 150 associated with the access control device 140. A message indicating the authorization status can be sent from the central access control 120 back to the access control device 140. In instances where the authorization is positive, the access control device 140 can communicate with the actuator of the access point 150 to grant the user access. Alternatively, the message indicating a positive authorization can be sent directly to the actuator of the access point 150 without passing through access control device 140. Other information may be transmitted between the access control device 140 and the central access control 120 to further enhance the integrity of the access control system 100, for example error codes indicating tampering, power failures, etc.

Referring to FIG. 2, shown therein is a rearward view of one embodiment of an access reader 200. The access reader 200 includes a case or housing 202. The housing 202 houses a printed circuit board (not shown) and other associated electronics (not shown) such that the reader 200 can receive and/or interpret one or more inputs from a card, keypad or other device, can communicate with and/or receive communications from the central access control 120, and/or can perform other desired functions. The access reader 200 can receive various inputs, such as from a multi-frequency smart card, a proximity card, and/or other radio-frequency identification (RFID) cards, devices, fobs, etc., examples of which are disclosed in commonly-owned U.S. Patent Application Publication No. 2011/0115603 filed November 10, 2010, the contents of which are incorporated herein by reference. The access reader can further receive inputs from a keypad, keyboard, or other types of data input devices.

The access reader 200 further includes a connector 204 in electronic communication with electronics (not shown) inside the housing 202. The connector 204 is structured to be connected to another connector or wiring harness 206. The wiring harness 206 is connected to a cable 210. The cable 210 includes a plurality of wires or leads across which electronic communications or signals are transmitted. Electronic communications/signals can include analog or digital signals, data, electric current or voltage, various waveforms, credentials, inputs or outputs, and/or any other forms of electrical communications or signals. Each of the plurality of wires within the cable 210 can be connected to an individual receiving member or pin 230 within the harness 206.

The cable 210 can be connected to the central access control 120 and a power source, among other possible connections for the cable 210. The cable 210 can be a

dedicated access cable to provide power and electronic communication to the access reader 200. The cable 210 can pass through portions of a structure, such as through walls, conduit, etc., in order to provide electronic communications and signals to/from the access reader 200 and the central access control 120.

The connector 204 mates with the wiring harness 206 in a manner such that electronic communications/signals pass therethrough. In one form, the harness 206 includes a plurality of receiving members or pins 230 structured to receive a plurality of receiving members or pins 228 located in the connector 204. It is contemplated that the connector 204 can include a plurality of pins 228 to be received by a plurality of receiving members 230 in the harness 206, or the connector 204 can alternatively include a plurality of receiving members which receive a plurality of pins in the harness. The plurality of pins 228 can be raised from a surface of the housing 202 or can be flush with the housing 202, and the receiving members 230 can be recessed to receive the plurality of pins 228 or can be flush with a housing of the harness 206. It is contemplated that the pins 228 and the receiving members 230 can take any form such that upon connection of the harness 206 to the connector 204, electronic communications/signals can pass between the pins 228 and the receiving members 230.

Additionally, the connector 204 and the harness 206 can include any number of pins 228 and receiving members 230 depending upon the application and the extent of electronic communications/signals to be transferred from or received by the access reader 200. In various forms, the connector 204 and harness 206 can include between four to twelve pin connections. In one specific form, the cable 210 includes twelve

discrete wires, each connected to a corresponding one of the receiving members 230. In this form, the connector 206 can include a 4x3 array of pins 228, and the harness 206 can include a corresponding 4x3 array of receiving members 230, thereby forming a twelve pin connection as illustrated in FIG. 2. An illustrative example of electronic communications/signals transmitted across each wire/pin 228/pin receiving member 230 is shown in Table 1 below.

Pin #	Function
1	Z(485)/unused
2	Power
3	Ground
4	Red LED
5	Y(485)/unused
6	Ground
7	Not used
8	Tamper
9	Data 0
10	Beeper
11	Data 1
12	Green LED

Table 1

The connector 204 and the wiring harness 206 are retained in such a manner as to prevent a break in the electronic communication between the pins 228 and the receiving members 230. In one form, a projecting walled structure 216 surrounding the plurality of pins 228 is raised and is configured to be received within a recess 214 in a housing of the harness 206. The walled structure 216 can include sidewalls 240, 242 which are shorter than the sidewalls 250, 252. The sidewalls 240, 242, 250, and 252 can engage in a plurality of corresponding recesses (not shown) or a single recess 214

in the harness 206 so as to form a protective boundary to effectively isolate the electrical contacts from degradation due to environmental effects. In one specific form, the sidewall 252 can include a slot to align with a corresponding tab within the harness 206 to provide a keying feature (not shown) structured to permit the harness 206 and connector 204 to mate in a single direction/orientation. The connector 204 can additionally or alternatively be retained in secure engagement with the harness 206 via one or more clips 208. The clips 208 are configured to lockingly engage with one or more corresponding recesses or notches 212 in the harness 206. The clips 208 can be tapered inwardly such that as the harness 206 is pressed onto the connector 204, the clips deflect outwardly and then snap back to engage the recess 212.

The singular connection between the connector 204 and the harness 206 can complete all the electrical connections necessary to place the access reader 200 into communication with the access control system 100. This connection can provide power to the access reader 200, place the access reader 200 in electronic communication with the central access control 120, provide credential inputs from the access reader 200 to the central access control 120, provide updates from the central access control 120 to the access reader 200, and/or can provide other types of electronic communications or signals to the access reader 200.

The housing 202 can further include a magnetic swipe reader connector 220. A magnetic swipe reader (not shown) can be integrated with the access reader 200. In other forms, the magnetic swipe reader can be mounted near or on an outer housing of the access reader 200. The magnetic swipe reader may be placed in electronic communication with the access reader 200 through the magnetic swipe reader

connector 220. As discussed above regarding other inputs, a magnetic swipe reader input can be communicated from the access reader 200 through the connectors 204, 206, across the cable 210, and to the central access control 120.

The housing 202 can further include a tamper detector 226. In one embodiment, the tamper detector 226 can be an optical sensor 226, a magnetic sensor, a motion sensor, or any other sensor or detector 226 that is operable to detect movement of the housing 202 relative an object to which the housing 202 is retained, such as a backplate. The tamper detector 226 can communicate a tamper signal from the access reader 200 to the central access control 120 or to an alarm (not shown). The housing 202 can include one or more mounting holes 218 to retain the housing 202 to the backplate 308, as illustrated in FIG. 3.

Referring to FIG. 3, the housing 202 can be retained to a backplate 308. The backplate 308 includes a hole of sufficient size to permit the harness 206 to pass therethrough to connect with the connector 204 of the access reader 200. The backplate 308 can be mounted directly to a wall 304 or to a gang box 306 inserted into an opening or recess in the wall 304. Although FIG. 3 illustrates the backplate 308 as being coupled to the access reader 200 prior to installation of the backplate 308 to the wall 304, in another embodiment, an installer can set the access reader 200 aside, pull the harness 206 through the hole 310 in the backplate 308, and then install a plurality of screws 312 extending through holes 314 either directly into the wall 304 or into screw receiving openings 302 in the gang box 306, thereby attaching the backplate 308 to the wall 304. An installer can then grasp the access reader 200, connect the harness 206 to the connector 204, push any excess cable 210 into the gang box 306 or the wall 304,

and attach the access reader 200 to the backplate 308. The backplate 308 can cover the backside of the housing 202 and can extend onto a side wall of the housing 202. The backplate 308 can further include a sensing pad, optic tape, or other device (not shown) to cooperate with the tamper detector 226 and allow the tamper detector 226 to detect movement of the housing 202 relative the backplate 308.

Referring now to FIG. 4, various stages of assembly of the access reader 200 are illustrated. The backplate 308 is illustrated as being attached to the wall 304, with the harness 206 and a portion of the cable 210 extending through the hole 310 of the backplate. Upon connection of the connector 204 to the harness 206, the access reader 200 can be retained to the backplate 308. The access reader 200 can be retained to the backplate 308 through a plurality of screws, such as screws 312 which extend through a portion of the access reader 200 and into the backplate 308. A plurality of clips, retainers, or any other suitable retention device can be used to retain the access reader 200 to the backplate 308. The assembly can also include a coverplate 404 which can cover a portion of the housing 202 and any fasteners which retain the housing 202 to the backplate 308. The coverplate 404 can be retained to the access reader 200 via a fastening device such as, for example, a clip 406, a clip 406 and a screw, a plurality of screws, a plurality of clips, or any other fastening devices capable of attaching the coverplate 404 to the access reader 200.

FIG. 4 further illustrates that the access reader 200 can include a plurality of keys, such as in the form of keypad 402, to permit a user to enter a numeric, alphabetic, or other inputs into the access reader 200, as an alternative or in addition to the use of a card including a credential as aforementioned. The access reader 200 can additionally

include a plurality of features including lights (such as LED lights to indicate when access has been granted, denied, or if a card is in proximity to the access reader 200), a beeper (to indicate if access has been granted or denied), an alarm (to indicate if the tamper sensor 226 has detected motion or other tampering), or any other suitable features and/or devices which would be deemed desirable for inclusion within the housing 202.

While the invention has been described in connection with what is presently considered to be the most practical and preferred embodiment, it is to be understood that the invention is not to be limited to the disclosed embodiment(s), but is instead intended to cover various modifications and equivalent arrangements included within the spirit and scope of the appended claims, which scope is to be accorded the broadest interpretation so as to encompass all such modifications and equivalent structures as permitted under the law.

Furthermore it should be understood that while the use of the word preferable, preferably, or preferred in the description above indicates that feature so described may be more desirable, it nonetheless may not be necessary and any embodiment lacking the same may be contemplated as falling within the scope of the invention, that scope being defined by the claims that follow. In reading the claims, it is intended that when words such as "a," "an," "at least one" and "at least a portion" are used, there is no intention to limit the claim to only one item unless specifically stated to the contrary in the claim. Further, when the language "at least a portion" and/or "a portion" is used, the item may include a portion and/or the entire item unless specifically stated to the contrary.

CLAIMS

What is claimed is:

1. A system, comprising:

a central access control in electronic communication with an access control database, the access control database including an access credential;

a wiring harness;

an access reader including a housing, the housing including a connector structured to receive and retain the wiring harness, wherein the access reader is further structured to receive an input;

wherein the access reader is structured to electronically communicate the input through the connector and the wiring harness to a cable, the cable being electronically coupled to the wiring harness, wherein the input is communicated to the central access control through the cable; and

wherein the central access control compares the input with the access credential to verify access.

2. The system of claim 1, wherein one of the connector and the wiring harness is a male pin adaptor and the other of the wiring harness and the connector is a female pin receiver.

3. The system of claim 1, further comprising a backplate structured to be fastened to one of a wall or a gang box, the backplate including an aperture structured to permit the wiring harness to pass therethrough for connection to the connector, wherein the

backplate is structured to retain the housing to the backplate after the wiring harness has been engaged with the connector.

4. The system of claim 1, further including a tamper sensor located in a portion of the housing.

5. The system of claim 1, wherein the access reader is structured to receive the input from an RFID card.

6. The system of claim 1, wherein the housing further includes a keypad and wherein the access reader is structured to receive the input from the keypad.

7. The system of claim 1, wherein the housing further includes a clip located in juxtaposition to the connector, wherein the clip is structured to be received by a notch in a housing of the wiring harness.

8. A method, comprising:

connecting a wiring harness to a cable, the cable including a plurality of wires, wherein connecting the wiring harness to the cable includes placing at least one of the plurality of wires in electronic communication with the wiring harness, wherein the at least one of the plurality of wires is in electronic communication with a central access control; and

coupling the wiring harness to a connector located in a housing of an access reader, whereby the access reader is placed in electronic communication with the central access control.

9. The method of claim 8, further including:

inserting the wiring harness through an aperture in a backplate;

fastening the backplate to one of a gang box and a wall, wherein the cable extends from an interior cavity of the wall outwardly through the one of the gang box and the wall; and

coupling the access reader to the backplate.

10. The method of claim 9, further including positioning a tamper detector within the housing adjacent a portion of the backplate upon coupling the access reader to the backplate.

11. The method of claim 8, wherein placing at least one of the plurality of wires in electronic communication with the wiring harness further includes placing between four to twelve wires in electronic communication with the wiring harness, wherein the connector is structured to receive independent electronic communication from the four to twelve wires.

12. An apparatus, comprising:

a central access control system; and

an access reader structured to receive an access credential from the central access control system, wherein the access reader includes a first connector connected with a second connector, the second connector being connected to a cable, the cable in electronic communication with the central access control system; and

wherein connection of the first connector and the second connector places the access reader in electronic communication with the central access control system.

13. The apparatus of claim 12, further including a backplate configured to be fastened to a wall, the backplate including an aperture to allow the second connector to pass therethrough, wherein the backplate retains the access reader to the structure.

14. The apparatus of claim 13, further including a tamper detector located on one of the backplate and the access reader, wherein the tamper detector is placed adjacent the other of the backplate and the access reader, wherein the tamper detector is structured to detect movement relative the backplate and the access reader.

15. The apparatus of claim 13, further including a coverplate disposed atop an outer surface of the access reader, the coverplate located on a side opposite the backplate.

16. The apparatus of claim 12, further including a ridge extending outwardly from a housing of the access reader, the ridge located in juxtaposition with the first connector,

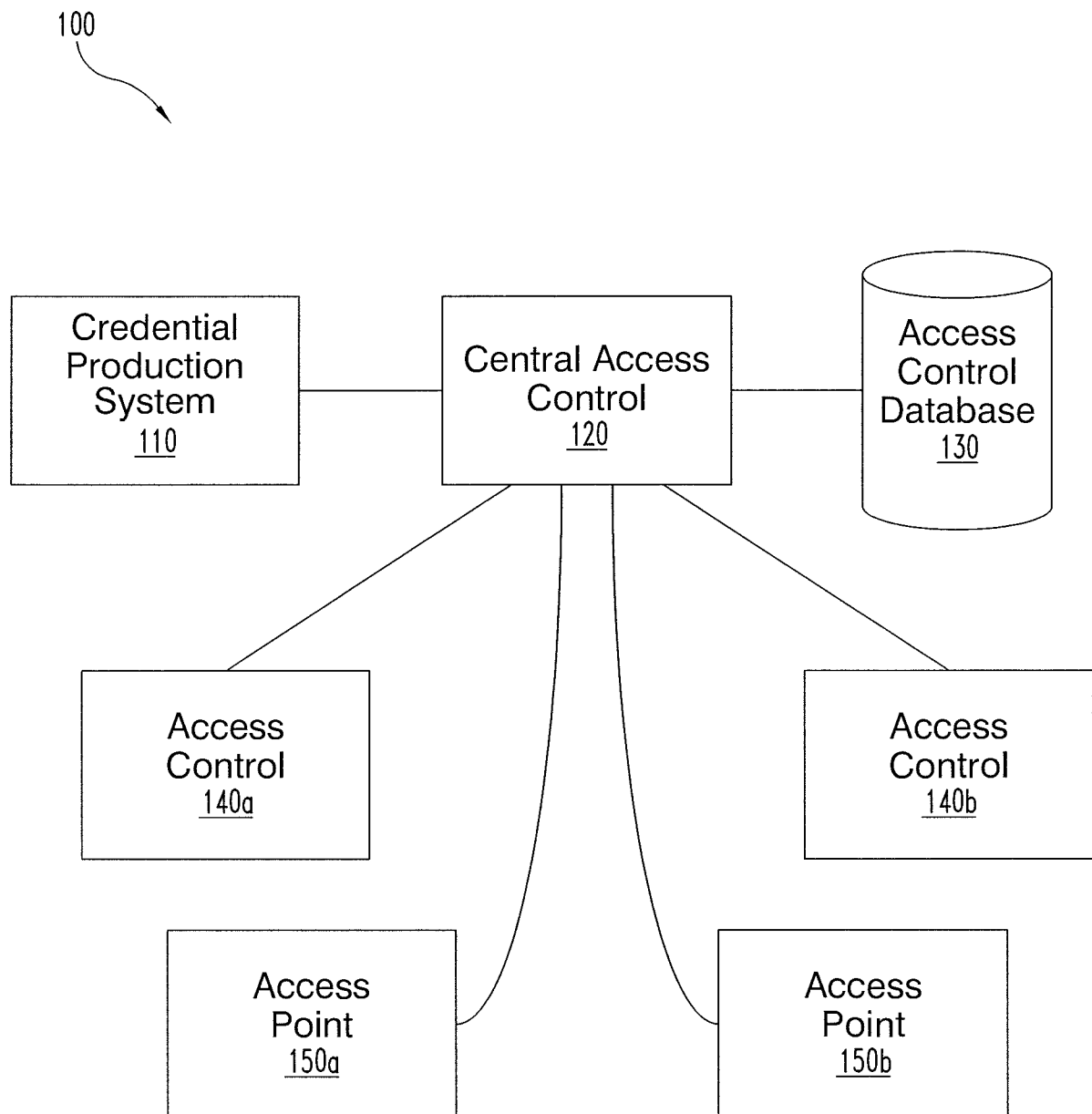
wherein the ridge is structured to be received by and retained in a recess in a housing of the second connector, wherein the recess is located between a portion of the housing of the second connector defining an outer perimeter of the housing of the second connector and a plurality of electronic connectors of the second connector.

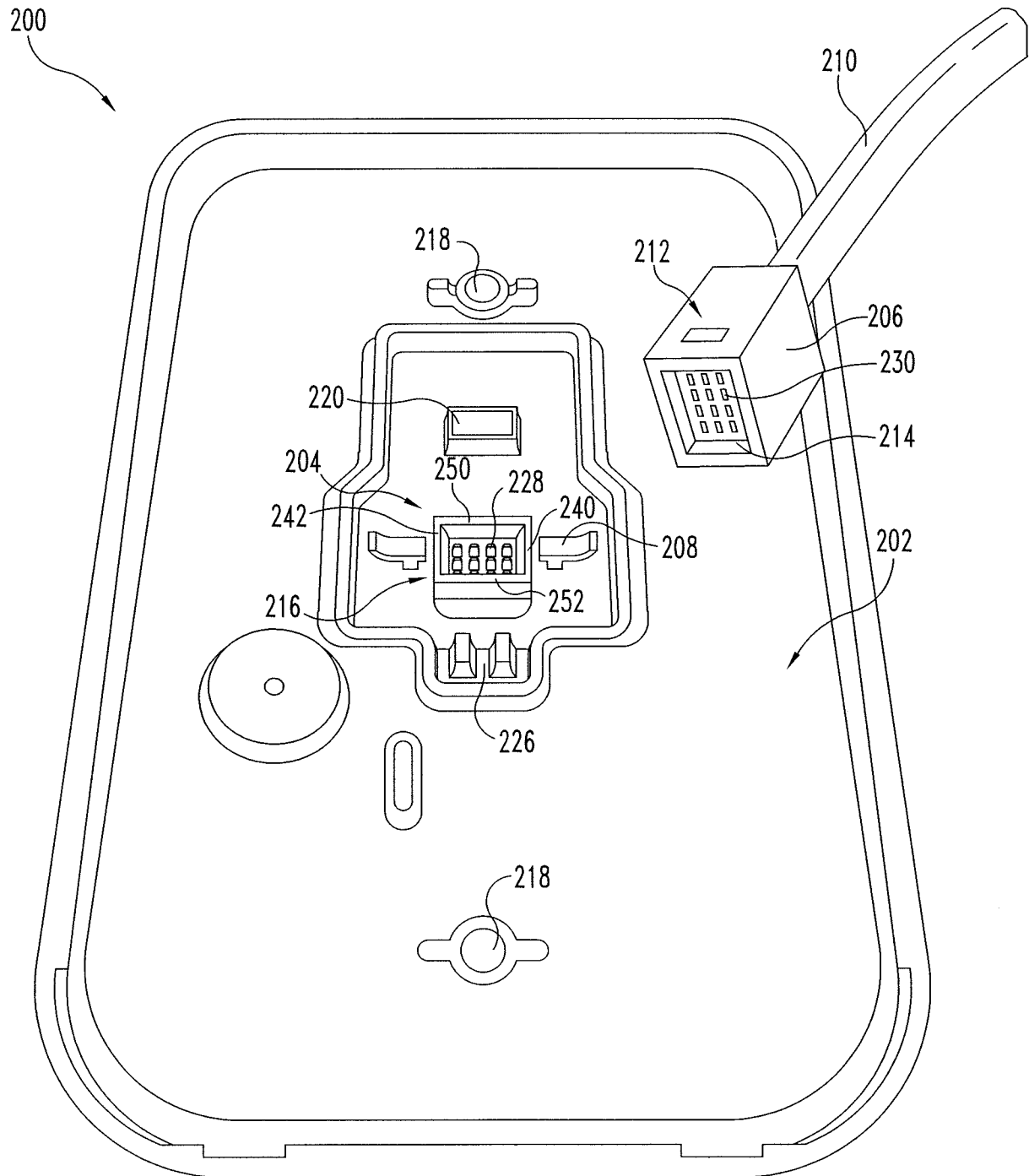
17. The apparatus of claim 12, further including a clip in juxtaposition with the first connector, wherein the clip is structured to be received by a recess in an outer surface of the second connector.

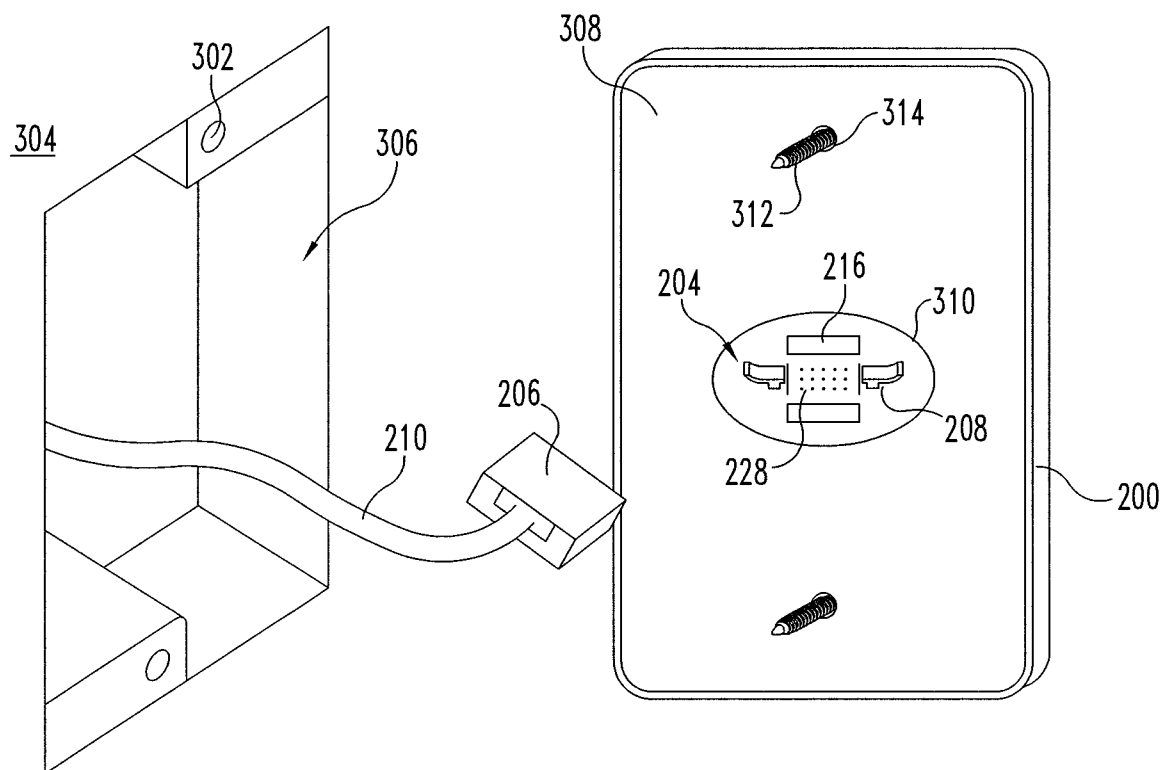
18. The apparatus of claim 12, wherein one of the first connector and the second connector comprises a male connector including a plurality of pins and wherein the other one of the first connector and the second connector comprises a female connector including a plurality of pin receiving members, whereby the pin and the pin receiving members are structured to engage one another in electronic communication to thereby permit electronic signals to flow therethrough.

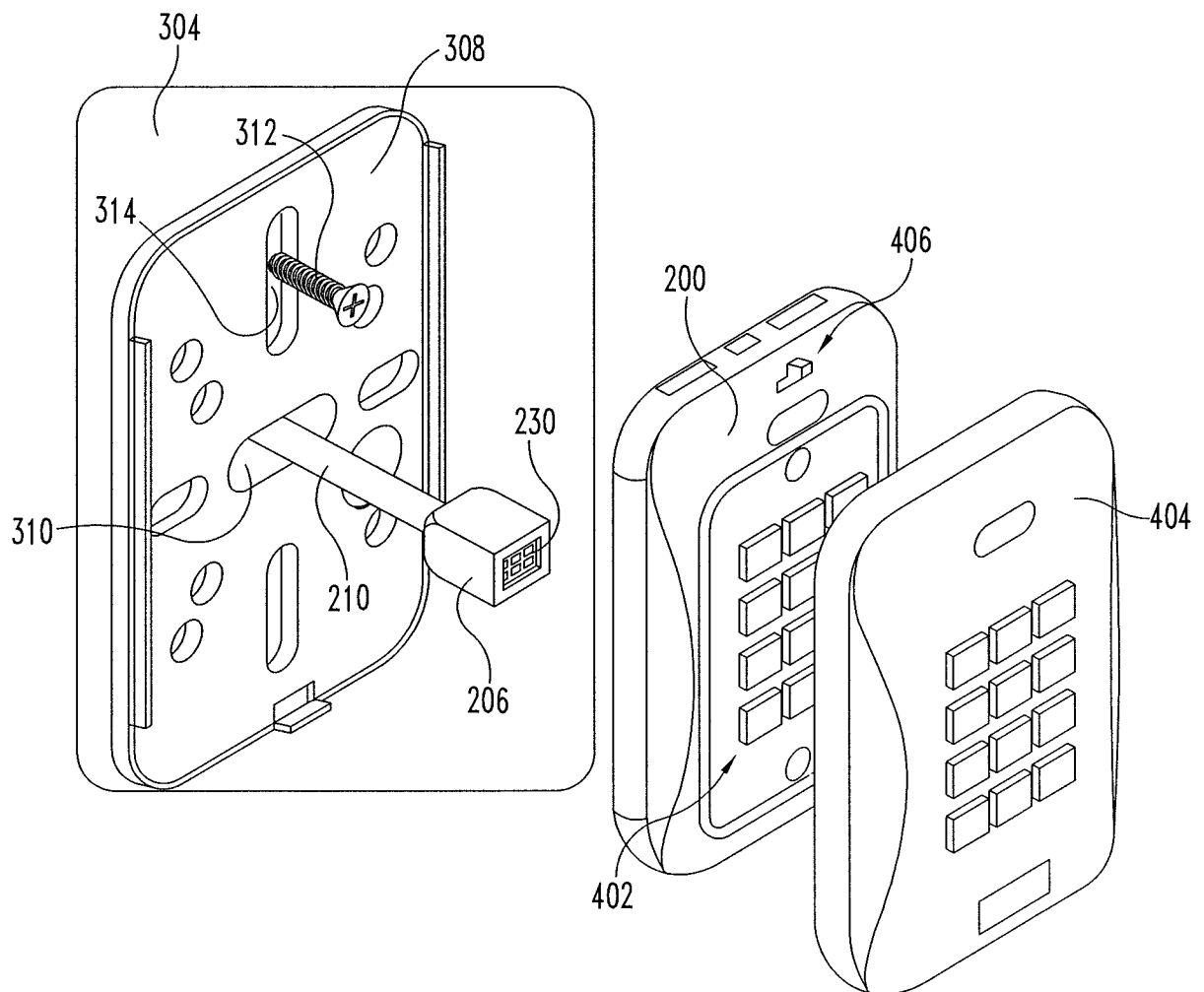
19. The apparatus of claim 12, wherein the second connector comprises a wiring harness.

20. The apparatus of claim 12, wherein the access reader further comprises at least one of a RFID reader and a keypad positioned in the housing.

**Fig. 1**

**Fig. 2**

**Fig. 3**

**Fig. 4**

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US13/47679

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F 17/30, 21/34 (2013.01)

USPC - 713/186, 185; 726/20

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(8) Classification(s): G06F 17/30, 21/34 (2013.01)

USPC Classification(s): 713/186, 185; 726/20

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 practicable, search terms used)

MicroPatent (US-G, US-A, EP-A, EP-B, WO, JP-bib, DE-C.B, DE-A, DE-T, DE-U, GB-A, FR-A); IP.com; Google.com; Google.com/Scholar; control; access; reader; cable; connector; harness

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X — Y	US 2011/0226849 A1 (PADILLA, TM et al.) September 22, 2011; figure 1, 2; paragraphs [0002], [0023], [0025], [0027], [0046], [0062]	1, 3-6, 8-10 — 2, 7, 11-15, 17-20
Y	US 7,583,495 B2 (CARNEVALI, JD) September 1, 2009; column 44, lines 25-50	2, 7, 11-15, 17-20
A	US 2003/0028814 A1 (CARTA, DR et al.) February 6, 2003; entire document	1-20

☐ Further documents are listed in the continuation of Box C.

* 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 application or patent 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

04 November 2013 (04.11.2013)

Date of mailing of the international search report

22 NOV 2013

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-3201

Authorized officer:

Shane Thomas

PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774