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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
06 September 2019 (06.09.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/169103 A1

(51) International Patent Classification:
G06F 21/31 (2013.01) *H04L 29/06* (2006.01)
G06F 21/86 (2013.01)

(21) International Application Number:
PCT/US2019/020002

(22) International Filing Date:
28 February 2019 (28.02.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
15/910,589 02 March 2018 (02.03.2018) US

(71) Applicant: **BENTLY NEVADA, LLC** [US/US]; 1631 Bently Parkway South, Minden, NV 89423 (US).

(72) Inventor: **MAYES, Nathan, Dean**; 1631 Bently Parkway South, Minden, NV (US).

(74) Agent: **ADAMS, Lisa** et al.; Mintz Levin Cohn Ferris Glovsky and Popeo, P.C., One Financial Center, Boston, MA 02111 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, SA, 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, ST, 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))*

(54) Title: TWO-STEP HARDWARE AUTHENTICATION

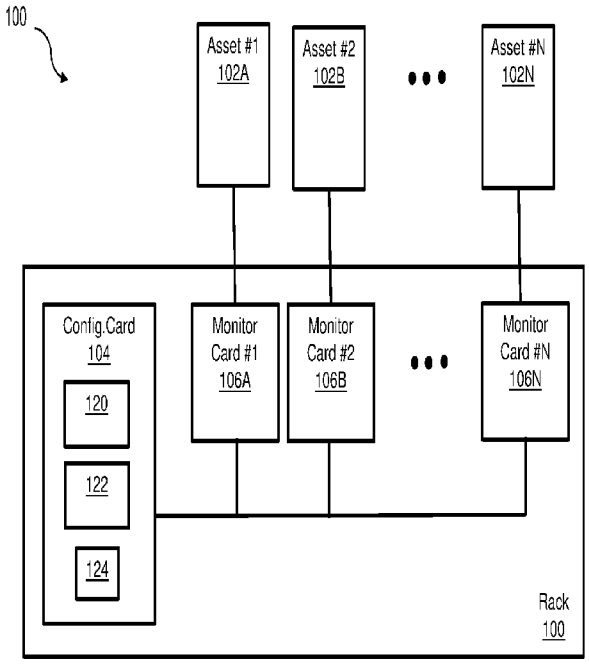


FIG. 1

(57) Abstract: Methods and systems are provided for two-step hardware authentication for machine monitoring systems. In one embodiment, a machine monitoring system can include a first hardware lock having a locked-state and an unlocked-state. The monitoring system can also include a second hardware lock including a sensor to detect first identification indicia of a user. The machine monitoring system can further include a data port configured to operatively couple to a computing device of the user. The data port can have an enable state and a disable state. The monitoring machine can include a processor operatively coupled to the first hardware lock, the second hardware lock, and the data port. The processor can be configured to receive data characterizing the activation of the first hardware lock and the first identification indicia of the user, and activate the data port to the computing device of the user.

WO 2019/169103 A1

TWO-STEP HARDWARE AUTHENTICATION

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority from U.S. Patent Application No. 15/910,589 filed on March 2, 2018, entitled "TWO-STEP HARDWARE AUTHENTICATION," the disclosure of which is hereby expressly incorporated herein by reference in its entirely.

BACKGROUND

[0002] Manually monitoring complex machines that have several moving and/or vibrating parts (e.g., turbines, compressors, etc.) can be difficult. Monitoring systems are commonly used to monitor the operation of a complex machine, and generate alarms when the machine is not operating as desired. Monitoring systems can include sensors to detect operational information (e.g., operating parameters, operational states, etc.) associated with the machine, and relay a signal to a computing device, which can generate alarms based on the operational information.

[0003] Alarms can be generated by comparing the operation information with one or more alarm set point values, which can be uniquely configured for the different operational states of a machine. For example, alarms can be generated when an operational parameter of a machine exceeds an alarm set point value or is less than an alarm set point value. In some cases, generation of an alarm can alter the operation of the machine (e.g., shut the machine down). Alarm set point values can play an important role in determining the operation of the machine because the generation of the alarm is based on the corresponding set point values.

[0004] Alarm set point values of an alarm may need to be changed, for example, based on the age of the machine. But, in order to ensure that unauthorized users do not change the alarm set point values, access to alarm set point values may need to be regulated.

SUMMARY

[0005] In general, apparatus, systems, methods and articles of manufacture for two-step hardware authentication for machine monitoring systems are provided.

[0006] In one embodiment, a machine monitoring system can include a first hardware lock having a locked-state and an unlocked-state. The first hardware lock can be configured to be

activated from the locked-state to the unlocked-state by a key. The monitoring system can also include a second hardware lock including a sensor configured to detect a first identification indicia of a user. The machine monitoring system can further include a data port configured to operatively couple to a computing device of the user. The data port can have an enable state and a disable state. The monitoring machine can include a processor operatively coupled to the first hardware lock, the second hardware lock, and the data port. The processor can be configured to receive data characterizing the activation of the first hardware lock, and receive data characterizing the first identification indicia of the user. The processor can also be configured to activate the data port from the disable state to the enable state to operatively couple to the computing device of the user. The processor can also be configured to determine a user access level based on the first identification indicia and a database of authorized users. The user access level can be indicative of a privilege assigned to the user to access (e.g., query, edit, and the like) a first alarm set point value of a machine (e.g., industrial machine). The processor can further be configured to receive a user input for the first alarm set point value of the machine from the computing device of the user.

[0007] One or more of the following features can be included in any feasible combination.

[0008] In one embodiment, a machine monitoring system can include a first hardware lock having a locked-state and an unlocked-state. The first hardware lock can be configured to be activated from the locked-state to the unlocked-state by a key. The monitoring system can also include a second hardware lock including a sensor configured to detect a first identification indicia of a user. The machine monitoring system can further include a data port configured to operatively couple to a computing device of the user. The data port can have an enable state and a disable state. The monitoring machine can include a processor operatively coupled to the first hardware lock, the second hardware lock, and the data port. The processor can be configured to receive data characterizing the activation of the first hardware lock, and receive data characterizing the first identification indicia of the user. The process can also be configured to activate the data port from the disable state to the enable state to operatively couple to the computing device of the user. The processor can also be configured to determine a user access level based on the first identification indicia and a database of authorized users. The user access level can be indicative of a privilege assigned to the user to access (e.g., query, edit, and the like) a first alarm set point value of amachine. The processor can further be configured to receive a user input for the first alarm set point

value of the machine from the computing device of the user.

[0009] In one embodiment, the machine monitoring system can include a monitor card associated with the machine. The monitor card can include a monitor card memory that stores the first alarm set point value. The machine monitoring system can also include a configuration card that can include the first hardware lock, the second hardware lock, the data port, the processor and a configuration card memory. The configuration card memory stores the database of authorized users. The processor can be operatively coupled to the monitor card and configured to execute a database operation on the first alarm set point value based on the user input.

[0010] In one embodiment, the processor can be configured to activate the data port from the disable state to the enable state by verifying the first identification indicia of the user. In another embodiment, the verification of the first identification indicia includes identifying a user identification value indicative of the first identification indicia in the database of authorized users. In yet another embodiment, the processor can be further configured to receive a second identification indicia of the user from the computing device via the data port.

[0011] In one embodiment, the processor can be further configured to verify the second identification indicia of the user based on a user name value and a user password value associated with the user identification value in the database of authorized users. In another embodiment, the processor can be configured to determine the user access level based on the user identification value, the user name value and the user password value. In yet another embodiment, the user access level can be indicative of an authorized database operation associated with the user. The authorized database operation can include one of reading the first alarm set point value and/or editing the first alarm set point value in a monitor card memory of the machine.

[0012] In one embodiment, the processor can be further configured to execute the user input based on the determined access level. In another embodiment, the user identification value, the username value, the user password value and information associated with the user access level can be stored in a user dataset in the database of authorized users. In yet another embodiment, the information associated with the user access level can include indicia of one or more set point values accessible to the user, and one or more authorized database

operations associated with each of the one or more set point values. In another embodiment, the sensor in the second hardware lock can be configured to detect the first identification indicia via one or more of RFID, Bluetooth, and keypad.

[0013] In one embodiment, a two-step hardware authentication method can include receiving data characterizing activation of a first hardware lock, and receiving data characterizing a first identification indicia of the user from a second hardware lock. The method can include activating a data port from a disable state to an enable state to operatively couple to a computing device of a user. The method can also include determining a user access level based on the first identification indicia and a database of authorized users. The user access level indicative of a privilege assigned to the user to access a first alarm set point value of an machine. The method can further include receiving a user input for the first alarm set point value of the machine from the computing device of the user. The method can also include executing a database operation on the first alarm set point value based on the user input.

[0014] In one embodiment, the method can include activating the data port from the disable state to the enable state by verifying the first identification indicia of the user. In another embodiment, verifying the first identification indicia can include identifying a user identification value indicative of the first identification indicia in the database of authorized users.

[0015] In one embodiment, the method can include receiving a second identification indicia of the user from the computing device via the data port. In another embodiment, the method can include verifying the second identification indicia of the user based on a user name value and a user password value associated with the user identification value. In yet another embodiment, determining the user access level can be based on the user identification value, the user name value and the user password value. The user access level can be indicative of an authorized database operation associated with the user. The authorized database operation can include one of reading the first alarm set point value and/or editing the first alarm set point value. In one embodiment, executing the database operation on the first alarm set point can include editing the first alarm set point value to a new value based on the user input.

[0016] These and other capabilities of the disclosed subject matter will be more fully understood after a review of the following figures, detailed description, and claims.

BRIEF DESCRIPTION OF THE FIGURES

[0017] These and other features will be more readily understood from the following detailed description taken in conjunction with the accompanying drawings, in which:

[0018] FIG. 1 is a system block diagram of an example machine monitoring system including an example two-step hardware authentication;

[0019] FIG. 2 is a system block diagram of an example configuration card including an example two-step hardware authentication of a machine monitoring system;

[0020] FIG. 3 is an example table of an example database stored in a configuration card memory;

[0021] FIG. 4 is a data flow diagram of an exemplary process of a two-step hardware authentication of a machine monitoring system; and

[0022] FIG. 5 is a process flow diagram illustrating an exemplary method for two-step hardware authentication by a processor.

DETAILED DESCRIPTION

[0023] Certain exemplary embodiments will now be described to provide an overall understanding of the principles of the structure, function, manufacture, and use of the systems, devices, and methods disclosed herein. One or more examples of these embodiments are illustrated in the accompanying drawings. Those skilled in the art will understand that the systems, devices, and methods specifically described herein and illustrated in the accompanying drawings are non-limiting exemplary embodiments and that the scope of the present invention is defined solely by the claims. The features illustrated or described in connection with one exemplary embodiment may be combined with the features of other embodiments. Such modifications and variations are intended to be included within the scope of the present invention. Further, in the present disclosure, like-named components of the embodiments generally have similar features, and thus within a particular embodiment each feature of each like-named component is not necessarily fully elaborated upon.

[0024] Some industrial machine monitoring systems can generate alarms when a parameter, such as vibration, exceeds a threshold values (also referred to as a set point). These alarms can enable machine operators to identify machine problems early and take corrective actions. In addition, a given monitoring system can monitor multiple machines, and so can have many

set points. But granting an individual access to the monitoring system to change a given set point can allow the individual to change any set point in the system, even those that the individual is not authorized to modify or should not modify.

[0025] To provide improved security, the current subject matter can include a two-step hardware authentication in which access to the set point values is permitted after a hardware lock in the monitoring system has been unlocked. This hardware lock can require a user to provide a unique identification via a sensor (e.g., an RFID reader, a keypad, and the like). Further, once the identity of the user is known, the current subject matter can limit access of the user to certain machines. The system can also limit the user to a type of operation (e.g., read access, write access, etc.). By including a user lock that requires user identity to unlock, the current subject matter can improve the security of the monitoring system.

[0026] FIG. 1 is a system block diagram of an example machine (e.g., industrial machine) monitoring system 100. The monitoring system 100 can include an example two-step hardware authentication that can improve security of the monitoring system. The monitoring system 100 can control the operation of machines / assets 102A-N at an industrial plant (e.g., a power plant). For example, the monitoring system 100 can monitor the operation of the machines and generate alarms when a machine is not operating as desired. For example, an alarm can be generated when an operating parameter of the machine exceeds a set point value or falls below a set point value. The set point value can be queried (e.g., read, edited, etc.) only by the authorized users.

[0027] The monitoring system 100 can include a configuration card 104 and multiple monitor cards 106A-N that can communicate with the configuration card 104. Each monitor card can be operatively coupled to a machine (e.g., one of machines 102A-N). In some implementations, a monitor card 106A can include a processor for monitoring the operation of a machine 102A, and a memory card for storing the alarm set points associated with the machine 102A. The configuration card 104 can include a first hardware lock 120, a second hardware lock 122 and a data port 124. The configuration card 104 can receive inputs from a user (e.g., via the first hardware lock 120, the second hardware lock 122, the data port 124, and the like), and can access (e.g., read, edit, and the like) set point values in the monitor cards 106A-N.

[0028] The first hardware lock 120 can include, for example, a lock that can be switched

from a locked state to an unlocked state by a key (e.g., physical key, passcode provided through a keypad lock). The second hardware lock can include a sensor that can detect a unique first identification indicia associated with a user. This can be done, for example, by radio-frequency identification (RFID), near field communication (NFC), Bluetooth, phone key, key fob and the like. In some implementations, the unique first identification indicia associated with the user can be acquired by a keypad in the second hardware lock. A user can enter in the first identification indicia via the keypad.

[0029] FIG. 2 is a system block diagram of an example configuration card 104 in the monitoring system 100. The configuration card 104 can include an example two-step hardware authentication that can improve security of the monitoring system. The configuration card 104 can include a processor 202 that can communicate with the first hardware lock 120, the second hardware lock 122, the data port 124, and a configuration card memory 204. The processor 202 can receive a signal that can include data characterizing the activation of the first hardware lock 120 from the locked state to an unlocked state (e.g., by turning a key in the first hardware lock). The processor 202 can also receive a signal from the second hardware lock that can include data characterizing the first identification indicia of the user. In some implementations, the processor 202 can activate the second hardware lock 122 after receiving data characterizing the activation of the first hardware lock. In another implementation, the second hardware lock 122 can be activated by the first hardware lock 120 after the latter is activated (e.g., first hardware lock 120 can provide an enable signal to second hardware lock 122). In some implementations, the second hardware lock 122 is activated before the first hardware lock 120. For example, the first hardware lock 120 can be activated by the second hardware lock 122 after the latter is activated (e.g., second hardware lock 122 can provide an enable signal to first hardware lock 120). In some implementations, both the first hardware lock 120 and the second hardware lock 122 are enabled such that the they can be unlocked in any order.

[0030] The processor 202 can verify the first identification indicia of the user by comparing it with user identities in a database of authorized users stored in the configuration card memory 204. FIG. 3 is an example table of an exemplary database of authorized users 300. The database 300 can include user data sets 302-308 having verification and access information of various users. A user data set can include values for various data fields, such as UserID 312, name of the users 314, login user names 316, login user passwords 318 and a user access

level 320. The processor 202 can retrieve the entire or a portion of the database of authorized users 300 from the configuration card memory 204. For example, the processor can retrieve the UserID data field that includes user identification values of all the user data sets. The processor 202 can verify the detected first identification indicia, for example, by comparing it with the user identification values in the UserID field 312. If a match is found (e.g., the detected first identification indicia matches a UserID value such as 302A of the user data set 302), it can be determined that the first identification indicia is valid.

[0031] The processor 202 can activate the data port 124 from a disabled state to an enabled state. This can be done based on verification of the first identification indicia detected by the second hardware lock, activation of the first hardware lock, and/or both. In the enabled state, the data port 124 can operatively couple to the computing device (e.g., laptop, tablet, etc.) of the user. The data port can receive information (e.g., user name, user password, set point value query, and the like) from the computing device, and can provide information (e.g., current or edited set point values of machines).

[0032] The processor 202 can receive a second identification indicia of the user from the computing device via the data port 124. The second identification indicia can include a user name and a user password. The processor 202 can verify the user name and the user password of the second identification indicia by comparing them with values in data fields of login user name 316 and a login user password 318. The processor 202 can determine that the second identification indicia is valid when the corresponding user name and the user password (e.g., received from the user via the data port 124) matches the login user name and login password values of the user data set associated with the first identification indicia. For example, if the detected first identification indicia matches the UserID value 302A of the user data set 302, the second identification indicia is considered valid if the received user name and the user password matches the login user name value 302C and the login user password value 302D, respectively.

[0033] The processor 202 can determine an access level of the user, which can be indicative of the privileges assigned to the user. The access level can indicate the set point values (e.g., set point values stored in memory cards of machines 106A-N) that the user can access. The access level can indicate one or more database operation (e.g., read, write, and the like) that the user can perform on the accessible set point values. In some implementations, access level information can be stored in the access level data field 320 of the authorized user

database. A user data set (e.g., 302), can have the access level information (e.g., 302E) stored in the access level data field 320. In some implementations, the user can be assigned an access level when both the first identification indica and the second identification indicia have been verified. For example, the user can be assigned an access level when he/she provides a valid RFID card to the second hardware lock, enters valid user name via the data port 124 and a valid user password via the data port 124.

[0034] The access level data field 320 can include an array of pointers that point to various set point values of the machines. For example, a pointer can point to set point value 250 in monitor card memory 210 of the monitor card 106A. The access level data field 320 can include one or more database operations (e.g., read / edit set point value 250) that an authorized user can perform on a set point value accessible to the user.

[0035] The processor 202 can also receive a user input for an alarm set point value (e.g., set point value 250 in monitor card memory 210 of the monitor card 106A). In some implementations, the processor 202 can prompt the user to provide a user input. The processor 202 can determine the validity of the user input. This can be performed if the access level of the user permits the user input. For example, if the user input includes a request for database operation on set point value 250, the processor can determine if access level information associated with the user includes a pointer for the set point value 250. If it is determined that the user input provided by the user is valid, the processor 202 can execute the database operation on the set point value (e.g., set point value 250). If it is determined that the user input provided by the user is invalid, the processor 202 may not execute the database operation, and the set point value remains unchanged.

[0036] The monitor card 106A can communicate with the machine 102A. For example, the monitor card 106A can receive operating parameters from the machine 102A (e.g., from sensors associated with the machine 102A). The monitor card 106A can also generate an alarm when a machine operating parameter exceeds a set point value. In some implementations, the monitor card can shut the machine down when the operating parameter exceeds a critical set point value.

[0037] FIG. 4 is a data flow diagram of an exemplary process of a two-step hardware authentication of an example machine monitoring system. At 405, the processor 202 can receive data characterizing the activation of the first hardware lock 120. The activation data

can be indicative, for example, that the first hardware lock has been activated from a locked-state to an unlocked-state by a key.

[0038] At 410, the processor 202 can receive data characterizing the first identification indicia from the second hardware lock. This data can include data received and/or detected by the second hardware lock 122 (e.g., via RFID, Bluetooth, keypad, and the like). In some implementations, the second hardware lock can include a sensor to detect a unique RFID card assigned to the user. In some implementations, the second hardware lock can include a keypad through which the user can enter a unique code associated with the user. Based on the first identification indicia (e.g., RFID detection, access code entry, and the like), the second hardware lock can generate a signal that includes data characterizing the first identification indicia.

[0039] At 415, the processor 202 can retrieve the entire or a portion of the authorized database table (e.g., database table 300) from the configuration card memory 204. In some implementations, processor 202 can selectively retrieve a data field (e.g. user identification data field 312) from the database of authorized user (e.g., database 300). In some implementations, the processor 202 can selectively retrieve information about a particular user (e.g., the processor 202 can retrieve values from the user data set 302).

[0040] At 420, the processor 202 can verify the first identification indicia. This can be done, for example, by comparing the first identification indicia (e.g., received at 410) with data from the database of authorized users (e.g., retrieved by the processor 202 at 415).

[0041] At 425, the processor 202 can activate the data port 124 from a disabled state to an enabled state (e.g., based on verification process at step 420 and/or activation of first hardware lock at step 405). In the enabled state, the data port 124 can operatively couple to a computing device of the user.

[0042] At 430, the processor 202 can receive the second identification indicia from the user device. The second identification indicia can include a user name and a user password. In some implementations, the processor 202 can prompt the computing device of the user to provide the user name and the user password. The processor 202 can save information related to the second identification (e.g., time of receiving the second identification) in the configuration card memory.

[0043] At 435, the second identification indicia can be verified by the processor 202. For example, the user name and the user password in the second identification indicia can be validated by comparing them with login user names and login user passwords in the authorized database table.

[0044] At 440, the processor can receive a user input from the computing device of the user via the data port 124. In some implementations, the processor 202 can prompt the computing device of the user to provide an input (e.g., query) for one or more alarm set points value. The user input can identify the set point values on which the user desires to perform a database operation. The user input can also identify the type of database operation and/or replacement values for set point values.

[0045] At 445, the processor 202 can determine the validity of the user input. This can be done, for example, by determining the access level authorized to the user (e.g., based on access level data in authorized user database), and by determining if the access level of the user permits the user input.

[0046] At 450, the processor 202 can execute the user input on a set point values in the memory of a monitor card of a machine. For example, if the database operation is an edit operation, the processor 202 can edit the set point value (e.g., set point value 250) and then save the edited set point value it in the monitor card memory (e.g., monitor card memory 210).

[0047] FIG. 5 is a process flow diagram illustrating an exemplary method for two-step hardware authentication that can improve security for machine monitoring system that can be executed by the processor 202. At 502, data characterizing the activation of the first hardware lock is received by the processor 202. The activation data can be indicative, for example, that the first hardware lock has been activated from a locked-state to an unlocked-state by a key.

[0048] At 504, data characterizing a first identification indicia of the user can be received from a second hardware lock. In some implementations, the second hardware lock can include a sensor to detect a unique RFID card assigned to the user. In some implementations, the second hardware lock can include a keypad through which the user can enter a unique code associated with the user. Based on the first identification indicia (e.g., RFID detection,

access code entry, and the like), the second hardware lock can generate a signal that includes data characterizing the first identification indicia.

[0049] At 506, the data port 124 can be activated from a disable state to an enable state enabling the port to operatively couple to a computing device of a user. In some implementations, the processor 202 can activate the data port 124 when the processor 202 can confirm that one or both of the first hardware lock and second hardware lock have been activated. The determining can be, for example, based on data received at steps 502 and 504.

[0050] At 508, a user access level can be determined based on the first identification indicia and a database of authorized users. The user access level can be indicative of a privilege assigned to the user to access (e.g., query) a first alarm set point value of a machine (e.g., industrial machine). The user access level can be determined when the first identification indicia received by the processor (e.g., at step 504) matches a user identity value in the database of authorized users. Determination of the access level can also depend on the validity of a second identification indicia provided by a computing device of the user via the data port 124. In some implementations, both the first identification indicia and the second identification indicia need to be valid for the determination of the user access level.

[0051] At 510, a user input for the first alarm set point value of the machine can be received from the computing device of the user. The user input can be received from the computing device of the user via the data port 124. In some implementations, the processor can prompt the computing device of the user to provide the user input. The user input can include information of one or more set point values associated with the user input. The user input can also include the database operations to be performed on the one or more set point values.

[0052] At 512, a database operation can be executed on the first alarm set point value based on the user input. This can be done, for example, by requesting the first alarm set point value (e.g., set point value 250) from a monitor card memory (e.g., memory 210) of a monitor card (e.g., 106A). If the database operation is a read operation, the processor can provide the first alarm set point value to the user (e.g., display the first alarm set point value on the computing device of the user). If the database operation is an edit operation, the processor 202 can edit the first alarm set point value and then save the edited first alarm set point value it in the monitor card memory (e.g., memory 210). In some implementations, the user can provide a replacement value for the first alarm set point in the user query or raise or lower the first

alarm by a set amount. The processor can access the first alarm set point value using an edit privilege and replace the first alarm set point value with the replacement value. The processor 202 can indicate to the user (e.g., by a message on the user computing device) that the data operation of the user input has been executed.

[0053] Other embodiments are within the scope and spirit of the disclosed subject matter. One or more examples of these embodiments are illustrated in the accompanying drawings. Those skilled in the art will understand that the systems, devices, and methods specifically described herein and illustrated in the accompanying drawings are non-limiting exemplary embodiments and that the scope of the present invention is defined solely by the claims. The features illustrated or described in connection with one exemplary embodiment may be combined with the features of other embodiments. Such modifications and variations are intended to be included within the scope of the present invention. Further, in the present disclosure, like-named components of the embodiments generally have similar features, and thus within a particular embodiment each feature of each like-named component is not necessarily fully elaborated upon.

[0054] The subject matter described herein can be implemented in digital electronic circuitry, or in computer software, firmware, or hardware, including the structural means disclosed in this specification and structural equivalents thereof, or in combinations of them. The subject matter described herein can be implemented as one or more computer program products, such as one or more computer programs tangibly embodied in an information carrier (e.g., in a machine-readable storage device), or embodied in a propagated signal, for execution by, or to control the operation of, data processing apparatus (e.g., a programmable processor, a computer, or multiple computers). A computer program (also known as a program, software, software application, or code) can be written in any form of programming language, including compiled or interpreted languages, and it can be deployed in any form, including as a stand-alone program or as a module, component, subroutine, or other unit suitable for use in a computing environment. A computer program does not necessarily correspond to a file. A program can be stored in a portion of a file that holds other programs or data, in a single file dedicated to the program in question, or in multiple coordinated files (e.g., files that store one or more modules, sub-programs, or portions of code). A computer program can be deployed to be executed on one computer or on multiple computers at one site or distributed across multiple sites and interconnected by a communication network.

[0055] The processes and logic flows described in this specification, including the method steps of the subject matter described herein, can be performed by one or more programmable processors executing one or more computer programs to perform functions of the subject matter described herein by operating on input data and generating output. The processes and logic flows can also be performed by, and apparatus of the subject matter described herein can be implemented as, special purpose logic circuitry, e.g., an FPGA (field programmable gate array) or an ASIC (application-specific integrated circuit).

[0056] Processors suitable for the execution of a computer program include, by way of example, both general and special purpose microprocessors, and any one or more processor of any kind of digital computer. Generally, a processor will receive instructions and data from a read-only memory or a random access memory or both. The essential elements of a computer are a processor for executing instructions and one or more memory devices for storing instructions and data. Generally, a computer will also include, or be operatively coupled to receive data from or transfer data to, or both, one or more mass storage devices for storing data, e.g., magnetic, magneto-optical disks, or optical disks. Information carriers suitable for embodying computer program instructions and data include all forms of non-volatile memory, including by way of example semiconductor memory devices, (e.g., EPROM, EEPROM, and flash memory devices); magnetic disks, (e.g., internal hard disks or removable disks); magneto-optical disks; and optical disks (e.g., CD and DVD disks). The processor and the memory can be supplemented by, or incorporated in, special purpose logic circuitry.

[0057] To provide for interaction with a user, the subject matter described herein can be implemented on a computer having a display device, e.g., a CRT (cathode ray tube) or LCD (liquid crystal display) monitor, for displaying information to the user and a keyboard and a pointing device, (e.g., a mouse or a trackball), by which the user can provide input to the computer. Other kinds of devices can be used to provide for interaction with a user as well. For example, feedback provided to the user can be any form of sensory feedback, (e.g., visual feedback, auditory feedback, or tactile feedback), and input from the user can be received in any form, including acoustic, speech, or tactile input.

[0058] The techniques described herein can be implemented using one or more modules. As used herein, the term "module" refers to computing software, firmware, hardware, and/or various combinations thereof. At a minimum, however, modules are not to be interpreted as

software that is not implemented on hardware, firmware, or recorded on a non-transitory processor readable recordable storage medium (i.e., modules are not software *per se*). Indeed "module" is to be interpreted to always include at least some physical, non-transitory hardware such as a part of a processor or computer. Two different modules can share the same physical hardware (e.g., two different modules can use the same processor and network interface). The modules described herein can be combined, integrated, separated, and/or duplicated to support various applications. Also, a function described herein as being performed at a particular module can be performed at one or more other modules and/or by one or more other devices instead of or in addition to the function performed at the particular module. Further, the modules can be implemented across multiple devices and/or other components local or remote to one another. Additionally, the modules can be moved from one device and added to another device, and/or can be included in both devices.

[0059] The subject matter described herein can be implemented in a computing system that includes a back-end component (e.g., a data server), a middleware component (e.g., an application server), or a front-end component (e.g., a client computer having a graphical user interface or a web browser through which a user can interact with an implementation of the subject matter described herein), or any combination of such back-end, middleware, and front-end components. The components of the system can be interconnected by any form or medium of digital data communication, e.g., a communication network. Examples of communication networks include a local area network ("LAN") and a wide area network ("WAN"), e.g., the Internet.

[0060] Approximating language, as used herein throughout the specification and claims, may be applied to modify any quantitative representation that could permissibly vary without resulting in a change in the basic function to which it is related. Accordingly, a value modified by a term or terms, such as "about" and "substantially," are not to be limited to the precise value specified. In at least some instances, the approximating language may correspond to the precision of an instrument for measuring the value. Here and throughout the specification and claims, range limitations may be combined and/or interchanged, such ranges are identified and include all the sub-ranges contained therein unless context or language indicates otherwise.

What is claimed is:

1. A system comprising:

a first hardware lock having a locked-state and an unlocked-state, the first hardware lock configured to be activated from the locked-state to the unlocked-state by a key;

a second hardware lock including a sensor configured to detect a first identification indicia of a user;

a data port configured to operatively couple to a computing device of the user, the data port having an enable state and a disable state; and

a processor operatively coupled to the first hardware lock, the second hardware lock, and the data port, wherein the processor is configured to:

receive data characterizing the activation of the first hardware lock;

receive data characterizing the first identification indicia of the user;

activate the data port from the disable state to the enable state to operatively couple to the computing device of the user;

determine a user access level based on the first identification indicia and a database of authorized users, the user access level indicative of a privilege assigned to the user to access a first alarm set point value of a machine; and

receive a user input for the first alarm set point value of the machine from the computing device of the user.

2. The system of claim 1, further comprising:

a monitor card associated with the machine, the monitor card including a monitor card memory that stores the first alarm set point value; and

a configuration card including the first hardware lock, the second hardware lock, the data port, the processor and a configuration card memory, wherein the configuration card memory stores the database of authorized users,

wherein the processor is operatively coupled to the monitor card and configured to execute a database operation on the first alarm set point value based on the user input.

3. The system of claim 1, wherein the processor is configured to activate the data port from the disable state to the enable state by verifying the first identification indicia of the user.

4. The system of claim 3, wherein verification of the first identification indicia includes identifying a user identification value indicative of the first identification indicia in the database of authorized users.

5. The system of claim 4, wherein the processor is further configured to receive a second identification indicia of the user from the computing device via the data port.

6. The system of claim 5, wherein the processor is further configured to verify the second identification indicia of the user based on a user name value and a user password value associated with the user identification value in the database of authorized users.

7. The system of claim 6, wherein the processor is configured to determine the user access level based on the user identification value, the user name value and the user password value.

8. The system of claim 7, wherein the user access level is indicative of an authorized database operation associated with the user, the authorized database operation including one of reading the first alarm set point value and/or editing the first alarm set point value in a monitor card memory of the machine.

9. The system of claim 7, wherein the processor is further configured to execute the user input based on the determined access level.

10. The system of claim 7, wherein the user identification value, the username value, the user password value and information associated with the user access level are stored in a user dataset in the database of authorized users.

11. The system of claim 10, wherein the information associated with the user access level includes indicia of one or more set point values accessible to the user, and one or more authorized database operations associated with each of the one or more set point values.

12. The system of claim 1, wherein the sensor in the second hardware lock is configured to detect the first identification indicia via one or more of RFID, Bluetooth, and keypad.

13. A method comprising:

receiving data characterizing activation of a first hardware lock;

receiving data characterizing a first identification indicia of the user from a second hardware lock;

activating a data port from a disable state to an enable state to operatively couple to a computing device of a user;

determining a user access level based on the first identification indicia and a database of authorized users, the user access level indicative of a privilege assigned to the user to

access a first alarm set point value of an machine;

receiving a user input for the first alarm set point value of the machine from the computing device of the user; and

executing a database operation on the first alarm set point value based on the user input.

14. The method of claim 13, further including activating the data port from the disable state to the enable state by verifying the first identification indicia of the user.

15. The method of claim 14, wherein verifying the first identification indicia includes identifying a user identification value indicative of the first identification indicia in the database of authorized users.

16. The method of claim 15, further comprising receiving a second identification indicia of the user from the computing device via the data port.

17. The method of claim 16, further comprising verifying the second identification indicia of the user based on a user name value and a user password value associated with the user identification value.

18. The method of claim 17, wherein determining the user access level is based on the user identification value, the user name value and the user password value.

19. The method of claim 18, wherein the user access level is indicative of an authorized database operation associated with the user, the authorized database operation including one of reading the first alarm set point value and/or editing the first alarm set point value.

20. The method of claim 13, wherein executing the database operation on the first alarm set point includes editing the first alarm set point value to a new value based on the user input.

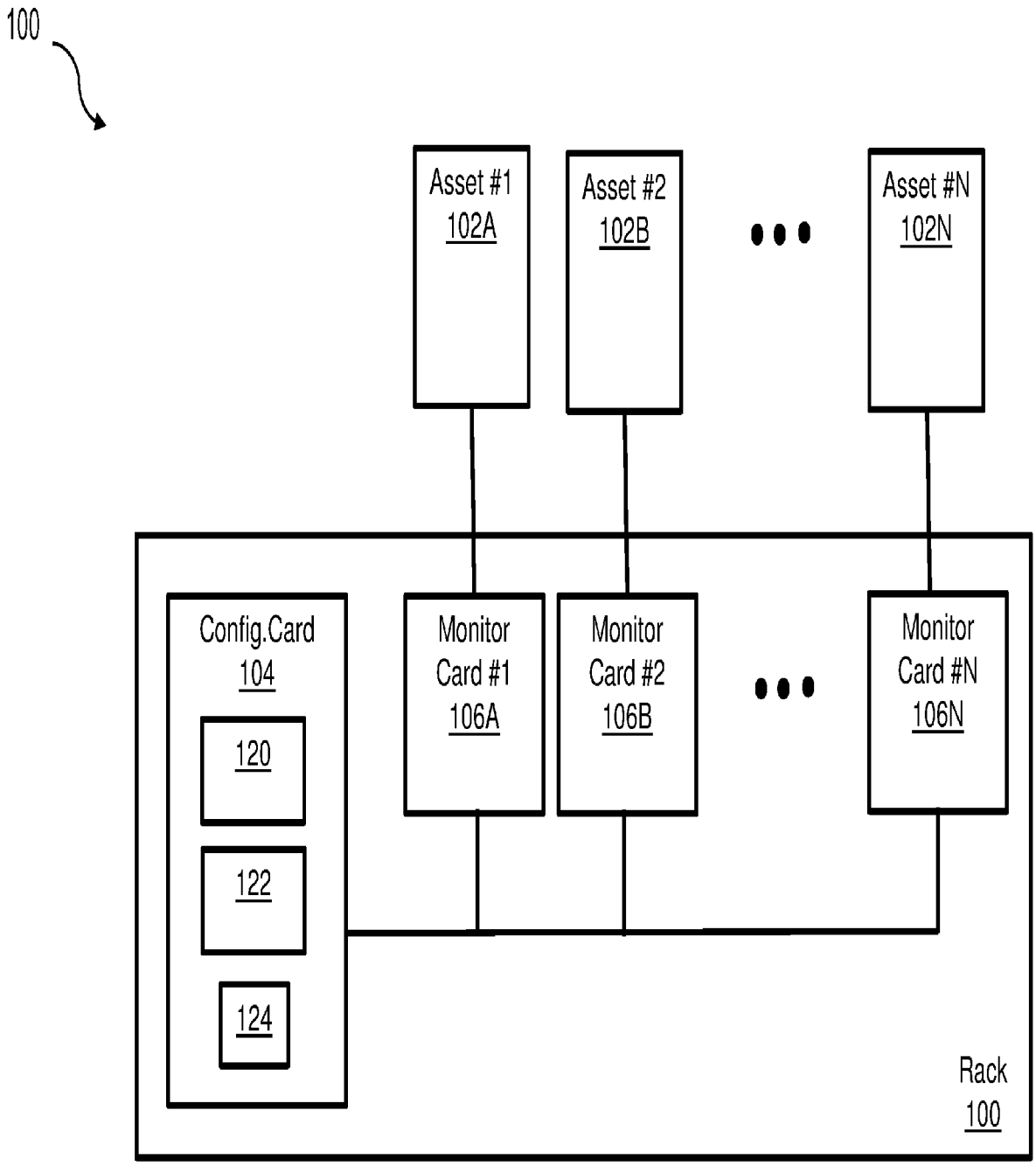

100
Asset #1
102A
Asset #2
102B
Asset #N
102N
Config.Card
104
120
122
124
Monitor
Card #1
106A
Monitor
Card #2
106B
Monitor
Card #N
106N
Rack
100

FIG. 1

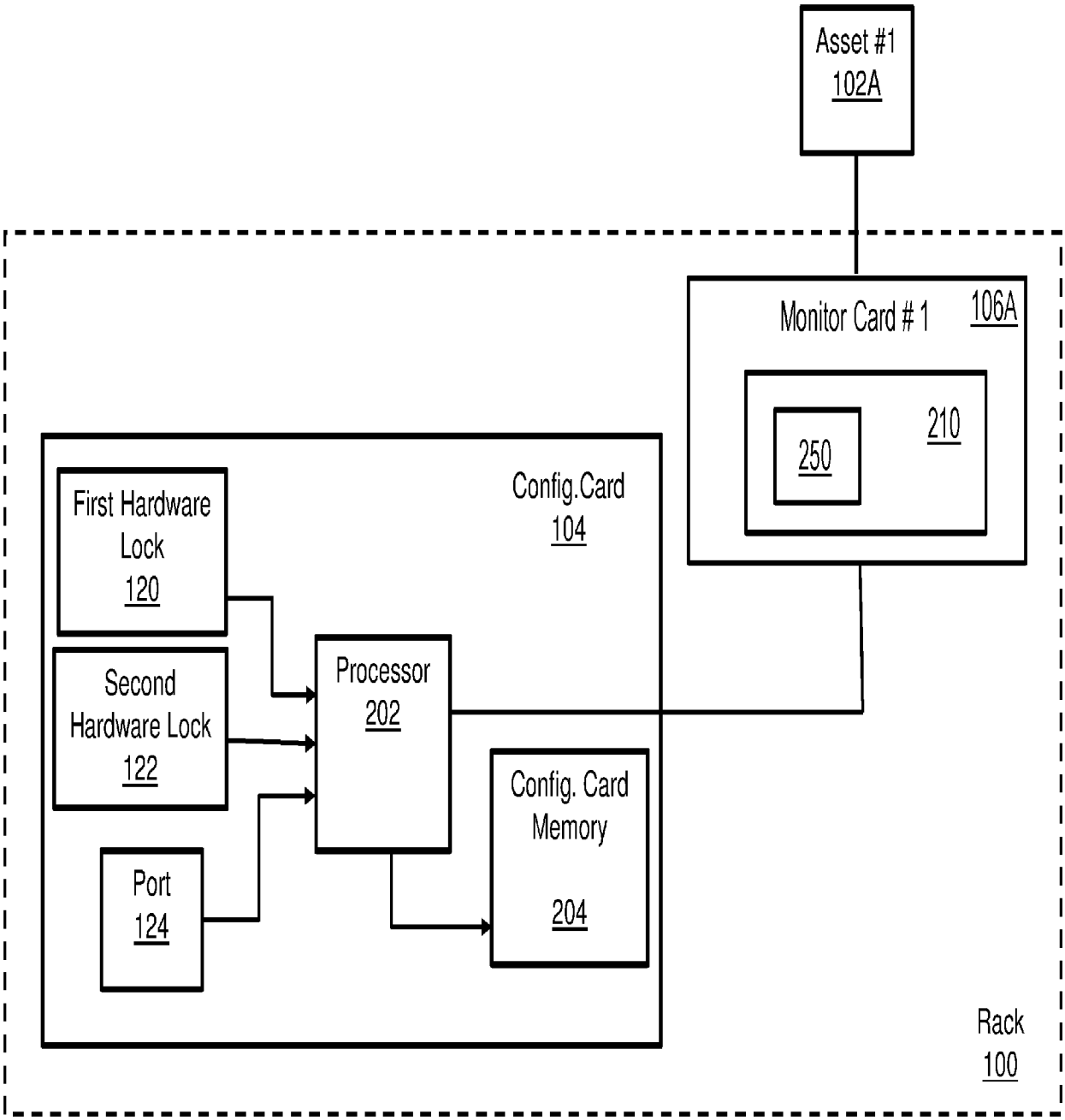
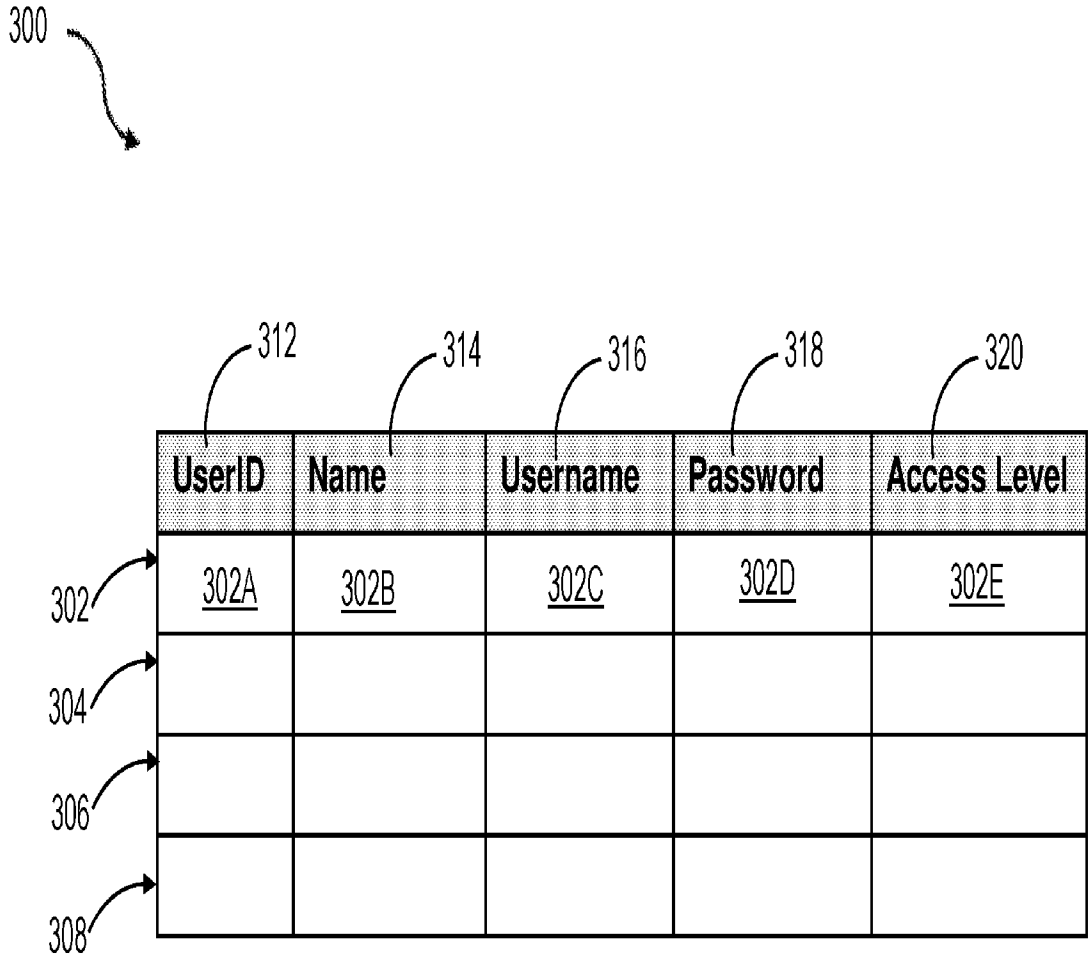

Asset #1
102A
Monitor Card # 1
106A
210
250
Config.Card
104
First Hardware
Lock
120
Second
Hardware Lock
122
Processor
202
Config. Card
Memory
204
Port
124
Rack
100

FIG. 2


300
312
314
316
318
320
UserID
Name
Username
Password
Access Level
302
302A
302B
302C
302D
302E
304
306
308

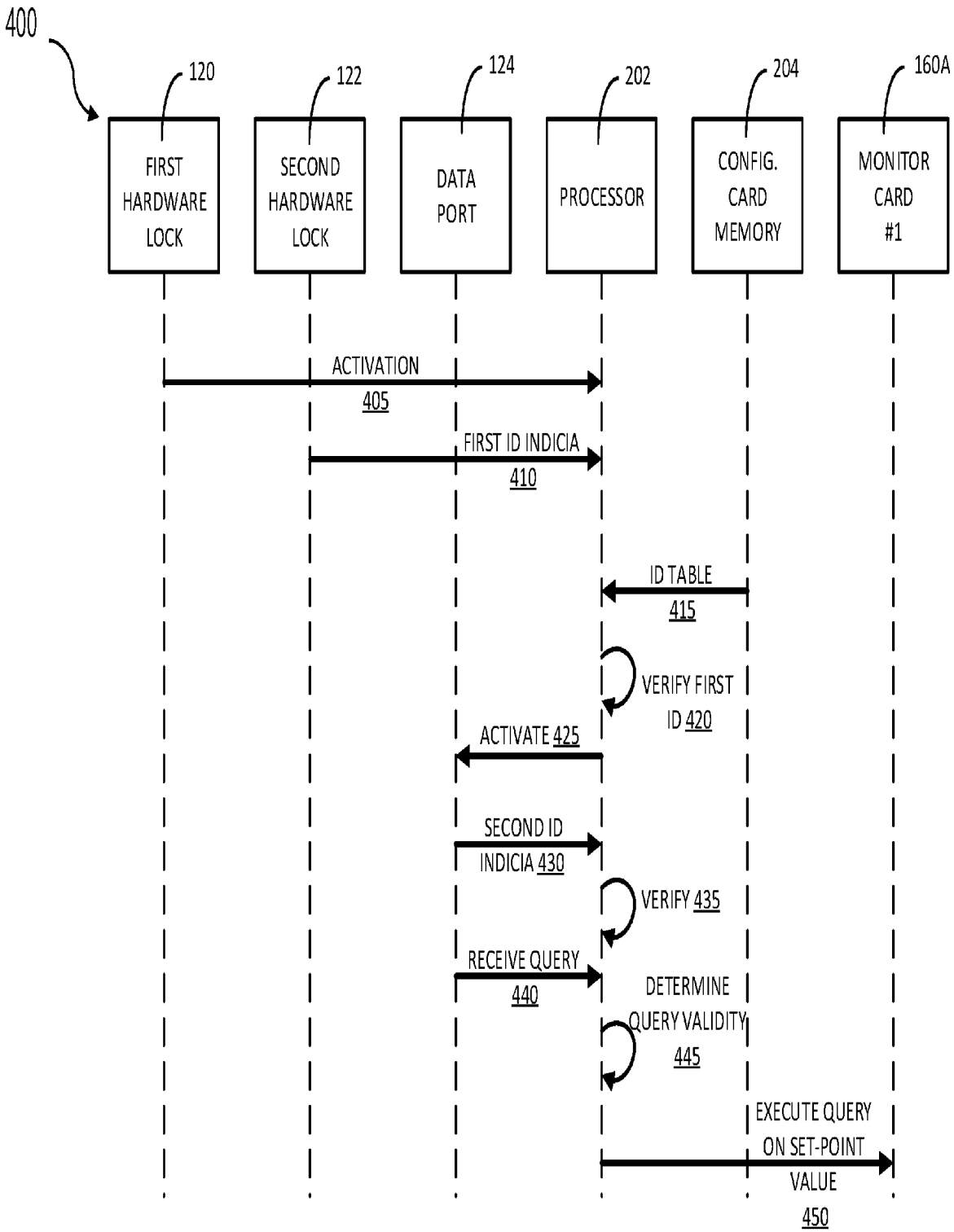

400
120
122
124
202
204
160A
FIRST HARDWARE LOCK
SECOND HARDWARE LOCK
DATA PORT
PROCESSOR
CONFIG. CARD MEMORY
MONITOR CARD #1
ACTIVATION 405
FIRST ID INDICIA 410
ID TABLE 415
VERIFY FIRST ID 420
ACTIVATE 425
SECOND ID INDICIA 430
VERIFY 435
RECEIVE QUERY 440
DETERMINE QUERY VALIDITY 445
EXECUTE QUERY ON SET-POINT VALUE 450

FIG. 4

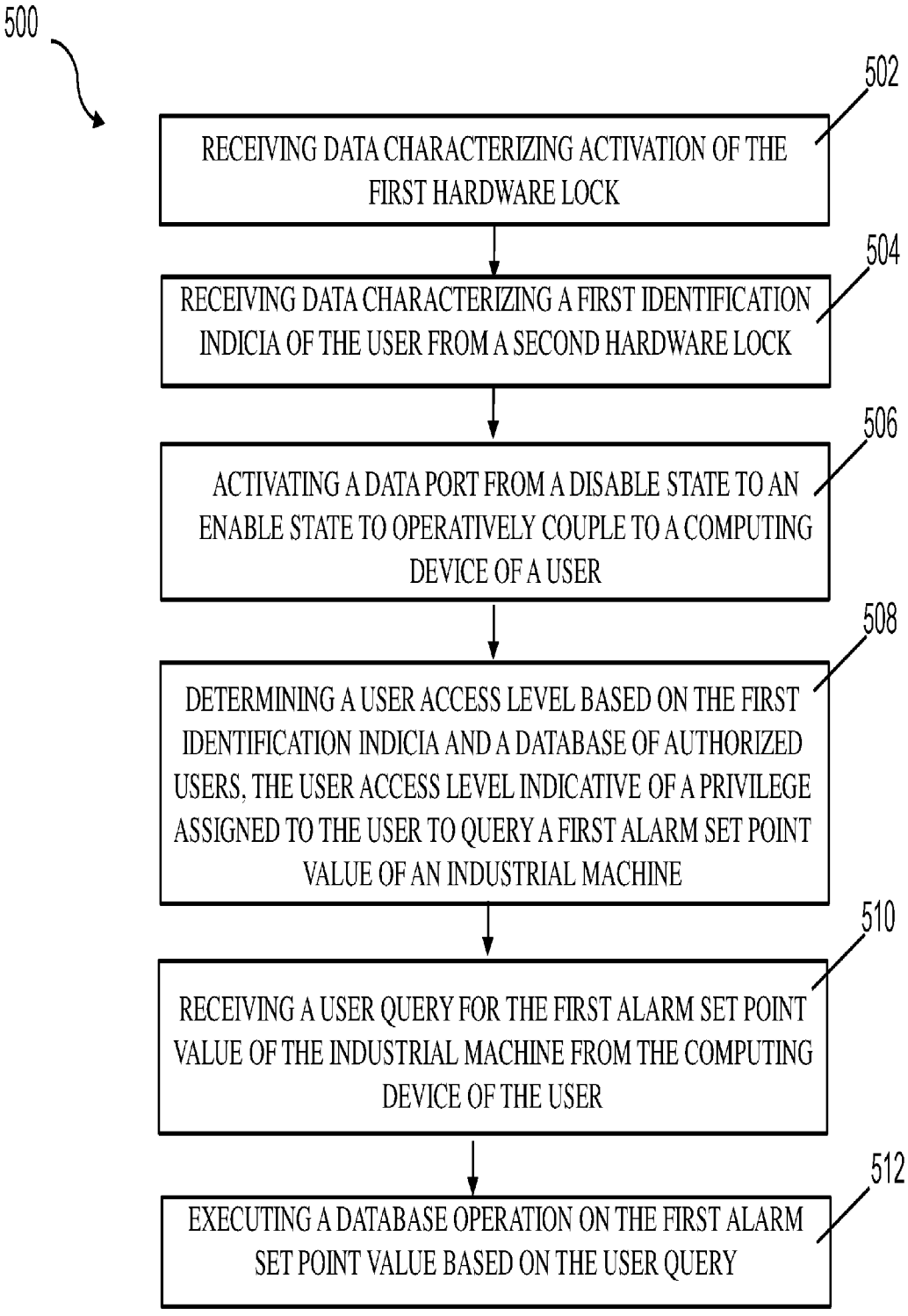

500
502
RECEIVING DATA CHARACTERIZING ACTIVATION OF THE FIRST HARDWARE LOCK
504
RECEIVING DATA CHARACTERIZING A FIRST IDENTIFICATION INDICIA OF THE USER FROM A SECOND HARDWARE LOCK
506
ACTIVATING A DATA PORT FROM A DISABLE STATE TO AN ENABLE STATE TO OPERATIVELY COUPLE TO A COMPUTING DEVICE OF A USER
508
DETERMINING A USER ACCESS LEVEL BASED ON THE FIRST IDENTIFICATION INDICIA AND A DATABASE OF AUTHORIZED USERS, THE USER ACCESS LEVEL INDICATIVE OF A PRIVILEGE ASSIGNED TO THE USER TO QUERY A FIRST ALARM SET POINT VALUE OF AN INDUSTRIAL MACHINE
510
RECEIVING A USER QUERY FOR THE FIRST ALARM SET POINT VALUE OF THE INDUSTRIAL MACHINE FROM THE COMPUTING DEVICE OF THE USER
512
EXECUTING A DATABASE OPERATION ON THE FIRST ALARM SET POINT VALUE BASED ON THE USER QUERY

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2019/020002

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/31(2013.01)i, G06F 21/86(2013.01)i, H04L 29/06(2006.01)i

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)
G06F 21/31; B60L 3/00; E05B 47/00; E05B 49/00; G05B 13/02; G05B 15/00; G06F 21/00; H04L 9/32; G06F 21/86; H04L 29/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: multiple, authentication, lock, unlock, verify, user, enable, disable, machine, parameter, alarm, access

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2008-0271122 A1 (JOHN EDWARD NOLAN et al.) 30 October 2008 See paragraphs [0006], [0015], [0019], [0029]-[0031], [0044]-[0046], [0054], [0068]; and figure 1.	1-20
Y	US 2005-0027376 A1 (J.MICHAEL LUCAS et al.) 03 February 2005 See paragraphs [0048], [0113], [0130], [0141], [0151], [0166]; and figure 14.	1-20
A	US 2014-0096178 A1 (KEITH SHIPPY et al.) 03 April 2014 See paragraphs [0014], [0020], [0039]; and figure 1.	1-20
A	US 2005-0134115 A1 (EDWARD H. BETTS JR. et al.) 23 June 2005 See paragraphs [0009], [0032], [0070]; and figure 1.	1-20
A	WO 2015-023737 A1 (UNIKEY TECHNOLOGIES, INC.) 19 February 2015 See paragraphs [0052], [0077]; and figure 1.	1-20

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

☒ See patent family 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 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	Date of mailing of the international search report
19 June 2019 (19.06.2019)	**19 June 2019 (19.06.2019)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
CHIN, Sang Bum
Telephone No. +82-42-481-8398

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2019/020002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008-0271122 A1	30/10/2008	None	
US 2005-0027376 A1	03/02/2005	CN 103616868 B	26/09/2017
		CN 1550976 A	01/12/2004
		CN 1702582 A	30/11/2005
		CN 1716137 B	16/01/2013
		DE 102004007435 A1	23/09/2004
		DE 102004038807 A1	22/12/2005
		DE 102004038808 A1	22/12/2005
		GB 2398659 B	05/12/2007
		GB 2414568 B	11/03/2009
		GB 2414814 B	12/08/2009
		GB 2443752 B	26/11/2008
		GB 2444857 B	11/03/2009
		GB 2449585 B	11/03/2009
		HK 1064174 A1	25/01/2008
		HK 1079864 A1	02/10/2009
		HK 1086081 A1	10/07/2009
		HK 1118104 A1	07/08/2009
		HK 1118914 A1	05/06/2009
		HK 1124669 A1	25/09/2009
		JP 2004-318830 A	11/11/2004
		JP 2005-339494 A	08/12/2005
		JP 2005-339495 A	08/12/2005
		JP 2011-204251 A	13/10/2011
		JP 4889929 B2	07/03/2012
		JP 4919588 B2	18/04/2012
		JP 4936641 B2	23/05/2012
		JP 5693371 B2	01/04/2015
		PH 12011000190 A1	07/09/2015
		US 2004-0199925 A1	07/10/2004
		US 2005-0027377 A1	03/02/2005
		US 2007-0061033 A1	15/03/2007
		US 2009-0287321 A1	19/11/2009
		US 2010-0228373 A1	09/09/2010
		US 2011-0224808 A1	15/09/2011
		US 7043311 B2	09/05/2006
		US 7117052 B2	03/10/2006
		US 7526347 B2	28/04/2009
		US 7729792 B2	01/06/2010
		US 7971052 B2	28/06/2011
		US 8473087 B2	25/06/2013
		US 8788071 B2	22/07/2014
US 2014-0096178 A1	03/04/2014	CN 104584024 B	19/06/2018
		CN 108664780 A	16/10/2018
		EP 2901352 A4	30/03/2016
		JP 2015-535357 A	10/12/2015
		JP 2018-106740 A	05/07/2018

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2019/020002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		JP 6342403 B2	13/06/2018
		KR 10-2015-0038430 A	08/04/2015
		US 2016-0080393 A1	17/03/2016
		US 2017-171218 A1	15/06/2017
		US 9223952 B2	29/12/2015
		US 9578037 B2	21/02/2017
		WO 2014-052069 A1	03/04/2014
US 2005-0134115 A1	23/06/2005	DE 102004060168 A1	28/07/2005
		JP 2005-200003 A	28/07/2005
		JP 4616630 B2	19/01/2011
		US 7295098 B2	13/11/2007
WO 2015-023737 A1	19/02/2015	EP 2941844 A4	31/08/2016
		US 2012-0234058 A1	20/09/2012
		US 2013-0176107 A1	11/07/2013
		US 2013-0237193 A1	12/09/2013
		US 2014-0077929 A1	20/03/2014
		US 2014-0292481 A1	02/10/2014
		US 2015-0211259 A1	30/07/2015
		US 2015-0213658 A1	30/07/2015
		US 2015-0213663 A1	30/07/2015
		US 2016-0035165 A1	04/02/2016
		US 2016-0086400 A1	24/03/2016
		US 2016-0098874 A1	07/04/2016
		US 2016-0104334 A1	14/04/2016
		US 2017-116799 A1	27/04/2017
		US 2017-116802 A1	27/04/2017
		US 9057210 B2	16/06/2015
		US 9196104 B2	24/11/2015
		US 9218696 B2	22/12/2015
		US 9336637 B2	10/05/2016
		US 9378598 B2	28/06/2016
		US 9501880 B2	22/11/2016
		US 9501883 B2	22/11/2016
		US 9972151 B2	15/05/2018
		US 9978195 B2	22/05/2018
		WO 2014-062321 A1	24/04/2014
		WO 2014-107196 A1	10/07/2014