



(11) **EP 3 048 523 B9**

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

(15) Correction information:  
**Corrected version no 1 (W1 B1)**  
**Corrections, see**  
**Description Paragraph(s) 103, 105**

(51) Int Cl.:  
**G06F 3/14** <sup>(2006.01)</sup> **G06F 9/44** <sup>(2018.01)</sup>  
**G06F 21/30** <sup>(2013.01)</sup> **G06F 21/31** <sup>(2013.01)</sup>  
**G06F 21/60** <sup>(2013.01)</sup> **G06F 21/62** <sup>(2013.01)</sup>  
**G06F 21/84** <sup>(2013.01)</sup> **H04N 1/44** <sup>(2006.01)</sup>  
**H04L 29/06** <sup>(2006.01)</sup>

(48) Corrigendum issued on:  
**26.09.2018 Bulletin 2018/39**

(45) Date of publication and mention  
of the grant of the patent:  
**25.04.2018 Bulletin 2018/17**

(21) Application number: **15196380.8**

(22) Date of filing: **25.11.2015**

---

(54) **PROGRAMMABLE DISPLAY**  
**PROGRAMMIERBARE ANZEIGE**  
**AFFICHEUR PROGRAMMABLE**

---

(84) Designated Contracting States:  
**AL AT BE BG CH CY CZ DE DK EE ES FI FR GB**  
**GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO**  
**PL PT RO RS SE SI SK SM TR**

(30) Priority: **22.01.2015 JP 2015010459**

(43) Date of publication of application:  
**27.07.2016 Bulletin 2016/30**

(73) Proprietor: **OMRON CORPORATION**  
**Kyoto, Kyoto 600-8530 (JP)**

(72) Inventor: **NAGATA, Yuta**  
**Kyoto, Kyoto 600-8530 (JP)**

(74) Representative: **Horn Kleimann Waitzhofer**  
**Patentanwälte PartG mbB**  
**Ganghoferstrasse 29a**  
**80339 München (DE)**

(56) References cited:  
**JP-A- 2008 033 573 US-A1- 2004 260 408**  
**US-A1- 2013 066 945 US-A1- 2014 215 356**  
**US-B1- 8 185 550**

---

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

---

## Description

### FIELD

**[0001]** The present invention relates to a programmable display that allows viewing of and interaction with a control system that includes a control device.

### BACKGROUND

**[0002]** At a typical production site, manufacturing devices, robots, and the like are controlled using a control device called a programmable logic controller (PLC). The demand for efficiency and these production sites and the progress made in Information and Communication Technology and the like has led to the development of technologies that allow for remote viewing and interaction using networking technologies.

**[0003]** For instance, JP 2008-033573 A discloses remotely displaying a screen displayed by a programmable display, and allowing interactions identical to that with a programmable display on the screen being displayed. More specifically, the programmable display described in JP 2008-033573 A use is a Virtual Network Computing (VNC) server to transmit an image of the screen being displayed thereon (image data) to a plurality of client computers.

**[0004]** US 2004/260408 A1 describes a process plant which includes a safety system that is physically and logically integrated with a process control system such that the safety system and the process control system can use common communication, while still providing functional isolation between the safety system controllers and the process control system controllers.

**[0005]** US 2013/066945 A1 shows a mechanism for presenting a software application to a plurality of users in a cloud computing environment, wherein multiple cloud users may launch and execute the application by using a web-based interface.

**[0006]** US 8 185 550 B1 describes methods and systems for providing elevated system access to users based on an alert from a monitoring tool or a request for change (RFC). Using the alert or RFC information, a provisioning server may reference the name of an impacted system against a database of privileges needed to allow elevated access to that system. The provisioning server may then initiate a task to provision a user's existing ID or a new ID with the necessary elevated privileges. Once the person closes the alert or RFC, the provisioning server may then remove access for that person, thus providing indirect and temporary access to a company's IT infrastructure and business applications without the use of a group ID or other mechanism to affect repairs on the impacted system(s).

**[0007]** US 2014/215356 A1 describes a method, a transmitting device, and a computer-readable storage medium for sharing image data between a source device and at least one receiving device, wherein image data of

a shared screen is periodically send to the at least one receiving device using a sharing connection. The method also includes the steps of receiving a request associated with activating a user interface component involving confidential information, suspending updating of the image data responsive to the received request, and periodically sending suspended image data to the at least one receiving device while updating is suspended.

### 10 SUMMARY

#### Technical Problem

**[0008]** However it must be said that there are issues with security regarding the programmable display described in the above Japanese Unexamined Patent Application Publication No. 2008-33573, because the image of the screen being displayed (image data) is transmitted as is to a plurality of client computers. At a production site, for example numerous activities require tacit knowledge, and it is necessary to restrict the number of persons capable of accessing this kind of information. On one hand, the viewing and control of a manufacturing device requires this kind of tacit knowledge which is also presented on the programmable display. However, given that the programmable display described in Japanese Unexamined Patent Application Publication No. 2008-33573 allows all the information displayed thereby to treat is presented to all the client computers regardless of the security access level or the importance, the programmable display cannot appropriately protect the above-described tacit knowledge.

**[0009]** Therefore, for a programmable display that allows remote viewing of content displayed thereon what is desired is a configuration therefor that appropriately preserves the security level of the content displayed. Solution to Problem

**[0010]** A programmable display is provided for connection to a control device. According to embodiments of the invention the programmable display includes: a user management unit configured to identify a user accessing the programmable display; a generation unit configured to generate an interface screen containing information from the control device in accordance with privileges assigned the user identified by the user management unit; a display unit configured to output the interface screen; a connection management unit configured to, in response to a request for access from a user on an external device, establish a connection with the external device on the basis of identification of the user by the user management unit, and to send the interface screen to an external device with which a connection is established; and the user management unit is configured to prohibit simultaneous access to the programmable display by a plurality of users each having different privileges assigned and to allow simultaneous access to the programmable display by a plurality of users each having the same privileges assigned.

**[0011]** The user management unit is configured to terminate access to the programmable display as a first user assigned a first privilege when a second user assigned a second privilege that is lower than the first privilege attempts to access the programmable display while the first user assigned the first privilege is accessing the programmable display.

**[0012]** Further, the user management unit may notify a first user assigned a first privilege of a second user assigned a second privilege that is lower than the first privilege attempting to access the programmable display when the second user attempts to access the programmable display while the first user is accessing the programmable display.

**[0013]** Furthermore, the user management unit may deny the access of the second user to the programmable display in response to an instruction from the first user.

**[0014]** Alternatively, the user management unit may terminate access to the programmable display as the first user in response to an instruction from the first user.

**[0015]** The user management unit may permit the second user to access the interface screen with greater limitations than the limitations on the first user in response to an instruction from the first user.

#### Effects

**[0016]** Embodiments of the invention allow a programmable display that allows remote viewing of the content displayed thereon, to appropriately preserve the security level of the content displayed.

#### BRIEF DESCRIPTION OF THE DRAWINGS

##### **[0017]**

Figure 1 is a schematic view illustrating an overall configuration of a control system according to an embodiment;

Figure 2 is a block diagram illustrating a hardware configuration in a programmable display according to an embodiment;

Figure 3 is a schematic view for describing the viewing and operation functions provided by the programmable display according to an embodiment;

Figures 4(A) and 4(B) illustrates an example of the contents displayed on an HMI screen presented by the programmable display according to an embodiment;

Figure 5 illustrates an example of a development program used to design an HMI screen presented by the programmable display according to an embodiment;

Figure 6 illustrates an example of a development program used to design an HMI screen presented by the programmable display according to an embodiment;

Figures 7(A), 7(B), 7(C) are schematic views for de-

scribing a function for appropriately maintaining the security level provided by a programmable display according to an embodiment;

Figure 8 is a block diagram illustrating a functional configuration in a programmable display according to an embodiment;

Figures 9(A), 9(B), 9(C), and 9(D) are schematic views for describing a first example of the processing performed in a programmable display according to an embodiment;

Figures 10(A), 10(B), and 10(C) are schematic views for describing the first example of the processing performed in a programmable display according to an embodiment;

Figures 11(A), 11(B), and 11(C) are schematic views for describing the first example of the processing performed in a programmable display according to an embodiment;

Figures 12(A), 12(B) are schematic views for describing the first example of the processing performed in a programmable display according to an embodiment;

Figure 13 is a flowchart for describing the processing procedure in the first processing example in a programmable display according to an embodiment;

Figure 14 illustrates an example of setting the permissions for an HMI screen in a programmable display according to an embodiment;

Figures 15(A), 15(B), and 15(C) are schematic views for describing a second example of the processing performed in a programmable display according to an embodiment;

Figures 16(A) and 16B are schematic views for describing a modification to the second example of the processing performed in a programmable display according to an embodiment; and

Figures 17(A) and 17(B) are diagrams for explaining an example of an implementation of user authentication in a display according to an embodiment.

#### DETAILED DESCRIPTION

**[0018]** Embodiments of the present invention will be described in detail with reference to the drawings. The same or corresponding elements within the drawings will be given the same reference numerals and the explanations therefor will not be repeated. In discussing the embodiment, a control system 1 containing a programmable display 100 and a control device 200 is described. However, the control system 1 as described below is merely an example of the application of the programmable display 100; the technical scope of the invention of the present application should be logically interpreted on the basis of the description in the claims. Note that, in the following description the programmable display 100 is sometimes merely referred to as display 100.

## A. Overall Configuration of Control System 1

**[0019]** First, an overall configuration of a control system 1 according to the embodiment is described. Figure 1 is a schematic view illustrating an overall configuration of a control system according to an embodiment. Referring to Figure 1, the control system 1 includes a production site 2 where actual manufacturing operations are carried out, and a remote site 4 from which the production site 2 remote viewing or operation may take place. The production site 2 and the remote site 4 are connected through a desired network 6 such as the Internet, or a Virtual Private Network (VPN). Note that communications between the production site 2 of the remote site 4 are preferably secure; typically the technique adopted may be to encrypt the data transmitted and received, and/or to ensure that the communication line itself is secure.

**[0020]** A control device 200 and a display 100 are arranged at the production site 2. The control device 200 is used to control a manufacturing device, a robot or the like, and the display 100 is connected to the control device 200.

**[0021]** The control device 200 is an industrial controller (referred to as a programmable logic controller, PLC) that exchanges field signals between controlled devices (manufacturing device, or robot, and the like) to thereby control the devices. The field signals are (analog and/or digital) input signals detected by various sensors, and the (analog and/or digital) output signals provided to various actuators.

**[0022]** At the production site 2, a remote input-output (I/O) device 202 is connected to the control device 200 via a field bus 14. The remote I/O device 202 exchanges field signals between the control device 200 and a controlled device located at a separate location away from the control device.

**[0023]** The display 100 is also connected to the control device 200 via a field bus 12. The display 100 presents a user with information retained in the control device 200 and sends internal commands to the control device 200 in accordance with interactions from the user. A human machine interface screen (HMI) displayed on the display 100 can be prepared by a user as desired and typically is made up to display screens and information supporting the production site 2.

**[0024]** The display 100 according to the embodiment includes a function that transmits the contents displayed to an external device (generally referred to below as a "client device 300"). The types of external device is not particularly limited so long as the device is capable of communicating by some means to the display 100; for instance, the external device may be a personal computer, a smart phone, or a different programmable display. The methods that may be used to communicate with the programmable display 100 may be any publicly known method such as universal serial bus (USB) communication, serial communication, parallel communication, a

wired network such as Ethernet (Registered Trademark), a wireless network such as wireless LAN or BLUETOOTH (Registered Trademark).

**[0025]** Within the control system in Figure 1, personal computers are provided as examples of the client device 300, and these personal computers may be directly or indirectly connected to the display 100 via a network. More specifically, a client device 300\_1 is placed at the production site 2 and connected it to the display 100 via a network 8; client devices 300\_2, 300\_3 are placed at the remote site and connected to the display 100 via a network 6 and a network 10.

**[0026]** Each of the client devices 300\_1 to 300\_3 (referred to generally below as "client device 300") accesses the display 100 to provide a user with a user interface from the display 100 (i.e., presenting a user with contents displayed on the display 100, and issuing internal commands responsive to interactions from the user). In other words, through the client device 300 a user may view and interact with the display 100 as if sitting in front of the display 100. In the description that follows, for convenience these kinds of functions provided the display 100 is referred to as the "remote viewing and operation function".

## B. Hardware Configuration of Display 100

**[0027]** Next, the hardware configuration of the display 100 is described. Figure 2 is a block diagram illustrating a hardware configuration in a display 100 according to an embodiment. The display 100 according to the embodiment possesses a hardware configuration that has a general-purpose architecture. That is, the display 100 may be implemented as one kind of personal computer. The display 100 may be implemented in not only general-purpose hardware, but also in dedicated hardware.

**[0028]** More specifically, referencing Figure 2, the display 100 includes: a processor 102 such as a central processing unit (CPU) or a microprocessing unit (MPU); a main memory 104; a flash memory 110; a network interface 112; an input output (I/O) interface 114, a field bus interface 116 and a touchscreen 120. These components are capable of data communication with each other via an internal bus 128.

**[0029]** The processor 102 executes programs pre-installed on the display 100 to thereby implement the various later described functions and processes. That is, the processor 102 reads a system program and a user program (not shown) stored in the flash memory 110 into the main memory 104, and executes the system program and the user program to implement control of the controlled device. Namely, the processor 102 coordinates between the main memory 104 and the flash memory 110 to implement a control unit that executes control computations.

**[0030]** The data exchange between the display 100 and then external device is mediated by the network interface 112, the I/O interface 114, and the field bus in-

terface 116. More specifically, the network interface 112 mediates communication with the client device 300 via the network 8 and the like (Figure 1). For instance, a component capable of communication in accordance with the Ethernet protocol may be adopted as the network interface 112. The I/O interface 114 mediates the communication with the various user interface devices such as a keyboard and a mouse. For instance a component capable of communication via USB or serial communications may be adopted as the I/O interface 114. The field bus interface 116 mediates the exchange of data with the control device 200. A component capable of communication in accordance with the EtherCAT (Registered Trademark) protocol, or similar to the network interface 112, a component capable of communication in accordance with the Ethernet protocol may be inducted as a field bus interface 116.

**[0031]** The touchscreen 120 presents various kinds of information to the user and accepts input from the user. More specifically, the touchscreen 120 includes a display unit 122 and a touchscreen panel 124. Typically the display unit 122 is constituted by a liquid crystal display (LCD) or an organic (electroluminescence) display unit the touchscreen panel 124 is mounted on the display unit 122 and accepts touch-based input from the user. In general, a pressure-sensitive or piezo-switch type device may be used in the display unit 122.

#### C. Hardware Configuration of Control Device 200 and Client Device 300

**[0032]** A PLC is usually adopted for the control device 200. Since the hardware configuration of a PLC is common knowledge, a detailed explanation therefor is not provided here.

**[0033]** Additionally, a general-purpose personal computer is usually adopted as the client device 300. Since the hardware configuration of a general-purpose personal computer is common knowledge, a detailed explanation therefor is not provided here. However, note that a program is installed on the client device 300 for exchanging data with the display 100 (later described).

#### D. Remote Viewing and Operation Function

**[0034]** Next, the remote viewing and operation function provided by the display 100 is described. Figure 3 is a schematic view for describing the remote viewing and operation function provided by the display 100 according to an embodiment. Referring to figure 3, the display 100 transmits content identical to the content displayed (dual-sided display) on the touchscreen 120 (more accurately, the display unit 122) to the client device 300. The display unit for the client device 300 presents the contents transmitted thereto. In addition, when the content (screen display) presented on the display unit of the client device 300 is subject to some kind of user interaction CL1, processing is executed that is identical to when the touch-

screen 120 (more accurately, the touchscreen panel 124) is subject to a user interaction CL2 which corresponds to the user interaction CL1. That is, input information representing the screen display presented on the client device 300 and the positional relationship of the user interaction CL1 thereon is sent to display 100, and the display 100 executes input processing in accordance with input entered corresponding to the input information.

**[0035]** Namely, the client device 300 acts as a type of clone of the display 100.

**[0036]** This kind of remote viewing and operation function may be implemented using any desired technology, however typically a virtual network computing (VNC) is used to implement this function. A module installed on the display 100 according to the embodiment functions as a VNC server so that the display 100 may provide the remote viewing and operation function to the client device 300. A software configuration for the display 100 is described later.

#### E. Security Level Setting Function

**[0037]** The display 100 according to the embodiment includes a user identification function and a function that changes the content displayed in accordance with the privileges established for a user. In the description that follows, for convenience these functions are referred to as the "security level setting function".

**[0038]** The user identification function may be implemented by adding an authentication function that requires each user using the system to enter a user name and a password, or requiring entry of a user name and a password (or only a password) only when the device is in a specific mode. In the latter case, the user identification function may identify a user as a normal user if a user name and password is not entered.

**[0039]** As a simple example, consider that the user identification function can create a user having administrator privileges (also referred to below as an "administrator"), and a user having no administrator privileges, in other words a user having only normal user privileges (also referred to below as a "normal user"). In this case, for instance, the user identification function may require at least a password only when a user having administrator privileges (administrator) is using the programmable display as an administrator. Note that the methods for user authentication are not limited to password authentication, and any desired and commonly known methods may be adopted such as various kinds of biometric authentication, e.g., fingerprint authentication, face authentication, voiceprint authentication, or authentication using an IC card.

**[0040]** Finally, the display 100 becomes capable of changing the content displayed in accordance with the privileges possessed by a user.

**[0041]** Figures 4(A) and 4(B) illustrate an example of the contents displayed on an HMI screen presented by the display 100 according to an embodiment. Figure 4(A)

presented display example of an HMI screen for a user having administrator privileges; Figure 4(B) present a display example of an HMI screen for user having no administrator privileges.

**[0042]** More specifically, the HMI screen illustrated in Figures 4(A) and 4(B) is related to a food-processing device. The HMI screen for a user having administrator privileges (Figure 4(A)) displays a recipe 141 needed for operating the food processing device, and a button 142 for downloading or uploading the recipe 141. In contrast, the recipe 141 and the button 142 are unavailable in the HMI screen for a user having no administrator privileges (Figure 4(B)).

**[0043]** In the example of the HMI screen presented in Figures 4(A) and 4(B), the HMI screen is designed so that non-administrator users cannot manipulate any functions related to the recipe. In this manner, the display 100 according to the embodiment can change whether or not to display or to make a control component available for each control component placed on the HMI screen in accordance with the privileges of the user.

**[0044]** Figure 5 and Figure 6 illustrate examples of a development program used to design an HMI screen presented by the display 100 according to an embodiment. Figure 5 depicts a security settings screen 400, and Figure 6 depicts an HMI screen design screen 410. The details of a user account may be setup from a dialog 401 on the security settings screen 400 depicted in Figure 5. Namely, the name for each user, password, the privileges, comments and the like may be entered in the dialog 401. The particulars regarding permissions may be entered in accordance with each privilege in a dialog 402. That is, for each privilege created in the dialog 401, an allowable level of access (permissions) may be set up in the dialog 402. In the security settings screen 400, a "permission" signifies a type of attribute like a group; permissions are set for each HMI screen or each control component. Thus, the content of the HMI screen or control component is displayed to only the user having the permissions provided by these settings. For instance, in the dialog 403, "Level 4" is set as the permission for a "system menu", and in dialog 402 only a user possessing Administrator (admin) privileges are assigned the permission "Level 4". With the privileges established in this manner, only a user with administrator privileges is shown a "system menu".

**[0045]** Additionally, a security level is established for each desired control component included in an HMI screen the design screen 410 illustrated in Figure 6. In the example illustrated in Figure 6, the security level is said in a dialog 412 for a control component 411. In the example illustrated in Figure 6, a visibility level for the control component 411 is set to Level 3; therefore, the user that will be displayed the control component 411 is the user assigned an attribute of Level 3 in the security settings screen 400 illustrated in Figure 5; in other words, the display of the control component is limited to a user having the privileges of an Administrator (admin).

**[0046]** As above described, the security level setting function in the display 100 according to the embodiment can control the HMI screen in accordance with the privileges each user possesses.

## F. Overview

**[0047]** The display 100 according to the embodiment deals with novel security issues that arise when the above-described remote viewing and operation function, and the security level setting function are combined. In other words, the display 100 provides a novel function that appropriately preserves the security level of the contents displayed.

**[0048]** More specifically, the display 100 prohibits simultaneous logins (access) to the display 100 from a plurality of users each having different privileges assigned thereto. For instance, it is possible to restrict or ban simultaneous access to the display 100 from a user having administrator privileges (admin) and a user with no administrator privileges (normal user) with the above-described privilege settings [function].

**[0049]** Figures 7(A), 7(B), 7(C) are schematic views for describing a function for appropriately maintaining the security level provided by a display 100 according to the embodiment. Figures 7(A), 7(B), 7(C) depict the client device 300 connecting to the display 100. As illustrated in Figure 7(A), an administrator HMI screen can be displayed when a user having administrator privileges is logged in from both the display 100 and the client device 300. As illustrated in Figure 7(B), a normal-user HMI screen can be displayed on the display 100 and the client device 300 when a user having no administrator privileges (normal user) is using both the display 100 and the client device 300.

**[0050]** While there are no security problems regarding either Figure 7(A) or Figure 7(B), the issue arises in the kind of case depicted in Figure 7(C). Namely, when a user having administrator privileges is logged into the display 100 while a user having no administrator privileges (normal user) is logged using the client device 300, the administrator HMI screen is provided to the normal user.

**[0051]** Therefore, when the situation illustrated in Figure 7(C) arises, the display 100 restricts or prohibits usage thereof by one user to maintain the security that was established. Generally, more important information is contained in the administrator HMI screen, and therefore the user having administrator privileges is logged out of the display 100 when the situation in Figure 7(C) arises. Hereby, the normal-user HMI screen may be displayed on both the display 100 and the client device 300.

## G. Functional Configuration of Display 100

**[0052]** Next, the functional configuration of the display 100 is described. Figure 8 is a block diagram illustrating a functional configuration in the display 100 according to

an embodiment. Referring to Figure 8, the display 100 contains a data storage unit 150, a rendering unit 160, an I/O data manager 162, user manager 164, display output unit 166, a user input receiver 168, a VNC server 170, and a proxy 172 as part of the functional configuration.

**[0053]** The data storage unit 150 stores data needed to display the HMI screen on the display 100. In concrete terms, the data storage unit 150 contains HMI screen settings data 152, and user registration data 154.

**[0054]** The HMI screen settings data 152 is information for displaying the HMI screen, and may be designed using the kind of design screen depicted in Figure 6. The user registration data 154 contains information on the user accounts allowed to log into the display 100. The user registration data 154 can be created using the kind of security settings screen 400 illustrated in Figure 5.

**[0055]** The user manager 164 includes a user manager function that identifies the user accessing the display 100 and processes the user log in. The user manager 164 also executes the processing that preserves the security level as described above for Figure 7. That is, the user manager 164 prohibits simultaneous access to the display 100 by a plurality of users each having different privileges assigned. The processing that prohibits this simultaneous access is described below in detail.

**[0056]** The rendering unit 160 reads the HMI screen settings data 152 contained in the data storage unit 150, and generates a screen image that is presented as the HMI screen. More specifically, the rendering unit 160 dynamically generates the HMI screen to reflect the field signals exchanged with the control device 200 via the I/O data manager 162. In addition, the rendering unit 160 acquires the privilege information for a user currently logged in from the user manager 164. The rendering unit 160 determines for each control component defined in the HMI screen settings data 152 whether or not to display or make a control component available based on the permissions assigned thereto, and reflects these permissions on HMI screen. In other words, the rendering unit 160 generates an HMI screen (interface screen) containing information from the control device 200 in accordance with the privileges assigned to a user identified by the user manager 164 (user management unit).

**[0057]** The I/O data manager 162 mediates the exchange of field signals between the rendering unit 160 and the control device 200.

**[0058]** The display output unit 166 outputs the screen image generated by the rendering unit 160 on the display unit 122. The display unit 122 thus outputs the HMI screen (the interface screen).

**[0059]** The user input receiver 168 detects input the user enters on the touchscreen panel 124, and outputs the detection results as user input to the rendering unit 160.

**[0060]** The VNC server 170 provides the client device 300 with the screen image generated by the rendering unit 160, and accepts inputs interaction from the client

device 300. The proxy 172 provides a relay function that mediates the exchange of data between the VNC server 170 and the client device 300. More specifically, the proxy 172 establishes a session between one or a plurality of client devices 300, and manages the communications with each of the client devices 300. At this point, the proxy 172 establishes a session based on the results of identifying a user carried out in the user manager 164. In other words, the VNC server 170 and the proxy 172 establish a connection with a client device 300 based on the results of the user manager 164 identifying a user in response to a request for access from a user on an external device, e.g., the client device 300. The VNC server 170 and the proxy also manage the connection that transmits an HMI screen (interface screen) to the client device 300 with which a connection is established.

**[0061]** Note that the functional configuration illustrated in Figure 8 is merely one example, and the more appropriate modules may be adapted when implementing these functions; moreover, a portion of those functions may be implemented outside of the display 100. Typically, a portion of the functions illustrated in Figure 8 may be implemented in a server device (cloud system) or a desired local server connected to the display 100 via a network.

#### H. Processing Examples

**[0062]** Examples of the processing provided in the display 100 according to an embodiment are described below. In the explanation that follows, for simplicity the processing example is described on the basis of requiring a predetermined authentication process for only a user having administrator privileges (admin), and not requiring any kind of authentication process for a user having no administrator privileges (normal user). An administrator may login via input entered on the display 100 itself (console input), or additionally, via input through a client device 300.

**[0063]** Additionally, access from the client device 300 to the display 100 is implemented through VNC, and is therefore referred to as a "VNC connection" below.

##### H-1: First Processing Example

**[0064]** In the first processing example, the HMI screen is presented on one page. The following explanation assumes that an administrator is previously logged into the display 100. Figure 9(A) through Figure 12(B) are schematic views for describing the first example of the processing performed in a display 100 according to an embodiment.

**[0065]** Figures 9(A), 9(B), 9(C), and 9(D) illustrate a processing example where a normal user accesses the display 100 through a client device 300 while an administrator is logged into the display 100.

**[0066]** As illustrated in Figure 9(A) while a certain user is logged into the display 100 with administrator privilege-

es, the normal user attempts a VNC connection. Note that in the case depicted in Figure 9(A) the display 100 presents an administrator HMI screen 180.

**[0067]** On detecting a VNC connection with normal user privileges, the display 100 presents a warning message 182 on the HMI screen 180 as illustrated in Figure 9(B). The warning message 182 notifies of you are a viewer that a VNC connection request was made by a normal user, and presents a list of selectable actions to deal with the VNC connection from the normal user. That is, the user management function in the display 100 notifies an administrator (first user) assigned administrator privileges (a first privilege) of a normal user (second user) assigned normal user privileges (a second privilege) that is lower than the administrator privileges attempting to access the display 100 when the normal user attempts to access the display while the administrator is accessing the display 100.

**[0068]** When an administrator selects "Reject the connection" in the warning message 182 displayed in Figure 9(B), the request for VNC connection from the normal user is rejected. Namely, the display 100 does not permit the normal user to access the display 100 in response to an instruction from the administrator.

**[0069]** At this point, the display 100 provides an alert message 310 to the client device 300 (normal user) making the VNC connection request. At the same time, the display 100 provides notification in an alert message 184 on its own display unit 122 that the VNC connection requested the normal user was rejected.

**[0070]** In contrast, as illustrated in Figure 9(D), VNC connection from a user having administrator privileges is permitted because the privileges are the same as the user that is previously logged in. In other words, simultaneous logins into the display 100 by an administrator are possible via the console and via the client device 300. Note that when an administrator establishes a new VNC connection, the display 100 presents an event message 186 on the display unit 122 itself to provide notification that an administrator established a VNC connection. An administrator HMI screen 180 can be presented to the client device 300 (admin) with which the VNC connection was established via the VNC connection.

**[0071]** Once a VNC connection from an administrator an administrator is terminated an event message may be presented to provide notification that the VNC connection was terminated.

**[0072]** Figures 10(A), 10(B), and 10(C) illustrate the processing that takes place when in the above-mentioned processing the administrator selects "Log me out and allow the connection" from the warning message 182 shown in Figure 9(B). On detecting a VNC connection with normal user privileges, the display 100 presents a warning message 182 on the HMI screen 180 as illustrated in Figure 10(A). In the administrator selects "Log me out and allow the connection" from the warning message 182 displayed in Figure 10(A), the administrator is logged out and the VNC connection from the normal user

becomes possible as illustrated in Figure 10(B). Namely, the display 100 terminates the access to the display 100 as an administrator in response to an instruction from the administrator.

**[0073]** In this manner, the user management function in the display 100 terminates access to the display 100 as an administrator (first user) assigned administrator privileges (a first privilege) when a normal user (second user) assigned normal user privileges (a second privilege) that is lower than the administrator privileges attempts to access the display 100 while the administrator assigned the administrator privilege is accessing the display 100.

**[0074]** At this point the user logged in with administrator privileges is now accessing the display 100 as a normal user. In other words, a normal user is now accessing the display 100 from both the display 100 and the client device 300. At this point, the display 100 presents an alert message 188 on its own it display unit 122 indicating that the user logged in as an administrator has been logged out in order to permit the VNC connection from a normal user.

**[0075]** After logging out the admin, the display 100 in the client device 300 each display a normal user HMI screen 181. That is, in the state illustrated in Figure 10(B), the extent to which the HMI screen may be viewed or manipulated is limited to within the privileges assigned to a normal user. In the example of HMI screen illustrated in Figure 4(A) and 4(B), for instance the state where the normal user is not able to display or download or upload a recipe is preserved. In this manner, placing limitations on the HMI screen displayed ensures this kind of information remains secure against access from the client device 300.

**[0076]** Given that a normal user is accessing the display 100 from the display 100 and the client device 300 in the case illustrated in Figure 10(B), the display 100 may be configured so that a user having administrator privileges cannot log in with the administrator privileges. That is, as illustrated in Figure 10(C) an administrator that is temporarily logged out cannot log in with administrator privileges while there is a VNC connection for a normal user. The login is rejected even if the administrator performs the login procedure. In this case, the display 100 provides a warning message 190 on the HMI screen 181 detailing why the login cannot be completed.

**[0077]** However, the display 100 may be configured to prioritize a login from an administrator relative to access from a normal user. That is, the display 100 may be configured to block access from the normal user if a login from an administrator is successful while the normal user is on the VNC connection.

**[0078]** On one hand, the administrator may login if the VNC connection for the normal user is terminated, or is disconnected as illustrated in Figure 11(A). Namely, if there is no VNC connection from a normal user the administrator may login. Figure 11 (B) illustrates when an administrator has logged in again, and in this case the



display 100 presents the administrator HMI screen 180.

**[0079]** Note that as illustrated in Figure 11(C), if another administrator has created a VNC connection, logging into the display 100 as an administrator is possible. Alternatively, access to the display 100 via a VNC connection from a user having administrator privileges is permitted when an administrator is logged into the display 100. In this case, the administrator HMI screen 180 is presented on the display 100 and the client device 300 respectively.

**[0080]** The above Figure 10(A) illustrates when an administrator is logged into the display 100; in this case, a normal user may create a VNC connection remote viewing or operation are not permitted. Therefore, when the display 100 receives a request for a VNC connection from a normal user, the user logged in with administrator privileges is presented a warning message 182. For instance, when a normal user needs to perform remote maintenance or remote operations, the administrator may log out voluntarily. If the warning message 182 is not provided, the administrator logged into the display 100 will remain unaware of the normal user's request for a VNC connection, creating a bug where the normal user can never access the display 100. Therefore, the warning message 182 is preferably presented when there is a request for a VNC connection from a normal user to alert the administrator of the situation.

**[0081]** Figures 12(A) and 12(B) illustrate the processing that takes place when the administrator selects "Allow the connection, view only" from the warning message 182 shown in Figure 9(B). On detecting a VNC connection with normal user privileges, the display 100 presents a warning message 182 on the HMI screen 180 as illustrated in Figure 12(A). When the administrator selects "Allow the connection, view only" from the warning message 182 shown in Figure 12(A), access to the display 100 from the normal user is permitted as illustrated in Figure 12(B) and the administrator HMI screen 180 presented on the display 100 is also presented on the client device 300. However, the administrator HMI screen 180 is preferably only available to the normal user for viewing, and interactions therewith are preferably prohibited. That is, the display 100 permits the normal user access to the HMI screen 180 (interface screen) with greater limitations than the limitations on the administrator in response to an instruction from the administrator.

**[0082]** In the configuration example illustrated in Figure 12(B), while the normal user is permitted to view the HMI screen 180, the user cannot perform any interactions with the screen. Therefore, this configuration is preferably applied when needing to permit remote maintenance of, but prohibit remote operations on the control device 200.

**[0083]** As illustrated in Figure 12(B), when access from the normal user is permitted, the display 100 presents a warning message 192 to that effect on its on the display unit 122.

**[0084]** As above described, the embodiment manages

the login and controls the content displayed on an HMI screen in accordance with the privileges of the user using the display 100 and one or more client devices 300 respectively to thereby realize the appropriate security level. To summarize, the embodiment realizes the security level required by combining the procedure for limiting the VNC connection from a normal user while a user with administrator privileges is logged in, and the procedure for causing the administrator to logout depending on the status of the VNC connection from the client device 300.

**[0085]** Although the administrator is given three selectable options in the implementation of the warning message 182 (Figures 9(B), 10(A), and 12(A)) in the above-described processing example, all the options presented in the example need not be implemented. It is sufficient to have at least one option that may be executed in accordance with the policies of the operator of the control system 1.

**[0086]** Furthermore, although in the above-described processing example the administrator made an explicit selection to execute log out processing, this kind of processing where a user makes an explicit selection may be omitted. Instead, the administrator may be automatically logged out after the VNC connection from the normal user is detected.

**[0087]** As illustrated in Figures 10(A), 10(B), and 10(C), when a user with fewer privileges attempts remote access (VNC connection), the administrator is logged out to return the display 100 to a secure state. Adopting this technique prevents an administrator from unknowingly leaking information to a client device 300 logged on via a VNC connection, and prevents erroneous operations through the wrong input to the display.

**[0088]** As described in the first processing example, the display 100 according to the embodiment the user management function restricts a normal user (second user) assigned normal user privileges (a second privilege) lower than the administrator privileges (a first privilege) from access to an HMI screen (interface screen) generated for an administrator (a first user) assigned the administrator privileges (first privilege).

**[0089]** Next, the procedures for implementing the above first processing example are described. Figure 13 is a flowchart for describing the processing procedure in the first processing example in a display 100 according to an embodiment. Each of the steps illustrated in Figure 13 are realized by running a program on the processor 102 in the display 100.

**[0090]** The processor 102 in the display 100 determines whether or not a request for login was received from an administrator. When a request for administrator login is received (YES, in step S100), the processor 102 executes an authentication process for the administrator (step S102).

**[0091]** When no request for administrator login is received (NO, at step S100), or after executing step S102, the processor 102 dynamically generates (or updates) an HMI screen to reflect the field signals exchanged with

the control device 200 (step S104). The processor 102 changes the content displayed in accordance with the privileges of the user operating the display 100 (i.e., in accordance with whether or not an administrator is logged in).

**[0092]** The processor 102 determines whether or not there was some user interaction with the HMI screen (step S106). When there is some kind of user interaction with respect to the HMI screen (YES, at step S106), the processor 102 executes processing corresponding to the user interaction detected (step S108). Typically, a process is executed that outputs some kind of internal command to the control device 200.

**[0093]** The processor 102 then determines whether or not a request for VNC connection was received from any client devices 300 (step S110). When no requests for a VNC connection are received from any client devices 300 (NO, at step S110), processing is repeated from step S100.

**[0094]** In contrast, when a request for a VNC connection is received from any of the client devices 300 (YES, step S110), the processor 102 determines whether or not a user having administrator privileges is currently logged into the display 100 (step S112). When a user having administrator privileges is not currently logged in to the display 100 (NO, step S112), the processor 102 establishes a VNC connection between the display 100 and the client device 300 originating the request for the VNC connection (step S114). Processing then repeats from step S100. Note that when a VNC connection is established, the screen image generated is presented on the display 100 as well as the client device 300 with the established VNC connection.

**[0095]** When a user having administrator privileges is currently logged into the display 100 (YES, at step S112), the processor 102 determines whether or not the user requesting the VNC connection has administrator privileges (step S116). When the request for a VNC connection is made by user having administrator privileges (YES, at step S116), the processor 102 runs in authentication process with respect to the user requesting the VNC connection (step S118). When the authentication process completes successfully, the processor 102 establishes a VNC connection between the client device 300 originating the request for the VNC connection and the display 100 (step S120). Processing then repeats from step S100. Note that when a VNC connection is established, the screen image generated is presented on the display 100 as well as the client device 300 with the established VNC connection.

**[0096]** When the request for a VNC connection is made by user having no administrator privileges, i.e., a normal user (NO, at step S116), the processor 102 presents a warning message 192 (e.g., Figure 9(B)) so that a selection can be made to deal with the request from the normal user for the VNC connection (step S122).

**[0097]** When the user presented with the warning message 192 selects "Reject the connection" ("Reject the

connection" from step S122), the processor 102 rejects the request for the VNC connection, sends the client device 300 requesting the VNC connection an alert message and outputs an alert message to the display unit 122 indicating that the VNC connection was rejected (step S126). Processing then repeats from step S100.

**[0098]** On the other hand, when the user presented with the warning message 192 selects "Log me out and allow the connection" ("Logout" at step S122), the processor 102 logs out the user (administrator) that is currently logged in (step S128), and regenerates the HMI screen dynamically to reflect the field signals exchanged between the display 100 and the control device 200 (step S130). The processor 102 then establishes a VNC connection between the client device 300 originating the request for the VNC connection and the display 100 (step S132). Processing then repeats from step S100. When a VNC connection is established, the screen image generated is presented on the display 100 as well as on the client device 300 with the established VNC connection.

**[0099]** In contrast, when the user presented with the warning message 192 selects "Allow the connection, view only" ("View only" at step S122), the processor 102 establishes a one-way VNC connection with the client device 300 originating the request for a VNC connection (step S134). On a one-way VNC connection means that while the screen image generated for providing the HMI screen is sent from the display 100 to the connected client device 300, the user interaction the client device 300 receives from the user is not sent to the display 100. Processing then repeats from step S100.

## H-2: Second Processing Example

**[0100]** Next, a processing example where multiple pages of the HMI screen are presented is described. The display 100 according to the embodiment is capable of setting the accessibility of pages on a user account basis. Even in this case where the user that may access each page differs, adopting the following steps ensure the information remains secure.

**[0101]** Figure 14 illustrates an example of setting the permissions for an HMI screen in a display 100 according to the embodiment. Referring to Figure 14, the HMI screen is assumed to have two pages: Page A and Page B. For instance, an administrator may be allowed to view and interact with Page A and Page B. In contrast, a normal user may be prevented from viewing and interacting with Page A, while being allowed to only view Page B.

**[0102]** Figures 15(A), 15(B), and 15(C) are schematic views for describing a second example of the processing performed in the display 100 according to the embodiment. Figures 15(A), 15(B), and 15(C) illustrate a processing example where a normal user accesses the display 100 via a client device 300\_1, and an administrator is accessing the display 100 via a client device 300\_2, while an administrator is logged into the display 100.

**[0103]** As illustrated in Figure 15(A), assume a normal user enters a normal user password into the client device 300\_1 and attempts to establish a VNC connection to the display 100, and an administrator enters an administrator password into the client device 300\_2 and attempts to establish a VNC connection to the display 100. In this example, both VNC connections from the client devices 300\_1 and 300\_2 are permitted to allow remote access to the display 100 (via VNC connection). However, as illustrated in Figure 14, the normal user has limited permissions with respect to a portion of the pages on the HMI screen, therefore, the display 100 limits the HMI screen presented to the normal user in accordance with the permissions indicated in Figure 14.

**[0104]** As illustrated in Figure 15(B), for instance, when instructed to display Page A of the HMI screen, the display 100 presents an HMI screen 180A corresponding Page A on its own display unit 122, and provides HMI screen 180A to the client device 300\_2 being used by the user logged in as an administrator. Whereas, given that the viewing and interaction with Page A of the HMI screen is limited for the normal user, the display 100 does not provide the HMI screen 180A to the client device 300\_1 being used by the user logged in as a normal user. At this point, the normal user does not have the privileges for displaying and HMI screen on the client device 300\_1, and an alert message 310 to that effect is displayed thereon. However, the VNC connection is maintained between the display 100 and the client device 300\_1. That is, the display 100 transmits a screen image representing the alert message 310 to the client device 300\_1 instead of a screen image of the HMI screen 180A.

**[0105]** Next, as illustrated in Figure 15(C), when instructed to display Page B of the HMI screen, the display 100 presents an HMI screen 180B corresponding Page B on its own display unit 122, and provides HMI screen 180B to the client device 300\_1 being used by the user logged in as a normal user, and to the client device 300\_2 being used by the user logged in as an administrator. However, the normal user does not have the rights to interact with the screen, and thus even if the user enters some kind of input into the client device 300\_1, the input is not considered valid. In other words, the display 100 treats any user interaction provided from the client device 300\_1 as invalid.

**[0106]** As illustrated in Figures 15(A), 15(B), and 15(C), when a user with less privileges attempts remote access (VNC connection), the viewing and interaction with the HMI screen can be controlled in accordance with preliminarily established privileges. Adopting this kind of method of restricting access prevents an administrator from unknowingly leaking information to a client device 300 logged on via a VNC connection, and prevents erroneous operations through the wrong input to the display. Additionally, in the above described second processing example, the environment can remain secure even in cases where a plurality of users having different privileges assigned are connected, such as during a videoconference

or an emergency response situation.

**[0107]** In particular, the display 100 according to the embodiment can set a security level for each page in an HMI screen, and moreover, can set the security level for viewing and interactions independently. Therefore, the display 100 can support various kinds of uses such as never showing a normal user a specific page in an HMI screen, or permitting only viewing of a specific page.

**[0108]** Note that when a plurality of users assigned different privileges are viewing or interacting with the same HMI screen, there are many cases where it would be ideal to understand the security level one has or the status of other users. A number of modification examples are described below.

**[0109]** Figure 16(A) and 16B are schematic views for describing modifications to the second example of the processing performed in the display 100 according to the embodiment.

**[0110]** Figure 16(A) illustrates a processing example where the privileges assigned to the client device 300 (i.e., to the user using the client device 300) can be understood at a glance. More specifically, pop-ups 194\_1 and 194\_2 representing the privileges assigned to each user are respectively displayed on top of the HMI screen 180B on the client device 300\_1 and 300\_2 respectively. In the example illustrated in Figure 16(A), the pop-up 194\_1 includes a message: "View only" which is the privilege assigned to the normal user using the client device 300\_1; similarly the pop-up 194\_2 includes the message: "Interactions okay" which is a privilege assigned to the administrator using the client device 300\_1.

**[0111]** A more specific method of implementation would be for the proxy 172 in the display 100 to overwrite the screen image use for providing the HMI screen with images corresponding to the pop-up 194\_1 and 194\_2, and to transmit the rewritten image to the client devices 300\_1 and 300\_2 respectively.

**[0112]** Figure 16(B) illustrates a processing example where an administrator currently interacting with HMI screen can verify the state of the client devices 300 (or, the user privileges) with established VNC connections. More specifically, a pop-up 196 indicating the number of persons per each user account accessing the display 100 from the client device 300 via a VNC connection is placed on the HMI screen 180B that is being displayed on the display 100, as well as the client devices 300\_1 and 300\_2. In the example illustrated in Figure 16(B), the pop-up 196 includes a message indicating that the number of normal users using the client device 300\_1 is one person, and the number of administrators using the client device 300\_1 is one person.

**[0113]** Note that instead of the display format illustrated in Figure 16(B), an exclusive system page may be prepared for displaying the status of the client device 300 (or the privileges of the user) accessing the display via a VNC connection.

## I. The Proxy

**[0114]** Next, the functions and processes that take place in the proxy 172 (Figure 8) in the display 100 is described. As above described, the proxy 172 provides a relay function that mediates the exchange of data between the VNC server 170 and one or a plurality of client devices 300.

### I-1: The User Authentication Process

**[0115]** An authentication process is run between the proxy 172 and each of the client devices 300 in accordance with a predetermined procedure. Any desired and publicly known technique may be adopted as the procedure for the authentication process, however, the challenge-response protocol is usually suitable. With the challenge-response protocol, when a connection request is sent to the proxy 172 from a client device 300, the proxy 172 sends a challenge to the client device 300, and the client device 300 further sends a challenge-response in relation to the challenge. The proxy 172 then performs the authentication process on the basis of the challenge-response received, and response to the client device 300 indicating the client device is authenticated when the authentication process completes successfully. The client device 300 may establish a VNC connection with the display 100 through this series of processes.

**[0116]** Note that in a general-purpose authentication process for establishing a VNC connection, there is no concept of a "user account"; authentication takes place using only a password. In other words, the challenge-response sent from the client device 300 to the proxy 172 contains only a password. In this case, the following kind of technique may be implemented in order to allow the general-purpose authentication process for establishing a VNC connection to use a user account and a password. Figures 17(A) and 17(B) are diagrams for explaining an example of an implementation of user authentication in a display 100 according to an embodiment.

#### Implementation Example: Case 1

**[0117]** In Case 1 of this implementation example, a unique port may be assigned to each user account to thereby identify the user account. For instance, as illustrated in Figure 17(A), two ports, i.e., port number 5900 and 5901 are setup in the proxy 172, with each of the port numbers being associated with an administrator and a normal user, respectively. Moreover, the proxy may be configured to allow usage of an administrator password and a normal-user password that are mapped to the specific port numbers.

**[0118]** Each user operates the client device 300 to specify the port corresponding to its own privilege and to request a VNC connection. Each user then enters the relevant password during the authentication process when establishing this VNC connection. For instance, an

administrator specifies the port number 5900 and enters their own password: "12345". The proxy 172 reads the password corresponding to the port number specified by the client device 300, and determines whether or not the password from the client device 300 matches.

**[0119]** Adopting such an implementation, commonly known applications may be used to set the security level for each user account.

### 10 Implementation Example: Case 2

**[0120]** In Case 2 of this implementation example, a merging of the user account and the password may be used as the password in the authentication process. For instance, as illustrated in Figure 17(B), the proxy 172 is configured so that an administrator password and a normal-user password may be used. Each user operates the client device 300, and uses a predetermined separator when merging information about their group attribute and password, and sends the result as a password. For instance, a character string representing the group attribute "Administrator" and a character string of their password "12345" may be merged with a designated separator, e.g. "\" therebetween and the result entered. If receiving the password from the client device 300 unaltered, the proxy 172 may separate the two character strings based on the separator "\", and then run the authentication process. Note that when receiving an encrypted password from the client device 300, the proxy 172 may use character string obtained from encrypting the result of the two character strings in the authentication process.

**[0121]** Adopting such an implementation, commonly known applications may be used to set the security level for each user account.

### I-2: Displaying the Status of the VNC Connection

**[0122]** The information maintained by the VNC server 170 can be reflected on the HMI screen presented on the display 100.

**[0123]** For example, a status screen indicating the states of the VNC connection managed by the VNC server 170 may be displayed as an HMI screen. This kind of status screen may be a list of the user name, the IP address of the client device 300 used by each user, and when the VNC connection started for the VNC connections.

**[0124]** A user may manually activate the status screen from a system menu; the status screen presents the state of the VNC connections. For instance, the user may select an icon on the HMI screen to activate the status screen. Alternatively, the detection of the VNC connection by the VNC server 170 may be a trigger event that activates the status screen. Yet another alternative, may be to activate the status screen in response to the selection of a button on the HMI screen through a user interaction.

**[0125]** Finally, displaying the state of the VNC connections may be utilized as a control component used on the HMI screen. Preparing this kind of control component allows the user to cause the state of the VNC connections to be displayed at any desired location or page. Additionally, an event-driven message may be generated on the HMI screen in accordance with the start of a VNC connection and the like. Lastly, an always-present status bar may be prepared to provide the state of the VNC connections.

**[0126]** In this manner, the information on the status of the VNC connection may be included in the HMI screen presented on the display 100.

### I-3: Modification Examples

**[0127]** The above description, an example was given of using a VNC to realize a connection between the display 100 and the client device 300; however, other communication protocols may be adopted. Given that the display 100 according to the embodiment implements a proxy, there is no need to be limited to a specific communication protocol, and thus any desired communication protocol may be flexibly adopted. For example, a file transfer protocol (FTP), a hypertext transfer protocol, and the like may be used for the communication protocol.

**[0128]** When FTP is adopted as the communication protocol, the protocol should be implemented so that communication is only possible when a user having administrator privileges is logged in (or, only when a flag permitting FTP is on). By limiting the time period when this kind of FTP communication is permitted allows the system to protect the data that should not be accessed externally such as manufacturing data. In other words, it is sufficient to permit FTP communications from outside only in the case where an administrator is logged into the display 100.

**[0129]** An FTP connection may also be prohibited depending on the status of the display 100. For instance, the protocol may be configured so that file transfers cannot take place via FTP while the manufacturing devices operating. That is, ensuring that FTP is only possible when the manufacturing device is stopped protects the data such as manufacturing parameters that should not be updated while the manufacturing device is running.

**[0130]** Note that, the user may be warned during the FTP connection (i.e. when receiving files for sending files like). For instance, the user may be notified that an FTP transfer is taking place within message or an indicator to alert the user to the status. Alerting the user in this manner may prevent erroneous operation, such as powering down the display 100 during an FTP transfer.

**[0131]** Given that the settings of a normal FTP server do not change dynamically, more flexible operations may be possible by having the proxy change its mode of actions depending on the status of the display 100.

**[0132]** When the HTTP is adopted as the communication protocol, functions identical to using a VNC may be

realized even when implementing a remote maintenance function that uses a web browser and the like.

### J. Advantages

**[0133]** As above described a programmable display 100 according to the embodiments which provides functions that allow remote viewing and interaction with the content displayed thereon, is capable of appropriately preserving the security level of the content displayed even when providing these kinds of functions. Namely, compared to conventional devices the programmable display 100 according to the embodiments remains convenient, and improves the security level provided thereby.

**[0134]** More specifically, by adopting the following kinds of control the programmable display 100 prevents assigning unnecessary privileges to a client device 300.

**[0135]** For instance, the programmable display 100 can control the logging in and logging off of each user depending on the status of a VNC connection from a client device 300. Namely, the programmable display 100 according to the embodiment can change whether or not to display or to make a control component available dynamically for each control component placed on the HMI screen in accordance with the privileges assigned to the user operating the client device 300. Additionally, the programmable display 100 can control interaction or viewing via the VNC connection and the client device 300 depending on the privileges assigned to the user logged thereinto. The programmable display 100 can also control the limitations on the viewing and interaction with the HMI screen on a page-by-page basis, and the limitations on viewing and interaction that is made on the page level may be controlled in accordance with the privileges of the user operating the client device 300. Additionally, a plurality of user accounts may be created and privileges of mutually different levels established for each of the user accounts. For instance, creating a plurality of user accounts, such as an administrator, normal user, operator, and repair staff, each having different permissions, allows minute control of access to a plurality of pages in an HMI screen.

**[0136]** All aspects of the embodiments disclosed should be considered merely examples and not limitations as such. The scope of the present invention is not limited to the above description but to the scope of the claims, and is intended to include all equivalents and modifications allowable by the scope of the claims.

### Reference Numerals

#### **[0137]**

1	Control system
2	Production site
4	Remote site
6, 8, 10	Network

12, 14	Field Bus	
100	Programmable display (display)	
102	Processor	
104	Main memory	
110	Flash Memory	5
112	Network interface	
114	I/O Interface	
116	Field bus interface	
120	Touchscreen	
122	Display Unit	10
124	Touchscreen panel	
130	Internal bus	
150	Data storage unit	
152	HMI screen settings data	
154	User Registration Data	15
160	Rendering Unit	
162	I/O Data Manager	
164	User Manager	
166	Display Output Unit	
168	User Input Receiver	20
170	VNC Server	
172	Proxy	
200	Control Device	
202	Remote I/O device	
300	Client device	25

## Claims

1. A programmable display (100) for connection to a control device (200), the programmable display (100) comprising:
  - a user management unit (164) configured to identify a user accessing the programmable display (100);
  - a generation unit (160) configured to generate an interface screen (180) containing information from the control device (200) in accordance with privileges assigned to the user identified by the user management unit (164);
  - a display unit (122) configured to output the interface screen (180);
  - a connection management unit (170) configured to, in response to a request for access from a user on an external device (300), establish a connection with the external device (300) on the basis of identification of the user by the user management unit (164), and to send the interface screen (180) to the external device (300) with which a connection is established;
  - wherein the user management unit (164) is configured to prohibit simultaneous access to the programmable display (100) by a plurality of users each having different privileges assigned, and to allow simultaneous access to the programmable display (100) by a plurality of users each having the same privileges assigned,

## characterized in that

the user management unit (164) is configured to terminate access to the programmable display (100) as a first user assigned a first privilege when a second user assigned a second privilege that is lower than the first privilege attempts to access the programmable display (100) while the first user assigned the first privilege is accessing the programmable display (100).

2. The programmable display (100) according to claim 1, wherein the user management unit (164) is configured to notify a first user assigned a first privilege of a second user assigned a second privilege that is lower than the first privilege attempting to access the programmable display (100) when the second user attempts to access the programmable display (100) while the first user is accessing the programmable display (100).
3. The programmable display (100) according to claim 1 or 2, wherein the user management unit (164) is configured to deny the access of the second user to the programmable display (100) in response to an instruction from the first user.
4. The programmable display (100) according to any one of claims 1-3, wherein the user management unit (164) is configured to terminate access to the programmable display (100) as the first user in response to an instruction from the first user.
5. The programmable display (100) according to any one of claim 1 - 4, wherein the user management unit (164) is configured to permit the second user to access the interface screen (180) with greater limitations than the limitations on the first user in response to an instruction from the first user.

## Patentansprüche

1. Programmierbare Anzeige (100) zum Verbinden mit einer Steuervorrichtung (200), wobei die programmierbare Anzeige (100) aufweist:

eine Benutzerverwaltungseinheit (164), die dazu eingerichtet ist, einen Benutzer, der auf die programmierbare Anzeige (100) zugreift, zu identifizieren;

eine Erzeugungseinheit (160), die dazu eingerichtet ist, einen Interface-Bildschirm (180) zu erzeugen, der Informationen aus der Steuervorrichtung (200) in Übereinstimmung mit Rechten enthält, die einem Benutzer zugewiesen sind, der durch die Benutzerverwaltungseinheit (164) identifiziert wurde;

eine Anzeigeeinheit (122), die eingerichtet ist,

den Interface-Bildschirm (180) auszugeben;  
eine Verbindungsverwaltungseinheit (170), die  
eingerichtet ist, in Antwort auf eine Anfrage für  
einen Zugriff von einem Benutzer auf einer ex-  
ternen Vorrichtung (300) eine Verbindung mit  
der externen Vorrichtung (300) anhand der  
Identifikation des Benutzers durch die Benutzer-  
verwaltungseinheit (164) aufzubauen und den  
Interface-Bildschirm (180) an die externe Vor-  
richtung (300), mit welcher eine Verbindung auf-  
gebaut wurde, zu senden;

wobei die Benutzerverwaltungseinheit (164)  
eingerichtet ist, einen gleichzeitigen Zugriff auf  
die programmierbare Anzeige (100) durch meh-  
rere Benutzer, welche jeweils unterschiedliche  
Rechte zugewiesen haben, zu verbieten, und  
einen gleichzeitigen Zugriff auf die program-  
mierbare Anzeige (100) durch mehrere Benut-  
zer, welche die gleichen Rechte zugewiesen ha-  
ben, zu erlauben,

**dadurch gekennzeichnet, dass**

die Benutzerverwaltungseinheit (164) eingerich-  
tet ist, einen Zugriff auf die programmierbare An-  
zeige (100) als einen ersten Benutzer, dem ein  
erstes Recht zugewiesen ist, zu beenden, wenn  
ein zweiter Benutzer, dem ein zweites Recht zu-  
gewiesen ist, das niedriger als das erste Recht  
ist, versucht, auf die programmierbare Anzeige  
(100) zuzugreifen, während der erste Benutzer,  
dem das erste Recht zugewiesen ist, auf die pro-  
grammierbare Anzeige (100) zugreift.

2. Programmierbare Anzeige (100) gemäß Anspruch  
1, wobei die Benutzerverwaltungseinheit (164) ein-  
gerichtet ist, einen ersten Benutzer, dem ein erstes  
Recht zugewiesen ist, über einen zweiten Benutzer  
zu benachrichtigen, dem ein zweites Recht zugewie-  
sen ist, das niedriger als das erste Recht ist, der  
versucht, auf die programmierbare Anzeige (100)  
zuzugreifen, wenn der zweite Benutzer versucht, auf  
die programmierbare Anzeige (100) zuzugreifen,  
während der erste Benutzer auf die programmierba-  
re Anzeige (100) zugreift.

3. Programmierbare Anzeige (100) gemäß Anspruch  
1 oder 2, wobei die Benutzerverwaltungseinheit  
(164) eingerichtet ist, den Zugriff des zweiten Benut-  
zers auf die programmierbare Anzeige (100) in Ant-  
wort auf einen Befehl des ersten Benutzers zu ver-  
weigern.

4. Programmierbare Anzeige (100) gemäß einem der  
Ansprüche 1 bis 3, wobei die Benutzerverwaltungs-  
einheit (164) eingerichtet ist, den Zugriff auf die pro-  
grammierbare Anzeige (100) als erster Benutzer in  
Antwort auf einen Befehl des ersten Benutzers zu  
beenden.

5. Programmierbare Anzeige (100) gemäß einem der  
Ansprüche 1 bis 4, wobei die Benutzerverwaltungs-  
einheit (164) eingerichtet ist, dem zweiten Benutzer  
zu erlauben, auf den Interface-Bildschirm (180) mit  
größeren Einschränkungen zuzugreifen als die Ein-  
schränkungen des ersten Benutzers in Antwort auf  
einen Befehl des ersten Benutzers.

## Revendications

1. Dispositif d'affichage programmable (100) destiné à  
une connexion à un dispositif de commande (200),  
le dispositif d'affichage programmable (100)  
comprenant :

une unité de gestion d'utilisateurs (164) conçue  
pour identifier un utilisateur accédant au dispo-  
sitif d'affichage programmable (100) ;

une unité de génération (160) conçue pour pro-  
duire un écran d'interface (180) contenant des  
informations provenant du dispositif de com-  
mande (200) en conformité avec des privilèges  
attribués à l'utilisateur identifié par l'unité de ges-  
tion d'utilisateurs (164) ;

une unité d'affichage (122) conçue pour délivrer  
l'écran d'interface (180) ;

une unité de gestion de connexions (170) con-  
çue pour, en réponse à une demande d'accès  
émanant d'un utilisateur sur un dispositif externe  
(300), établir une connexion avec le dispositif  
externe (300) sur la base de l'identification de  
l'utilisateur par l'unité de gestion d'utilisateurs  
(164), et envoyer l'écran d'interface (180) au dis-  
positif externe (300) avec lequel une connexion  
est établie ;

dans lequel l'unité de gestion d'utilisateurs (164)  
est conçue pour interdire l'accès simultané au  
dispositif d'affichage programmable (100) à une  
pluralité d'utilisateurs disposant tous de privilè-  
ges attribués différents, et autoriser l'accès si-  
multané au dispositif d'affichage programmable  
(100) à une pluralité d'utilisateurs disposant tous  
des mêmes privilèges attribués,

**caractérisé en ce que :**

l'unité de gestion d'utilisateurs (164) est conçue  
pour mettre fin à un accès au dispositif d'afficha-  
ge programmable (100) en tant que premier uti-  
lisateur disposant d'un premier privilège, lors-  
qu'un second utilisateur disposant d'un second  
privilège qui est inférieur au premier privilège  
tente d'accéder au dispositif d'affichage pro-  
grammable (100), pendant que le premier uti-  
lisateur disposant du premier privilège accède au  
dispositif d'affichage programmable (100).

2. Dispositif d'affichage programmable (100) selon la revendication 1, dans lequel l'unité de gestion d'utilisateurs (164) est conçue pour informer un premier utilisateur disposant d'un premier privilège de la tentative d'accès au dispositif d'affichage programmable (100) d'un second utilisateur disposant d'un second privilège qui est inférieur au premier privilège, lorsque le second utilisateur tente d'accéder au dispositif d'affichage programmable (100), pendant que le premier utilisateur accède au dispositif d'affichage programmable (100). 5 10
3. Dispositif d'affichage programmable (100) selon la revendication 1 ou 2, dans lequel l'unité de gestion d'utilisateurs (164) est conçue pour refuser l'accès du second utilisateur au dispositif d'affichage programmable (100), en réponse à une instruction émanant du premier utilisateur. 15
4. Dispositif d'affichage programmable (100) selon l'une quelconque des revendications 1 à 3, dans lequel l'unité de gestion d'utilisateurs (164) est conçue pour mettre fin à un accès au dispositif d'affichage programmable (100) en tant que premier utilisateur, en réponse à une instruction émanant du premier utilisateur. 20 25
5. Dispositif d'affichage programmable (100) selon l'une quelconque des revendications 1 à 4, dans lequel l'unité de gestion d'utilisateurs (164) est conçue pour permettre au second utilisateur d'accéder à l'écran d'interface (180) avec des restrictions plus fortes que les restrictions imposées au premier utilisateur, en réponse à une instruction émanant du premier utilisateur. 30 35

40

45

50

55



FIG. 1

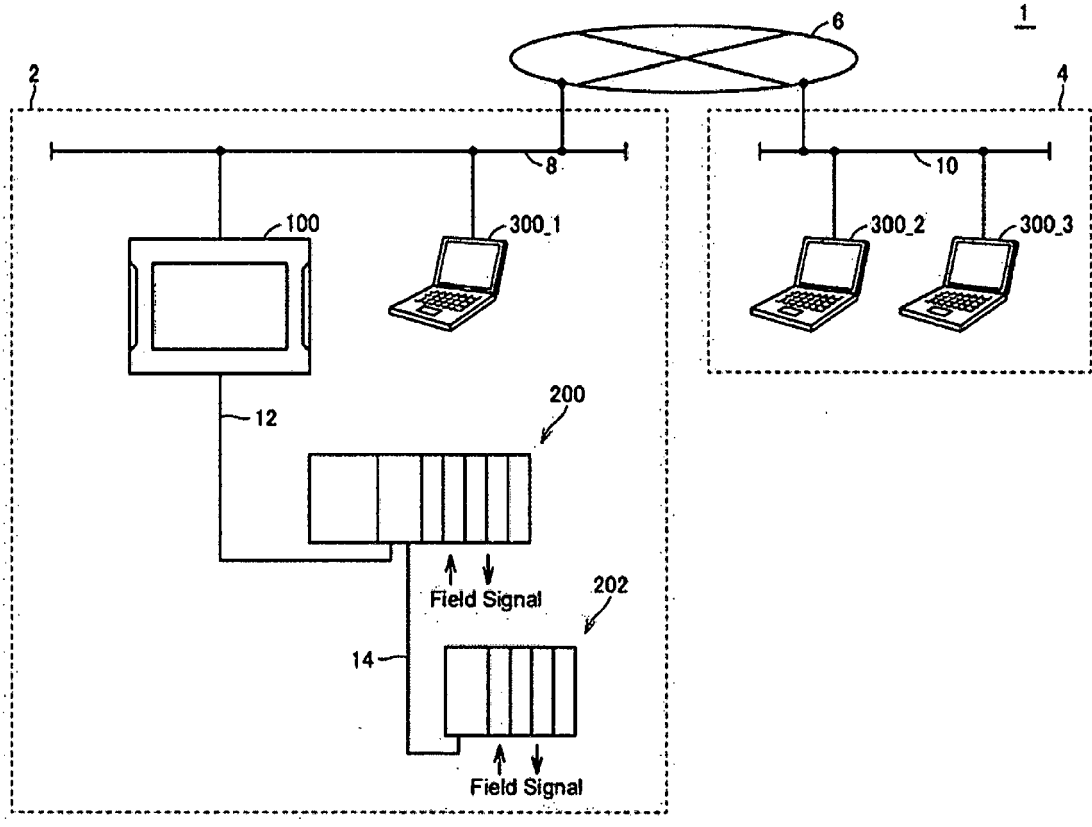


FIG. 2

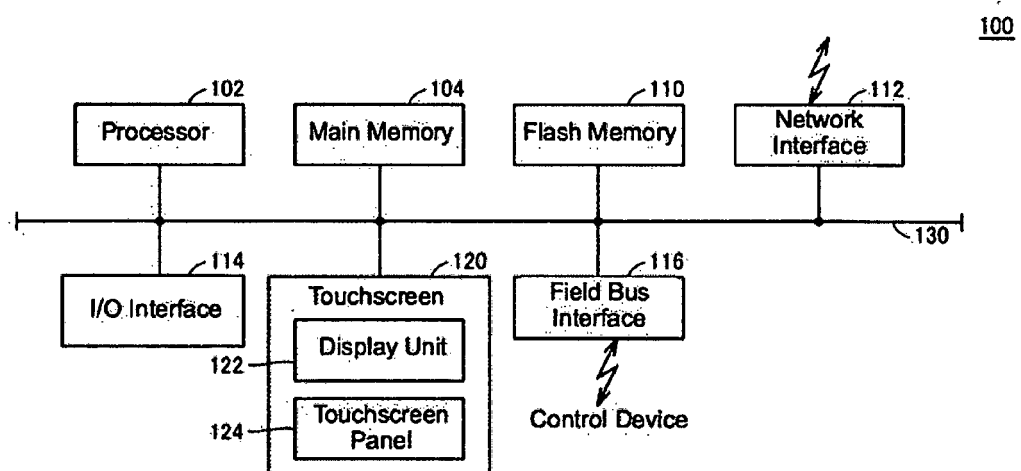


FIG. 3

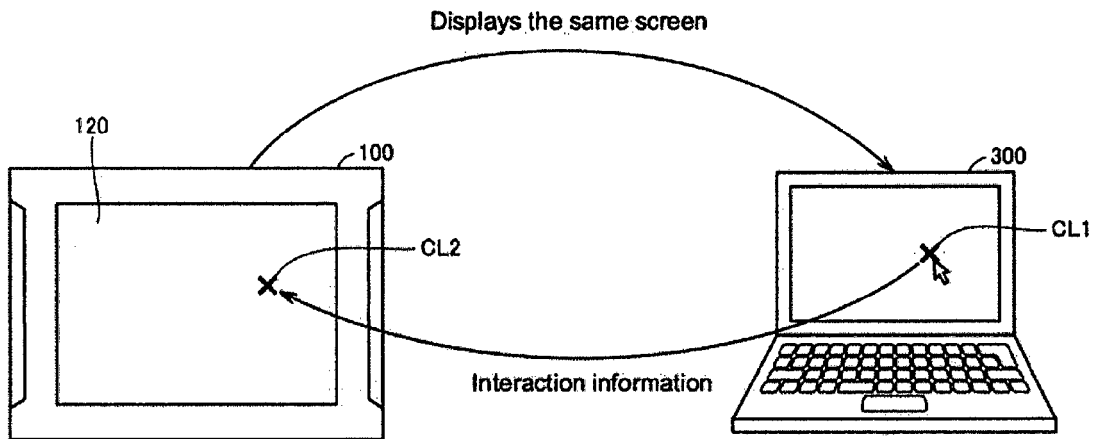


FIG. 4(A)

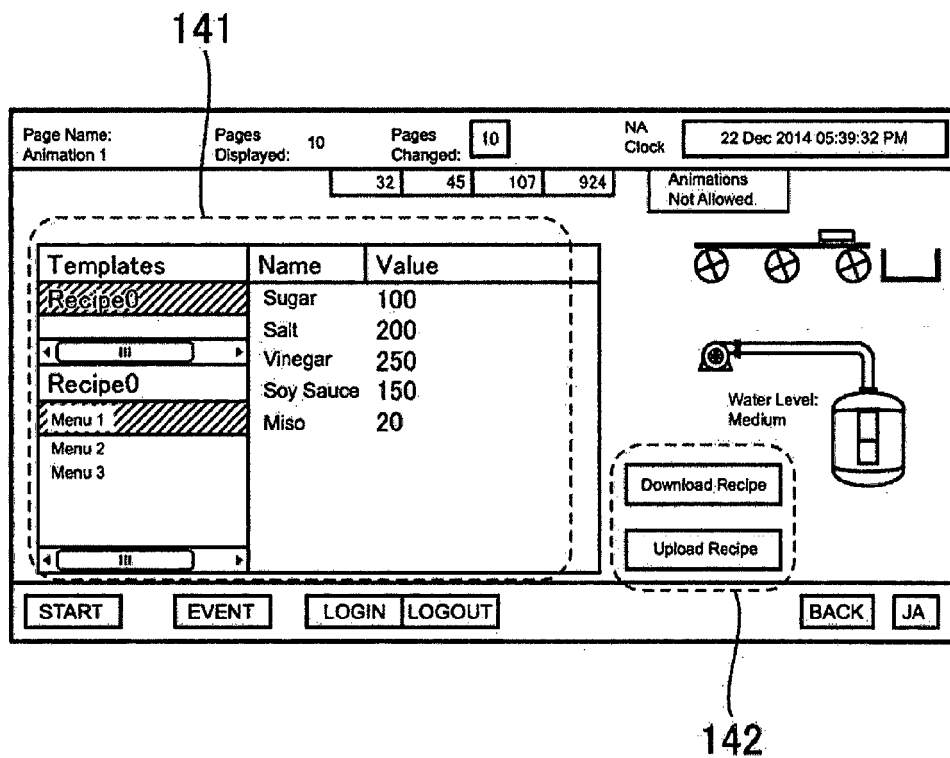


FIG. 4(B)

Page Name: Animation 1      Pages Displayed: 10      Pages Changed: 10      NA Clock: 22 Dec 2014 05:40:11 PM

11   3   10   798      Animations Not Allowed

You do not have administrator privileges.  
Recipe will not be displayed.

Water Level: Low

Download Recipe

Upload Recipe

START   EVENT   LOGIN   LOGOUT      BACK   JA

FIG. 5

Configuration and Settings

HMI   Security

▼ User Accounts

Name	Password	Type	Notes
UserB	*****	Operator	Operator
Administrator	*****	Administrator	Administrator
UserA	*****	User	TANAKA

401

▼ Privileges and Permissions

Privileges and Permissions	Level 1	Level 2	Level 3	Level 4	Level 5
Administrator	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
User	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Operator	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

402

▼ Security

System Menu - Permissions   Level 4 ▼

403

FIG. 6

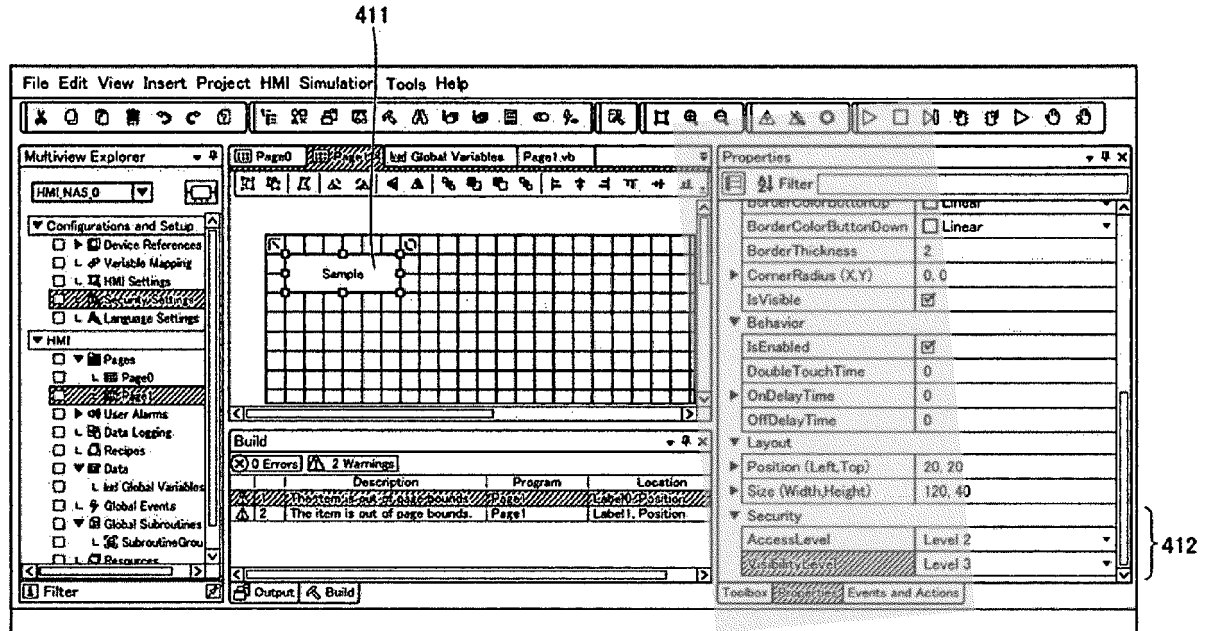


FIG. 8

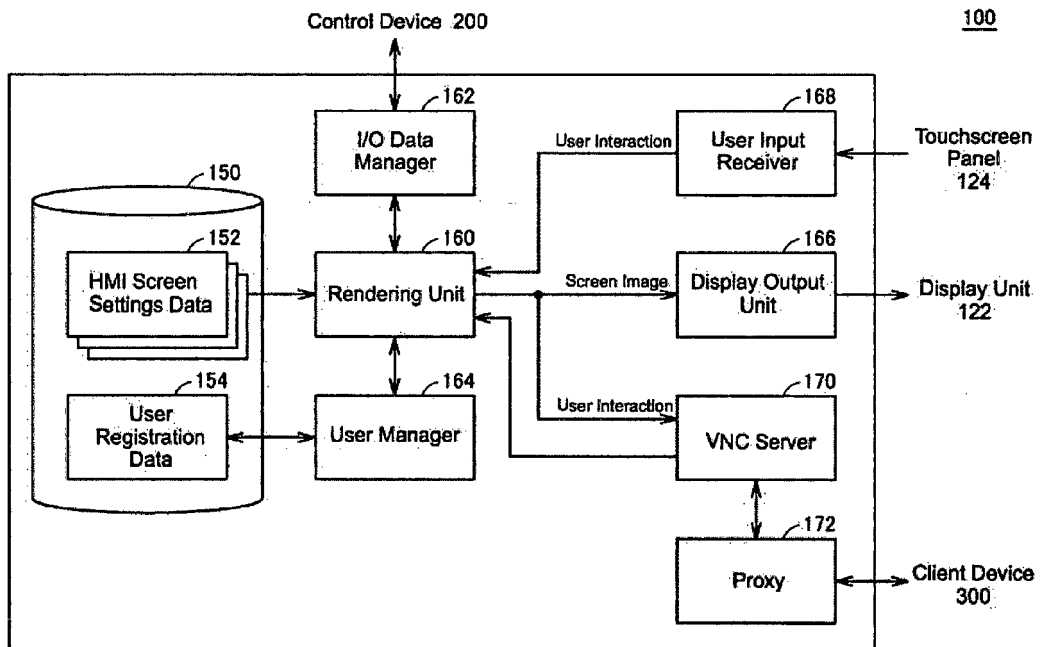


FIG. 7(A)

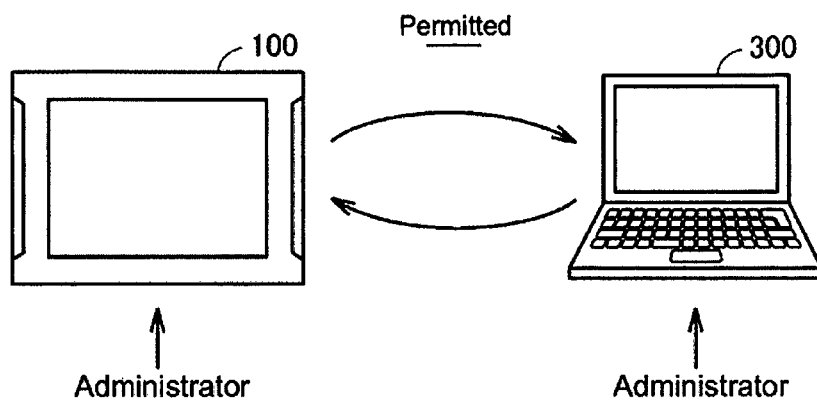


FIG. 7(B)

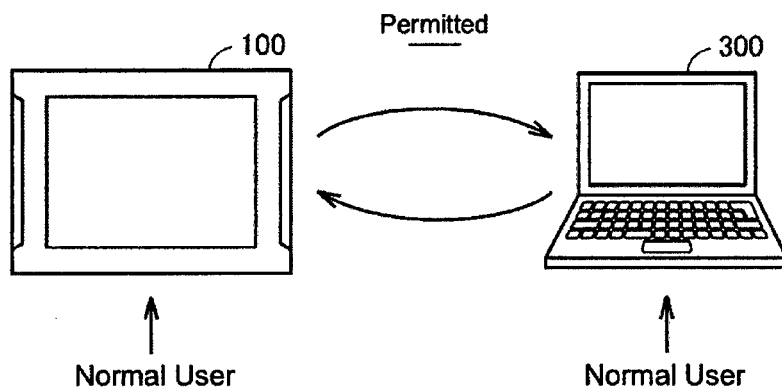


FIG. 7 (C)

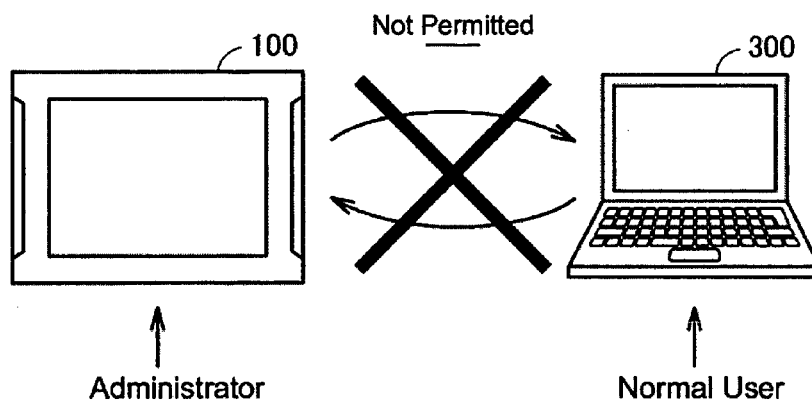


FIG. 9(A)

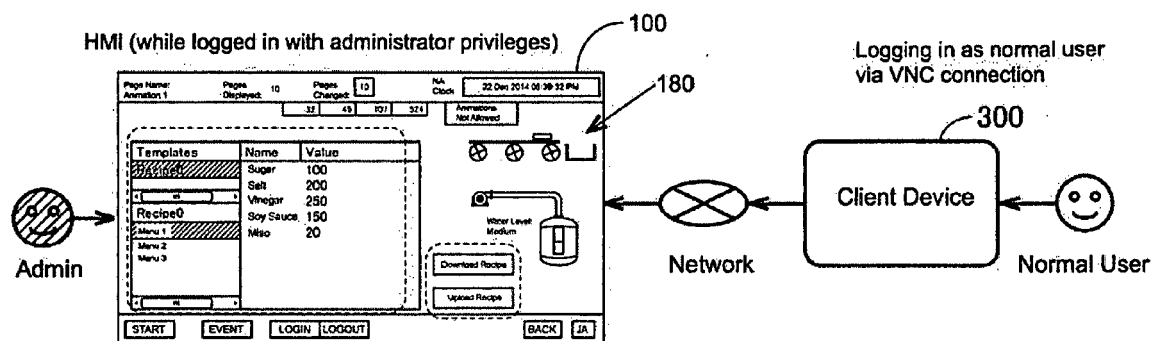


FIG. 9(B)

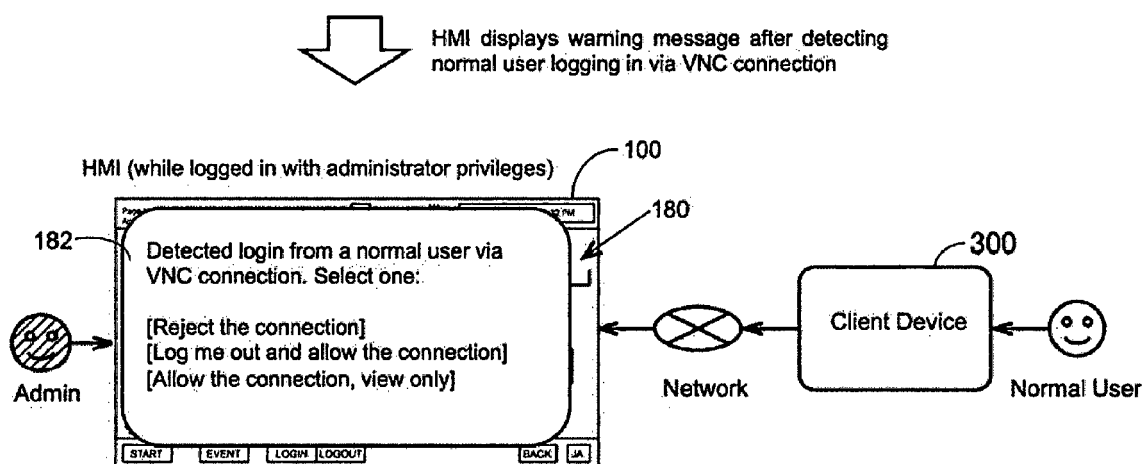


FIG. 9(C)

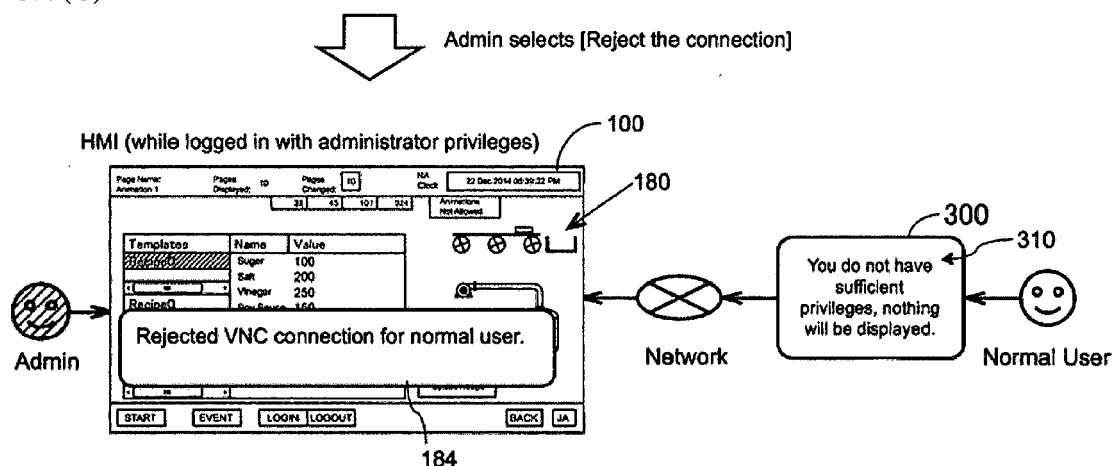


FIG. 9(D)

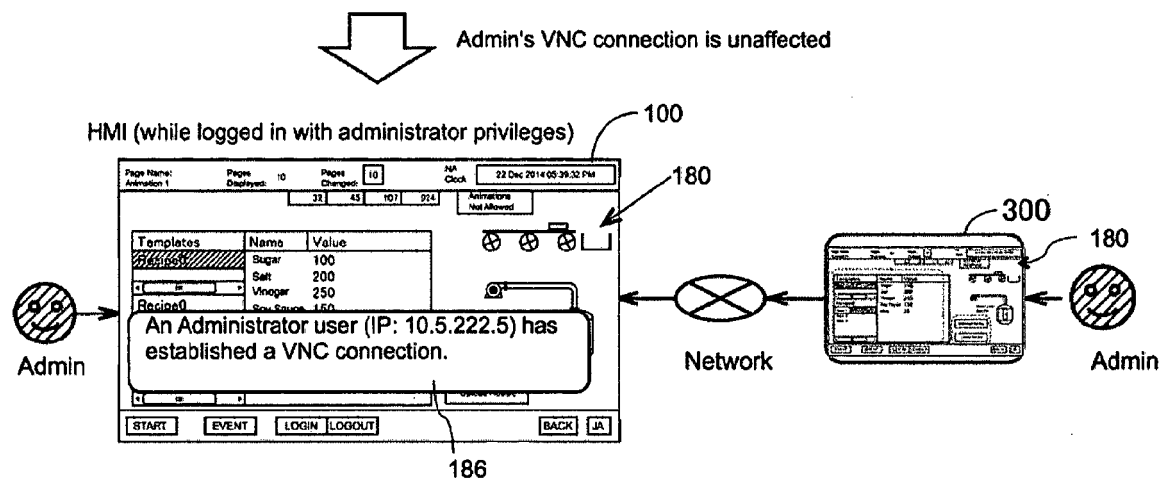


FIG. 10(A)

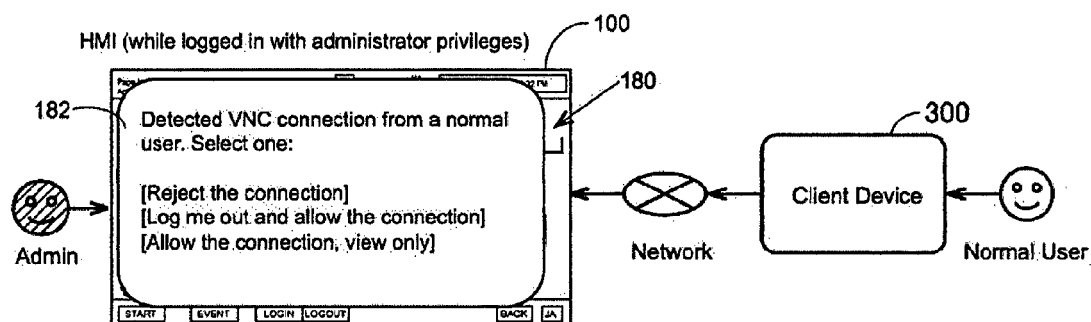


FIG. 10(B)

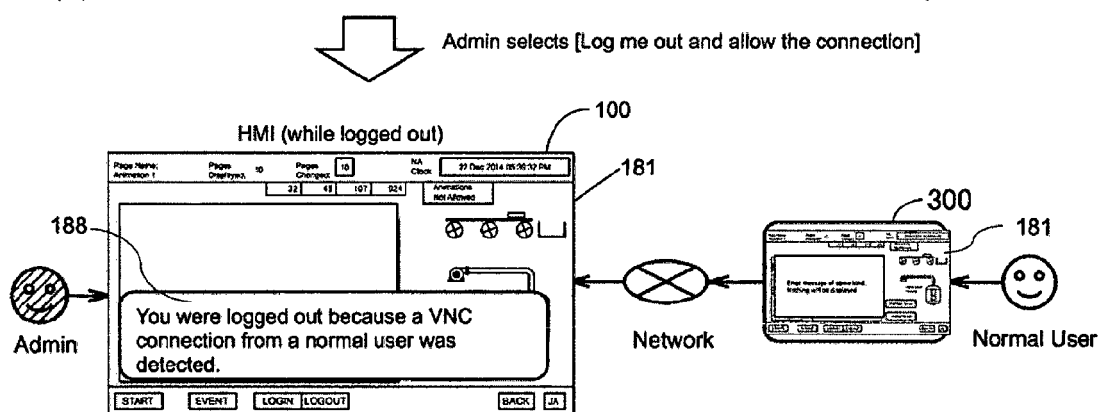


FIG. 10(C)

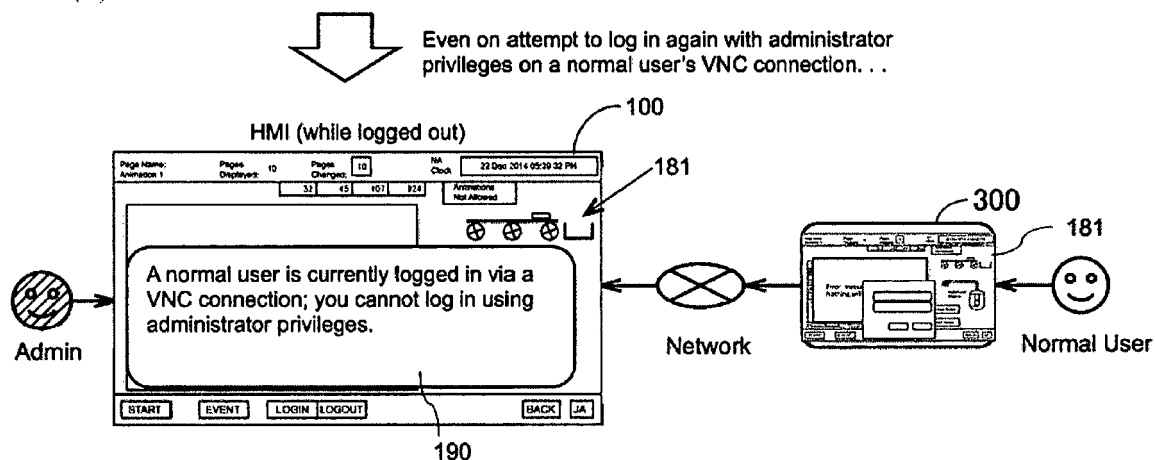


FIG. 11(A)

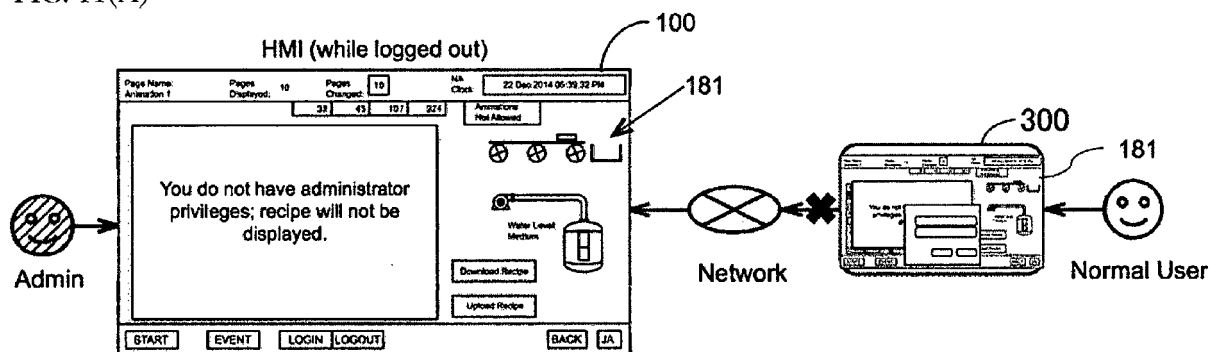
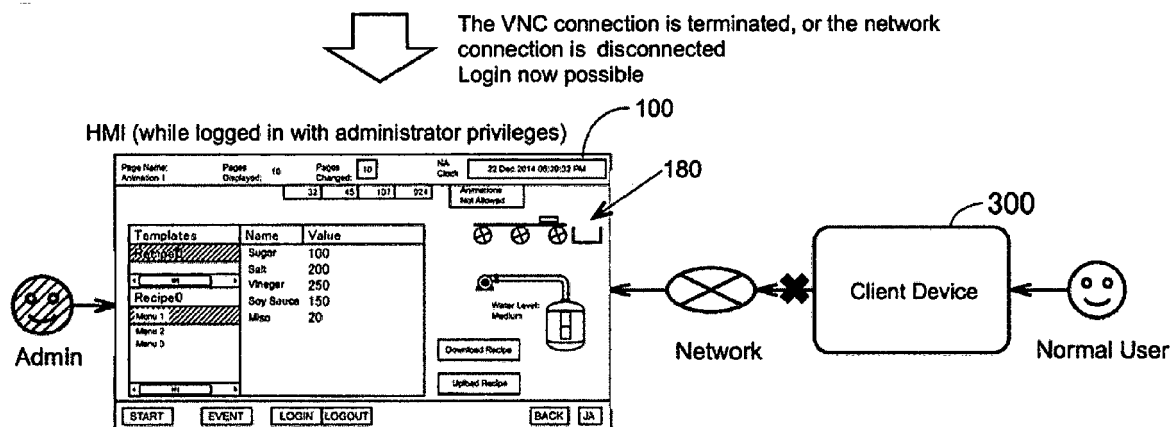


FIG. 11(B)



Log in possible if no VNC connection present



FIG. 11(C)

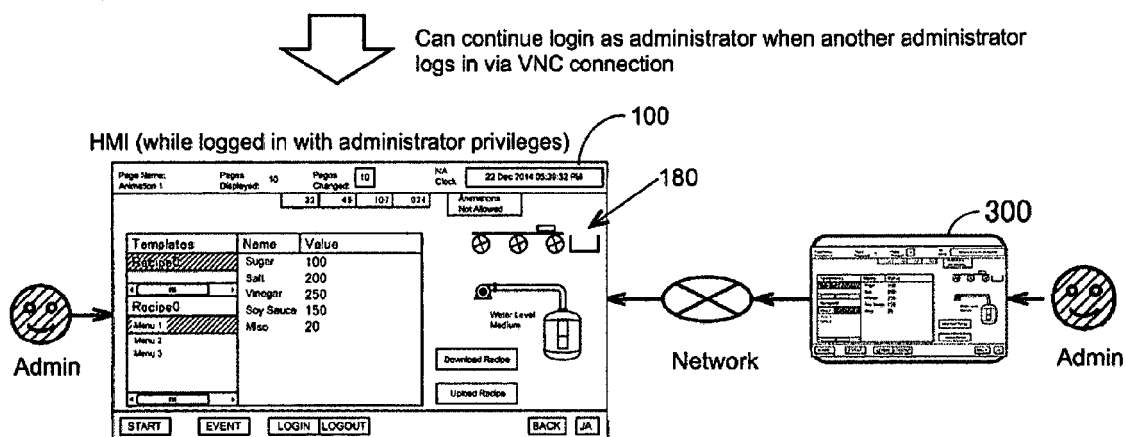


FIG. 12(A)

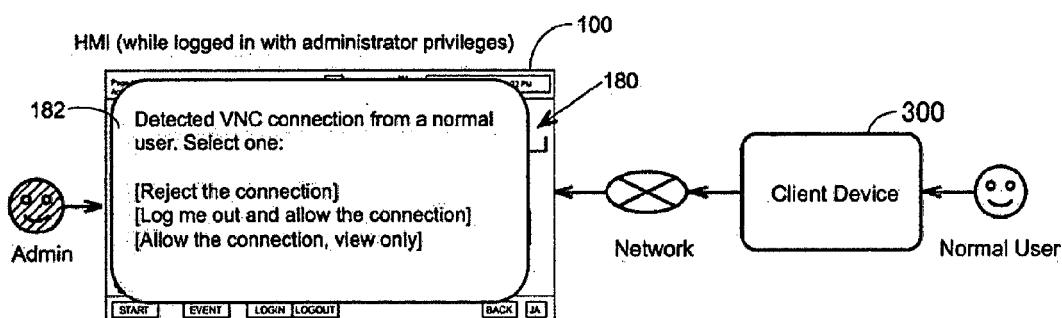


FIG. 12(B)

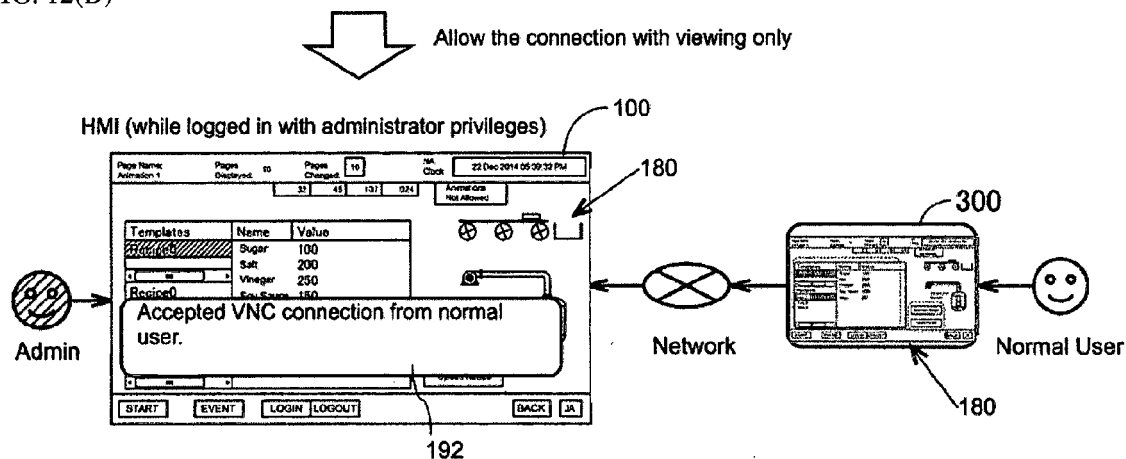


FIG. 13

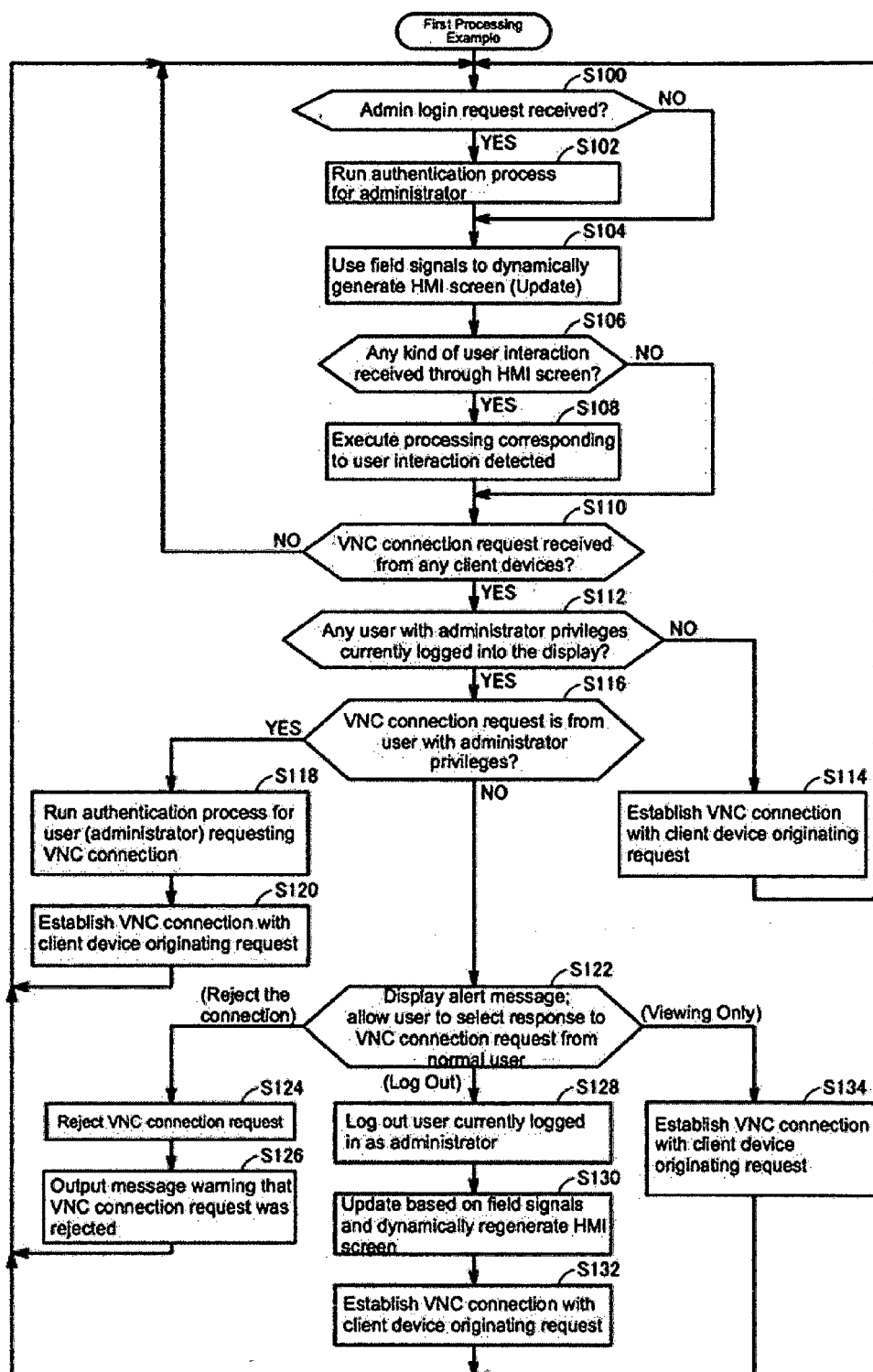


FIG. 14

	Administrator		Normal User	
	View	Control	View	Control
Page A	Allow	Allow	Deny	Deny
Page B	Allow	Allow	Allow	Deny

FIG. 15(A)

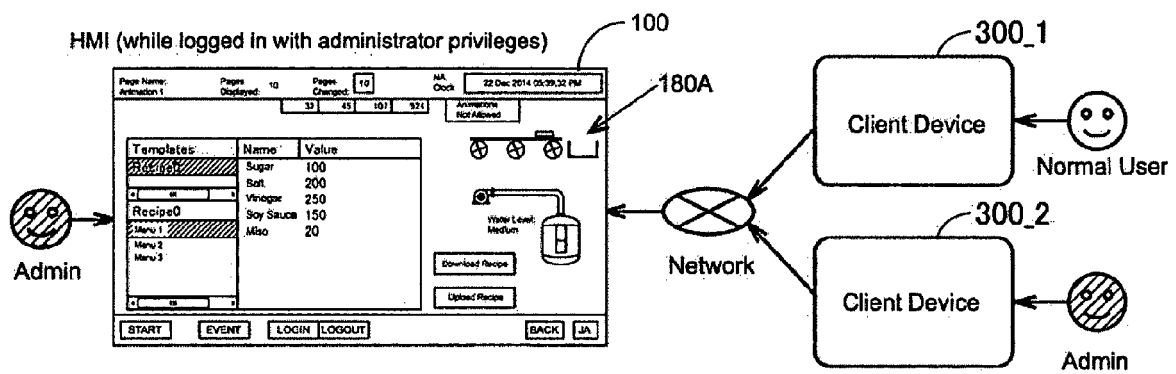


FIG. 15(B)

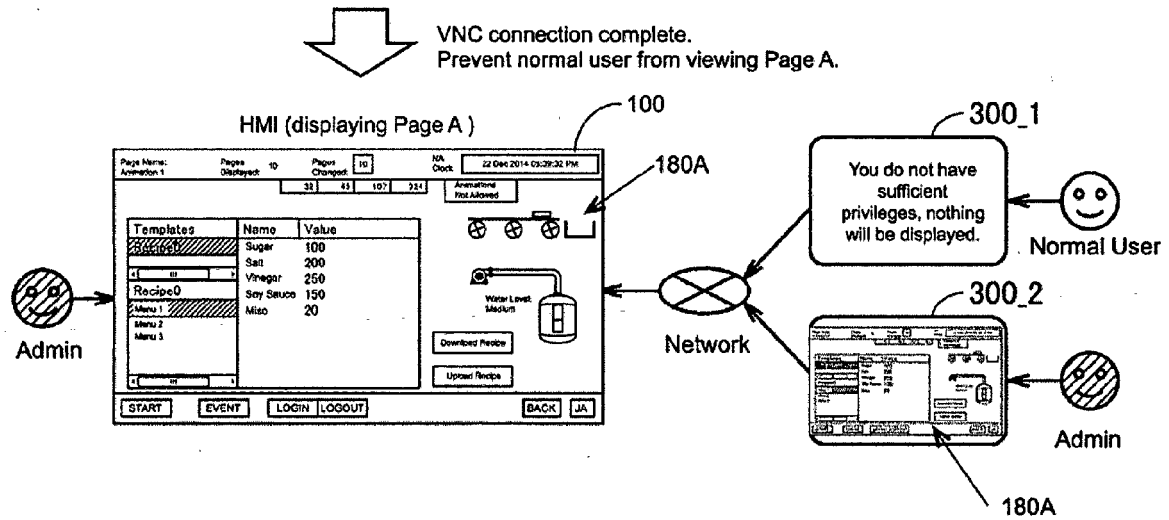


FIG. 15(C)

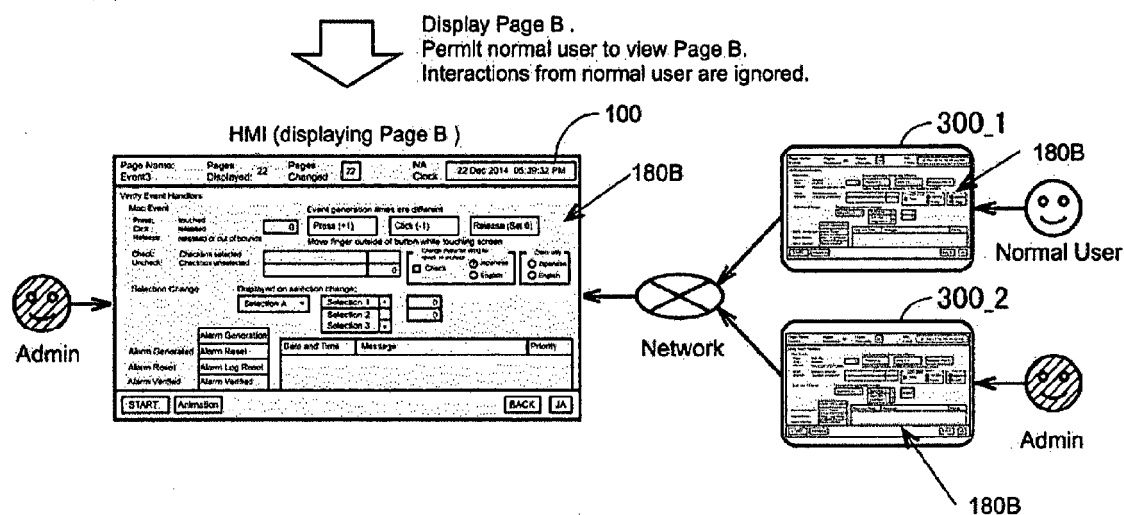


FIG. 16(A)

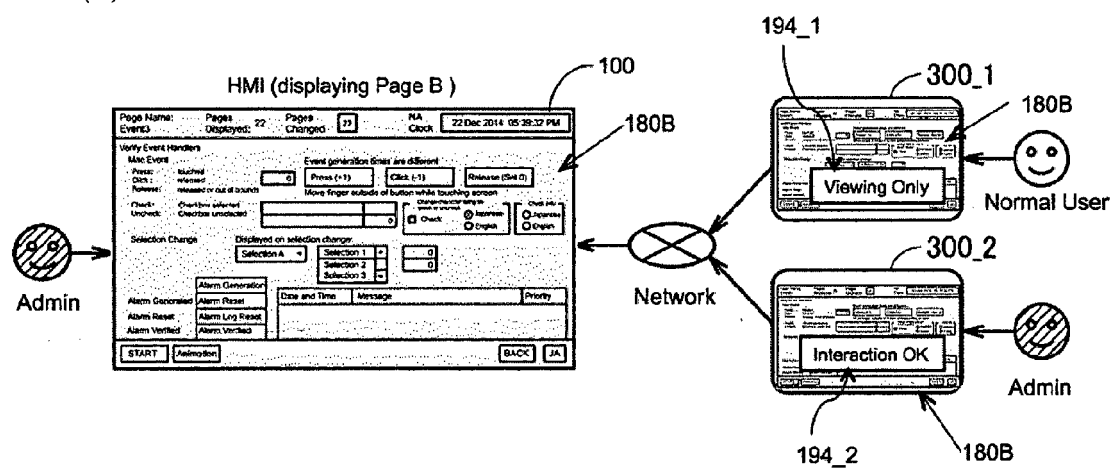


FIG. 16(B)

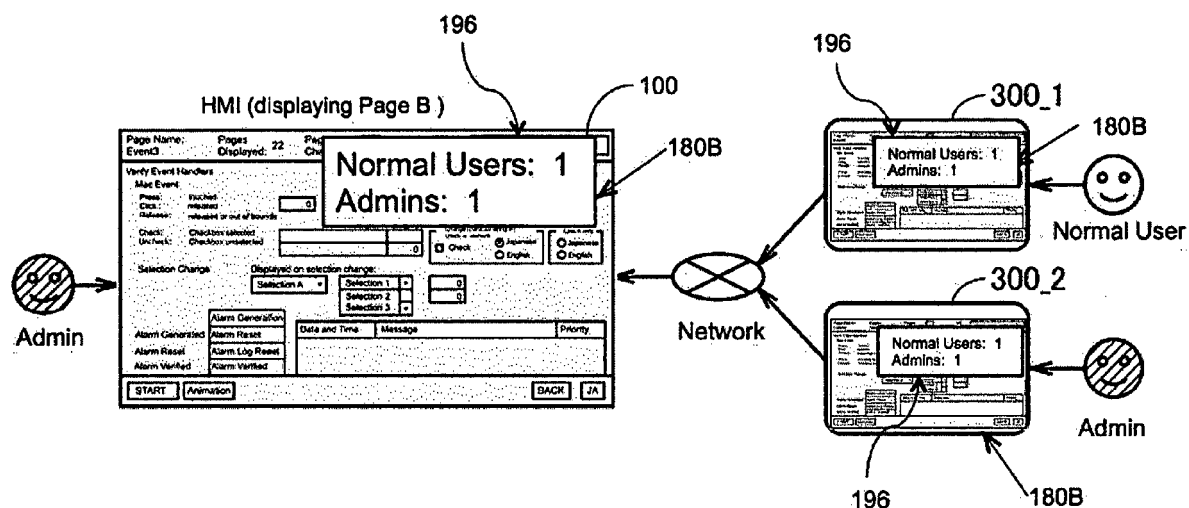


FIG. 17(A)

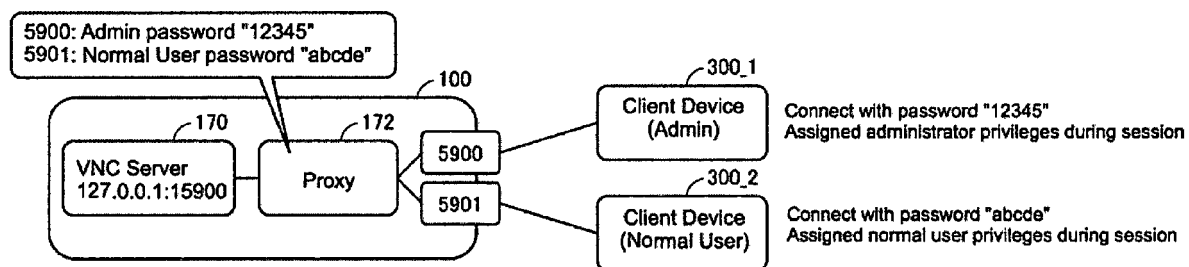
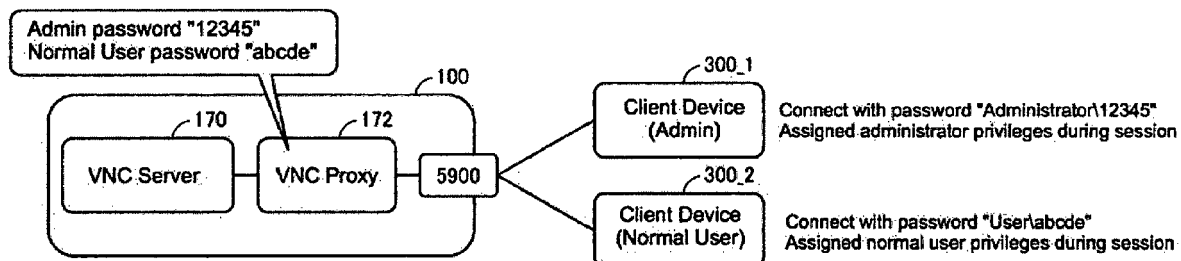


FIG. 17(B)



**REFERENCES CITED IN THE DESCRIPTION**

*This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.*

**Patent documents cited in the description**

- JP 2008033573 A [0003] [0008]
- US 2004260408 A1 [0004]
- US 2013066945 A1 [0005]
- US 8185550 B1 [0006]
- US 2014215356 A1 [0007]