(51) International Patent Classification:
G06F 21/53 (2013.01) G06B 19/418 (2006.01)

(21) International Application Number:
PCT/US2017/033034

(22) Filing Date:
17 May 2017 (17.05.2017)

(25) Filing Language:
English

(26) Publication Language:
English

(30) Priority Data:
62/345,661 03 June 2016 (03.06.2016) US
15/469,866 27 March 2017 (27.03.2017) US


(54) Title: SECURE APPROACH FOR PROVIDING COMBINDED ENVIRONMENT FOR OWNERS/OPERATORS AND MULTIPLE THIRD PARTIES TO COOPERATEVELY ENGINEER, OPERATE, AND MAINTAIN AN INDUSTRIAL PROCESS CONTROL AND AUTOMATION SYSTEM

(57) Abstract: A method includes creating (602), in a secure platform (204), multiple securely-partitioned system sandboxes (310a) under control of at least one user associated with an industrial process control and automation system (100). Different system sandboxes are associated with different third parties who are not owners or operators of the industrial process control and automation system. The method also includes receiving (612) content from the third parties in the system sandboxes. The method further includes receiving (614) from the at least one user a selective activation of at least some of the content in the system sandboxes in order to place the at least some of the content into use by the industrial process control and automation system. The content could include equipment configurations for equipment (102a - 140) associated with the industrial process control and automation system, and the equipment configurations could include control strategies and visualizations for the equipment.
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))
SECURE APPROACH FOR PROVIDING COMBINED ENVIRONMENT FOR OWNERS/OPERATORS AND MULTIPLE THIRD PARTIES TO COOPERATIVELY ENGINEER, OPERATE, AND MAINTAIN AN INDUSTRIAL PROCESS CONTROL AND AUTOMATION SYSTEM

CROSS-REFERENCE TO RELATED APPLICATION AND PRIORITY CLAIM


TECHNICAL FIELD

[0002] This disclosure relates generally to industrial process control and automation. More specifically, this disclosure relates to a secure approach for providing a combined environment for owners/operators and multiple third parties to cooperatively engineer, operate, and maintain an industrial process control and automation system.
BACKGROUND

[0003] Computer-based industrial process control and automation systems often incorporate a broad range of physical process equipment, which can often be packaged as modular "skids." This is true in systems such as Supervisory Control and Data Acquisition (SCADA) systems, Human Machine Interface (HMI) systems, and Distributed Control System (DCS) systems. An integrator or original equipment manufacturer (OEM) can construct a skid having key physical equipment, such as associated process controllers, instruments, and actuators.

[0004] In some cases, integrators and OEMs offer services beyond skid construction, such as process controller configuration. However, end users or owners of control and automation systems or their agents often need to map configurations of skids in terms of key variables to be monitored/controlled to named tags referenced in control and automation systems. Similarly, monitoring and control graphics of user interfaces for control and automation systems, along with other supervisory control functions (such as alarming, reporting, and historical data logging), often need to be built and mapped to these tags so that process operators can use these functions to effectively manage industrial processes.
SUMMARY

[0005] This disclosure provides a secure approach for providing a combined environment for owners/operators and multiple third parties to cooperatively engineer, operate, and maintain an industrial process control and automation system.

[0006] In a first embodiment, a method includes creating, in a secure platform, multiple securely-partitioned system sandboxes under control of at least one user associated with an industrial process control and automation system. Different system sandboxes are associated with different third parties who are not owners or operators of the industrial process control and automation system. The method also includes receiving content from the third parties in the system sandboxes. The method further includes receiving from the at least one user a selective activation of at least some of the content in the system sandboxes in order to place the at least some of the content into use by the industrial process control and automation system.

[0007] In a second embodiment, an apparatus includes at least one processing device configured to create, in a secure platform, multiple securely-partitioned system sandboxes under control of at least one user associated with an industrial process control and automation system. Different system sandboxes are associated with different third parties who are not owners or operators of the industrial process control and automation system. The at least one processing device is also configured to receive content from the third parties in the system sandboxes. The at least one processing device is further configured to receive from the at least one user a selective activation of at least some of the content in the system sandboxes in order to place the at least some of the content into use by the industrial process control and automation system.

[0008] In a third embodiment, a non-transitory computer readable medium contains computer readable program code that when executed causes at least one processing device to create, in a secure platform, multiple securely-partitioned system sandboxes under control of at least one user associated with an industrial process control and automation system. Different system sandboxes are associated with different third parties who are not owners or operators of the industrial process control and automation system. The medium also contains computer readable program code that when executed causes the at least one processing device to receive content from the third parties in the system sandboxes. The medium further contains computer readable program code that when executed causes the at least one processing device to receive from the at least one
user a selective activation of at least some of the content in the system sandboxes in order to place the at least some of the content into use by the industrial process control and automation system.

[0009] Other technical features may be readily apparent to one skilled in the art from the following figures, descriptions, and claims.
For a more complete understanding of this disclosure, reference is now made to the following description, taken in conjunction with the accompanying drawings, in which:

FIGURE 1 illustrates an example industrial process control and automation system according to this disclosure;

FIGURES 2 through 4 illustrate an example secure approach for providing a combined environment for owners/operators and multiple third parties to cooperatively engineer, operate, and maintain an industrial process control and automation system according to this disclosure;

FIGURE 5 illustrates an example device supporting a secure approach for providing a combined environment for owners/operators and multiple third parties to cooperatively engineer, operate, and maintain an industrial process control and automation system according to this disclosure; and

FIGURE 6 illustrates an example method for providing a combined environment for owners/operators and multiple third parties to cooperatively engineer, operate, and maintain an industrial process control and automation system using a secure approach according to this disclosure.
FIGURES 1 through 6, discussed below, and the various embodiments used to describe the principles of the present invention in this patent document are by way of illustration only and should not be construed in any way to limit the scope of the invention. Those skilled in the art will understand that the principles of the invention may be implemented in any type of suitably arranged device or system.

As described above, integrators and original equipment manufacturers (OEMs) can offer services related to equipment "skids," such as process controller configuration. However, this can require significant interactions between end users or owners of an industrial process control and automation system or their agents and the integrators and OEMs. While this could be achieved using sufficient manual interactions and sharing a range of documents, end users or owners seek the ability to streamline and support this interaction naturally, especially in the context of these systems being continually expanded. For instance, industrial processes can be expanded and changed to incorporate more equipment over time. As a result, the scenario of incorporating new physical equipment, programming control algorithms, and mapping this control to appropriate system graphics, reports, alarms, and history collections in order to achieve a desired overall function can continue indefinitely throughout the life of a control and automation system (possibly over multiple decades).

End users and owners with limited resources may also seek to extend the services that integrators and OEMs offer to the end users and owners as a standard capability. However, an end user or owner typically wants this to occur in a fashion that is both cyber-secure and under full control of the end user or owner with respect to allowed activities and access control for each user of a system.

An end user or owner may further require an integrator or OEM to be involved in checking out integration of new equipment with an overall system, performing simulated testing before equipment or skid shipment to a site, and supporting commissioning and troubleshooting on an ongoing basis using the unique expertise of that integrator or OEM. The lack of a standard mechanism for integrators and OEMs to provision these services makes them less economical or impractical in many cases due to complexity.

As end users and owners seek to reduce their costs, they may also look to standardize equipment and its configuration wherever possible. This can help to
normalize operation of the equipment and simplify service functions on that equipment, such as in environments with constrained resources and skills. A wide range of integrators and OEMs may be involved in supplying equipment, so standardization is a challenge for end users and owners with respect to control system integration.

[0020] In addition, physical distance between integrators or OEMs and end user or owner operation centers and other roles can be very significant, such as hundreds or thousands of kilometers. In these types of situations, some form of remote service provisioning may be required as a matter of practicality.

[0021] This disclosure provides a secure (and possibly cloud-based) environment for control system operations and provides standard secure mechanisms for OEMs, integrators, end users, owners, and others to connect, collaborate, and provide or receive services associated with industrial process control and automation systems. Moreover, these actions can occur under the control of the end users or owners.

[0022] FIGURE 1 illustrates an example industrial process control and automation system 100 according to this disclosure. As shown in FIGURE 1, the system 100 includes various components that facilitate production or processing of at least one product or other material. For instance, the system 100 is used here to facilitate control over components in one or multiple plants 101a-101n. Each plant 101a-101n represents one or more processing facilities (or one or more portions thereof), such as one or more manufacturing facilities for producing at least one product or other material. In general, each plant 101a-101n may implement one or more processes and can individually or collectively be referred to as a process system. A process system generally represents any system or portion thereof configured to process one or more products or other materials in some manner.

[0023] In FIGURE 1, the system 100 is implemented using the Purdue model of process control. In the Purdue model, "Level 0" may include one or more sensors 102a and one or more actuators 102b. The sensors 102a and actuators 102b represent components in a process system that may perform any of a wide variety of functions. For example, the sensors 102a could measure a wide variety of characteristics in the process system, such as temperature, pressure, or flow rate. Also, the actuators 102b could alter a wide variety of characteristics in the process system. The sensors 102a and actuators 102b could represent any other or additional components in any suitable process system. Each of the sensors 102a includes any suitable structure for measuring one or more
characteristics in a process system. Each of the actuators 102b includes any suitable structure for operating on or affecting one or more conditions in a process system.

[0024] One or more networks 104 are coupled to the sensors 102a and actuators 102b. The network 104 facilitates interaction with the sensors 102a and actuators 102b. For example, the network 104 could transport measurement data from the sensors 102a and provide control signals to the actuators 102b. The network 104 could represent any suitable network or combination of networks. As particular examples, the network 104 could represent an Ethernet network, an electrical signal network (such as a HART or FOUNDATION FIELDBUS network), a pneumatic control signal network, or any other or additional type(s) of network(s).

[0025] In the Purdue model, "Level 1" includes one or more controllers 106, which are coupled to the network 104. Among other things, each controller 106 may use the measurements from one or more sensors 102a to control the operation of one or more actuators 102b. Each controller 106 includes any suitable structure for controlling one or more aspects of a process system. As a particular example, each controller 106 could represent a computing device running a real-time operating system.

[0026] Redundant networks 108 are coupled to the controllers 106. The networks 108 facilitate interaction with the controllers 106, such as by transporting data to and from the controllers 106. The networks 108 could represent any suitable redundant networks. As particular examples, the networks 108 could represent a pair of Ethernet networks or a redundant pair of Ethernet networks, such as a FAULT TOLERANT ETHERNET (FTE) network from HONEYWELL INTERNATIONAL INC.

[0027] At least one switch/firewall 110 couples the networks 108 to two networks 112. The switch/firewall 110 may transport traffic from one network to another. The switch/firewall 110 may also block traffic on one network from reaching another network. The switch/firewall 110 includes any suitable structure for providing communication between networks, such as a HONEYWELL CONTROL FIREWALL (CF9) device. The networks 112 could represent any suitable networks, such as a pair of Ethernet networks or an FTE network.

[0028] In the Purdue model, "Level 2" may include one or more machine-level controllers 114 coupled to the networks 112. The machine-level controllers 114 perform various functions to support the operation and control of the controllers 106, sensors 102a, and actuators 102b, which could be associated with a particular piece of industrial
equipment (such as a boiler or other machine). For example, the machine-level controllers 114 could log information collected or generated by the controllers 106, such as measurement data from the sensors 102a or control signals for the actuators 102b. The machine-level controllers 114 could also execute applications that control the operation of the controllers 106, thereby controlling the operation of the actuators 102b. In addition, the machine-level controllers 114 could provide secure access to the controllers 106. Each of the machine-level controllers 114 includes any suitable structure for providing access to, control of, or operations related to a machine or other individual piece of equipment. Each of the machine-level controllers 114 could, for example, represent a server computing device running a MICROSOFT WINDOWS operating system. Although not shown, different machine-level controllers 114 could be used to control different pieces of equipment in a process system (where each piece of equipment is associated with one or more controllers 106, sensors 102a, and actuators 102b).

[0029] One or more operator stations 116 are coupled to the networks 112. The operator stations 116 represent computing or communication devices providing user access to the machine-level controllers 114, which could then provide user access to the controllers 106 (and possibly the sensors 102a and actuators 102b). As particular examples, the operator stations 116 could allow users to review the operational history of the sensors 102a and actuators 102b using information collected by the controllers 106 and/or the machine-level controllers 114. The operator stations 116 could also allow the users to adjust the operation of the sensors 102a, actuators 102b, controllers 106, or machine-level controllers 114. In addition, the operator stations 116 could receive and display warnings, alerts, or other messages or displays generated by the controllers 106 or the machine-level controllers 114. Each of the operator stations 116 includes any suitable structure for supporting user access and control of one or more components in the system 100. Each of the operator stations 116 could, for example, represent a computing device running a MICROSOFT WINDOWS operating system.

[0030] At least one router/firewall 118 couples the networks 112 to two networks 120. The router/firewall 118 includes any suitable structure for providing communication between networks, such as a secure router or combination router/firewall. The networks 120 could represent any suitable networks, such as a pair of Ethernet networks or an FTE network.

[0031] In the Purdue model, "Level 3" may include one or more unit-level
controllers 122 coupled to the networks 120. Each unit-level controller 122 is typically associated with a unit in a process system, which represents a collection of different machines operating together to implement at least part of a process. The unit-level controllers 122 perform various functions to support the operation and control of components in the lower levels. For example, the unit-level controllers 122 could log information collected or generated by the components in the lower levels, execute applications that control the components in the lower levels, and provide secure access to the components in the lower levels. Each of the unit-level controllers 122 includes any suitable structure for providing access to, control of, or operations related to one or more machines or other pieces of equipment in a process unit. Each of the unit-level controllers 122 could, for example, represent a server computing device running a MICROSOFT WINDOWS operating system. Although not shown, different unit-level controllers 122 could be used to control different units in a process system (where each unit is associated with one or more machine-level controllers 114, controllers 106, sensors 102a, and actuators 102b).

[0032] Access to the unit-level controllers 122 may be provided by one or more operator stations 124. Each of the operator stations 124 includes any suitable structure for supporting user access and control of one or more components in the system 100. Each of the operator stations 124 could, for example, represent a computing device running a MICROSOFT WINDOWS operating system. Other example types of operator stations 124 could include mobile devices, such as smartphones or tablet computers.

[0033] At least one router/firewall 126 couples the networks 120 to two networks 128. The router/firewall 126 includes any suitable structure for providing communication between networks, such as a secure router or combination router/firewall. The networks 128 could represent any suitable networks, such as a pair of Ethernet networks or an FTE network.

[0034] In the Purdue model, "Level 4" may include one or more plant-level controllers 130 coupled to the networks 128. Each plant-level controller 130 is typically associated with one of the plants I0La-I0Ln, which may include one or more process units that implement the same, similar, or different processes. The plant-level controllers 130 perform various functions to support the operation and control of components in the lower levels. As particular examples, the plant-level controller 130 could execute one or more manufacturing execution system (MES) applications, scheduling applications, or
other or additional plant or process control applications. Each of the plant-level
controllers 130 includes any suitable structure for providing access to, control of, or
operations related to one or more process units in a process plant. Each of the plant-level
controllers 130 could, for example, represent a server computing device running a
MICROSOFT WINDOWS operating system.

[0035] Access to the plant-level controllers 130 may be provided by one or more
operator stations 132. Each of the operator stations 132 includes any suitable structure for
supporting user access and control of one or more components in the system 100. Each of
the operator stations 132 could, for example, represent a computing device running a
MICROSOFT WINDOWS operating system.

[0036] At least one router/firewall 134 couples the networks 128 to one or more
networks 136. The router/firewall 134 includes any suitable structure for providing
communication between networks, such as a secure router or combination router/firewall.
The network 136 could represent any suitable network, such as an enterprise-wide
Ethernet or other network or all or a portion of a larger network (such as the Internet).

[0037] In the Purdue model, "Level 5" may include one or more enterprise-level
controllers 138 coupled to the network 136. Each enterprise-level controller 138 is
typically able to perform planning operations for multiple plants I0la-I0ln  and to
control various aspects of the plants I0la-I0ln. The enterprise-level controllers 138 can
also perform various functions to support the operation and control of components in the
plants I0la-I0ln. As particular examples, the enterprise-level controller 138 could
execute one or more order processing applications, enterprise resource planning (ERP)
applications, advanced planning and scheduling (APS) applications, or any other or
additional enterprise control applications. Each of the enterprise-level controllers 138
includes any suitable structure for providing access to, control of, or operations related to
the control of one or more plants. Each of the enterprise-level controllers 138 could, for
example, represent a server computing device running a MICROSOFT WINDOWS
operating system. In this document, the term "enterprise" refers to an organization having
one or more plants or other processing facilities to be managed. Note that if a single plant
101a is to be managed, the functionality of the enterprise-level controller 138 could be
incorporated into the plant-level controller 130.

[0038] Access to the enterprise-level controllers 138 may be provided by one or
more operator stations 140. Each of the operator stations 140 includes any suitable
structure for supporting user access and control of one or more components in the system 100. Each of the operator stations 140 could, for example, represent a computing device running a MICROSOFT WINDOWS operating system.

[0039] A historian 142 is also coupled to the network 136 in this example. The historian 142 could represent a component that stores various information about the system 100. The historian 142 could, for example, store information used during production scheduling and optimization. The historian 142 represents any suitable structure for storing and facilitating retrieval of information. Although shown as a single centralized component coupled to the network 136, the historian 142 could be located elsewhere in the system 100, or multiple historians could be distributed in different locations in the system 100.

[0040] Some of the operator stations described above may be situated remotely from other components of the control and automation system 100. For example, some of the operator stations could reside within an OEM or system integrator’s office. In those cases, network infrastructure (such as that of a telecom operator or other entity) can be used to couple the operator stations to the control and automation system 100.

[0041] Various portions of the industrial process control and automation system 100 could be obtained from integrators or OEMs as skids. Installation of the skids could be done by personnel of the control and automation system 100, by the integrators or OEMs, or by others. As described below, a secure collaboration platform can be used by personnel to facilitate installation, servicing, or other functions related to the industrial equipment.

[0042] Although FIGURE 1 illustrates one example of an industrial process control and automation system 100, various changes may be made to FIGURE 1. For example, industrial control and automation systems come in a wide variety of configurations, such as when redundant networks are not used at some or all levels or not all levels of the Purdue model are implemented in a system. The system 100 shown in FIGURE 1 is meant to illustrate one example operational environment in which secure collaboration between personnel may be used or supported. However, FIGURE 1 does not limit this disclosure to any particular configuration or operational environment.

[0043] FIGURES 2 through 4 illustrate an example secure approach for providing a combined environment for owners/operators and multiple third parties to cooperatively engineer, operate, and maintain an industrial process control and automation system.
according to this disclosure. For ease of explanation, the secure approach illustrated in FIGURES 2 through 4 may be described with respect to the industrial process control and automation system 100 of FIGURE 1. However, the secure approach illustrated in FIGURES 2 through 4 may be used with any other suitable industrial process control and automation system.

[0044] As shown in FIGURE 2, a system 200 supports secure collaboration between various personnel associated with industrial equipment used at one or more locations. In this example, the system 200 includes a number of computing nodes 202a-202n. The computing nodes 202a-202n denote any suitable computing or communication devices that can be used by personnel. The computing nodes 202a-202n could, for instance, denote desktop computers, laptop computers, tablet computers, or mobile smartphones. The computing nodes 202a-202n could be used by various personnel, such as different personnel working for an end user or owner of a control and automation system and different personnel working for an integrator or OEM. Some of the computing nodes 202a-202n could denote operator stations or other components in the system 100 of FIGURE 1.

[0045] The computing nodes 202a-202n are coupled directly or indirectly to a secure platform 204, which in this example is cloud-based and includes one or more servers or other computing devices 206 and one or more data storage devices 208. The computing device(s) 206 can execute applications or other logic that allows personnel using the computing nodes 202a-202n to collaborate and exchange information. The data storage device(s) 208 can store this information or other information related to one or more control and automation systems. In computing clouds, the specific device or devices executing logic and storing data can change over time, such as when different servers or other computing devices 206 are selected at different times for executing applications based on load balancing or other factors.

[0046] As described in more detail below, the computing devices 206 and the data storage devices 208 provide a secure environment for owners/operators and multiple third parties to cooperatively engineer, operate, and maintain an industrial process control and automation system, such as the system 100. The secure environment allows different types of users to access and share information related to an industrial process control and automation system. Among other tilings, the users are able to cooperatively design or engineer features of the industrial process control and automation system, operate
equipment of the industrial process control and automation system, and maintain
equipment of the industrial process control and automation system. Moreover, owners
and operators of the industrial process control and automation system have the ability to
control how other users (such as users associated with integrators and OEMs) can view or
modify data. This approach allows owners and operators of the industrial process control
and automation system to collaborate securely with other personnel to facilitate
installation, servicing, or other functions related to industrial equipment in the industrial
process control and automation system.

[0047] FIGURE 3 illustrates features of the secure platform 204 used to support
collaboration, and FIGURE 4 illustrates one example use of the secure platform 204. As
shown in FIGURE 3, the secure platform 204 is associated with various types of user
roles 302. Personnel having the various user roles 302 can use the computing nodes 202a-
202n to access the secure platform 204 in order to collaborate with one another and make
changes to an industrial process control and automation system. The different user roles
302 are associated with different types of personnel, so the different user roles 302 can be
associated with different actions or permissions in the secure platform 204.

[0048] In this example, the user roles 302 include field engineers, operations
personnel, and operations management personnel associated with an industrial process
control and automation system. Field engineers may denote personnel responsible for
configuring and maintaining field devices or other equipment in an industrial facility.
Operations personnel may denote personnel responsible for overseeing larger or more
complex areas of an industrial facility. Operations management personnel may denote
personnel responsible for controlling access to the secure platform 204. The user roles
302 also include system integrators associated with an integrator or OEM. System
integrators may denote personnel responsible for assisting in the installation or
configuration of equipment in an industrial facility. Of course, other or additional user
roles could also be supported by the secure platform 204.

[0049] The secure platform 204 supports the use of various views 304, which are
controlled using a view definition function 306. A view 304 defines the access level and
capabilities that a particular user role 302 has to assets in a control and automation
system. For example, a system integrator may have "commission and release"
capabilities to a specific asset in one location but no access to assets in other locations.
Different views 304 allow the secure platform 204 to control access by different user
roles 304 to a single model of a control or automation solution.

The view definition function 306 allows specified users to create, modify, or delete views 304. For instance, the view definition function 306 could support a graphical user interface that allows operations management personnel to create new views 304, review or modify existing views 304, and delete existing views 304. In some instances, the view definition function 306 could be accessible only to personnel associated with an industrial process control and automation system. This allows the owners or operators of an industrial process control and automation system to control which data associated with the control and automation system is made available to outside third parties and to control and modify that access over time.

At least one automation model 308 defines a set of equipment being monitored and controlled by users. An automation model 308 can include any suitable data related to a set of equipment, such as configuration and runtime properties, alarm and event definitions, and associated visualizations (like trend, schematic, and tabular diagrams). The automation model 308 can be generated in any suitable manner, such as with an automated tool that collects information from other components in a control and automation system and that generates the model 308 based on that information. The automation model 308 could also be generated or modified manually.

Equipment identified by an automation model 308 can be associated with a sandbox area 310a or with an online production area 310b. The sandbox area 310a generally denotes an area associated with equipment that is offline or not being used to actively control an industrial process. The online production area 310b denotes an area associated with equipment that is online and actually operating to actively control an industrial process. Equipment can be moved from the sandbox area 310a to the online production area 310b or vice versa, such as upon appropriate user approval. Also, multiple sandbox areas 310a and online production areas 310b could be associated with a single control and automation system. This may allow, for example, different third parties to access their own sandbox and production areas 310a-310b without having the ability to access other third parties' data areas.

Role capabilities can be different for the sandbox area 310a and the online production area 310b. For example, certain users may only be able to access information for equipment in the sandbox area 310a and not for equipment in the online production area 310b. This facilitates user workflows for building, commissioning, and operating at
an appropriately granular level of process equipment. Equipment and associated entities
can be easily moved from the sandbox area 310a to the online production area 310b and
removed from the online production area 310b.

[0054] Runtime values in an automation model 308 can read from or written to
process-connected controllers 312, such as by using or as part of a SCADA, HMI, or
DCS system. Runtime values can be defined and examined in the sandbox area 310a, and
runtime values can be read from or written to the controllers 312 using the online
production area 310b.

[0055] In addition, the secure platform 204 supports the use of various templates
314. Each template 314 defines one or more structures, one or more properties, one or
more relationships, one or more control strategies, and/or one or more visualizations
(referred to generally as configurations) to allow automation model elements (equipment)
to be easily configured. The templates 314 can be downloaded by various third parties
(such as system integrators) and used to perform various functions, such as defining
configuration and runtime properties for industrial equipment, defining alarm and event
conditions for the industrial equipment, and creating visualizations (like trend, schematic,
and tabular diagrams) for the industrial equipment. The templates 314 aid in the
standardization of visualizations and interactions across equipment built by different
system integrators.

[0056] Specific examples of the types of access and collaboration that could
occur between users are shown in FIGURE 4. As shown in FIGURE 4, personnel
associated with an industrial process control and automation system (such as field
engineers, operations personnel, and operations management personnel) can engage in
various activities via the secure platform 204. This includes commissioning new
equipment in the sandbox area 310a and monitoring operational equipment in the online
production area 310b. This also includes defining the views 304 and building the
templates 314. This further includes purchasing capacity in the secure platform 204.

[0057] System integrators or other third parties can also engage in various
activities via the secure platform 204. This includes downloading the templates 314 into
the third parties’ systems and using the templates 314 to help improve standardization of
visualizations and interactions across equipment in the control and automation system.
This also includes adding instances of new equipment in the sandbox area 310a, such as
for equipment that is being installed or replaced in a control and automation system. This
further includes the ability to commission equipment in the sandbox area 310a and to
transition that equipment into active equipment in the online production area 310b. In
addition, this includes the ability to monitor data and troubleshoot problems associated
with active equipment in the control and automation system

[0058] Note that all of the third-party functions are identified in FIGURE 4 as
being subject to access controls. As noted above, the owners or operators of an industrial
process control and automation system can have control over the information that is
accessible by third parties, such as via definitions of the views 304. Thus, third-party
system integrators or other third parties can obtain access to the information in the secure
platform 204 only as allowed by the owners or operators of an industrial process control
and automation system. Moreover, different third parties can have different access rights
to the information in the secure platform 204 as needed or desired, and the access rights
provided to a single third party could vary over time as needed or desired.

[0059] In one aspect of operation, personnel associated with integrators or OEMs
can download end user approved templates 314 to drive standardization of equipment
integration for a control and automation system. Flexible templating allows similar (but
not necessarily identical) equipment variations to map directly into a control and
automation system based on auto-generated displays and database mappings. Engineering
configurations can be created by end users, owners, integrators, or OEMs in a "safe area"
within the secure environment (the sandbox area 310a), and the environment facilitates
collaborative checkout of any defined configuration. Additionally, the end users or
owners have full control to approve and release new configurations into the online
production area 310b when appropriate.

[0060] This approach supports collaborative access by multiple third parties to
securely-partitioned system sandboxes (such as one or more per third party) under the
control of one or more end users (such as an owner or operator of the system 100). The
end user has an ability to jointly review information with the third party and to selectively
activate third party engineered content from one or more sandboxes to an operational
status without requiring file transfers or data re-entry. The end user also has an ability to
require that third parties implement configurations via nominated templates. Third party
access can be controlled in multiple dimensions, such as capabilities (like monitoring,
configuring, or commissioning), equipment groupings, and data classifications (like
process or maintenance). These and other features support collaboration that is
independent of personnel and physical automation equipment location and can include personnel in third party engineering offices, in end user offices, or in the field.

[0061] This environment provides the ability for end users and owners to allow secure access for integrators and OEMs to help commission, monitor, and troubleshoot equipment being supplied to the end users and owners as ongoing services. The overall system therefore acknowledges and supports the integrators and OEMs as third party providers within the system environment and provides built-in mechanisms to allow the appropriate interactions with user roles in a highly secure manner to protect system integrity at all times. It inherently provides for granular engineering, checkout, monitoring, and troubleshooting of equipment in a securely-managed and collaborative environment to greatly improve efficiency in the initial implementation and ongoing (potentially continuous) expansion and update of facilities.

[0062] Conventional approaches separate development systems of integrators and OEMs from deployed end user/owner systems. Engineering improvements involving an integrator or OEM assisting an end user or owner usually involve configuring one system, exporting and transmitting the configuration, and importing and checking out the configuration on the end user/owner system. Access to the end user/owner system would ordinarily have to be arranged as a custom communications arrangement for secure access through information technology (IT) infrastructures and networks. Additionally, any review and approval process would be managed as a manual workflow by the end user or owner without any obvious partitioning between parties. Similarly, any conventional monitoring services would have to be arranged in an ad hoc manner, and an end user or owner would normally have to manually configure any scope of access mapping for each integrator or OEM to equipment to be monitored or analyzed. Existing offerings do not provide end users or owners with the same level of access and configuration flexibility as the end users or owners have with on-premises systems. Rather, existing offerings usually have fixed configurations for all users, and configuration changes need to be requested from a hosted system provider. The approaches described in this disclosure help to reduce or avoid these problems. In some embodiments, the approaches described in this disclosure provide an ability to customize all key elements of an operational system (including graphics, reports, data points or tags, alarms, and history) in a manner similar to an on-premises experience.

[0063] Although FIGURES 2 through 4 illustrate one example of a secure
approach for providing a combined environment for owners/operators and multiple third parties to cooperatively engineer, operate, and maintain an industrial process control and automation system, various changes may be made to FIGURES 2 through 4. For example, while described here as being cloud-based, the secure platform could be implemented in other ways, such as when hosted by an end user/owner system or on a remote server system that is not cloud-based.

FIGURE 5 illustrates an example device 500 supporting a secure approach for providing a combined environment for owners/operators and multiple third parties to cooperatively engineer, operate, and maintain an industrial process control and automation system according to this disclosure. The device 500 could, for example, denote various computing devices in the system 100 of FIGURE 1 or in the system 200 of FIGURE 2.

As shown in FIGURE 5, the device 500 includes at least one processor 502, at least one storage device 504, at least one communications unit 506, and at least one input/output (I/O) unit 508. Each processor 502 can execute instructions, such as those that may be loaded into a memory 510. Each processor 502 denotes any suitable processing device, such as one or more microprocessors, microcontrollers, digital signal processors, application specific integrated circuits (ASICs), field programmable gate arrays (FPGAs), or discrete circuitry.

The memory 510 and a persistent storage 512 are examples of storage devices 504, which represent any structure(s) capable of storing and facilitating retrieval of information (such as data, program code, and/or other suitable information on a temporary or permanent basis). The memory 510 may represent a random access memory or any other suitable volatile or non-volatile storage device(s). The persistent storage 512 may contain one or more components or devices supporting longer-term storage of data, such as a read only memory, hard drive, Flash memory, or optical disc.

The communications unit 506 supports communications with other systems or devices. For example, the communications unit 506 could include a network interface card or a wireless transceiver facilitating communications over a wired or wireless network (such as the network 106b). The communications unit 506 may support communications through any suitable physical or wireless communication link(s).

The I/O unit 508 allows for input and output of data. For example, the I/O unit 508 may provide a connection for user input through a keyboard, mouse, keypad,
touchscreen, or other suitable input device. The I/O unit 508 may also send output to a
display, printer, or other suitable output device.

[0069] Although FIGURE 5 illustrates one example of a device 500 supporting a secure approach for providing a combined environment for owners/operators and multiple third parties to cooperatively engineer, operate, and maintain an industrial process control and automation system, various changes may be made to FIGURE 5. For example, various components in FIGURE 5 could be combined, further subdivided, or omitted and additional components could be added according to particular needs. Also, computing devices can come in a wide variety of configurations, and FIGURE 5 does not limit this disclosure to any particular configuration of computing device.

[0070] FIGURE 6 illustrates an example method 600 for providing a combined environment for owners/operators and multiple third parties to cooperatively engineer, operate, and maintain an industrial process control and automation system using a secure approach according to this disclosure. For ease of explanation, the method 600 is described as being performed using the system 200 of FIGURE 2 on behalf of owners/operators of the industrial process control and automation system 100 of FIGURE 1. However, the method 600 could be used in any other suitable system and for any other suitable industrial process control and automation system.

[0071] As shown in FIGURE 6, multiple sandboxes in a secure platform are created for multiple third parties associated with an industrial process control and automation system at step 602. This could include, for example, one or more users associated with the industrial process control and automation system 100 accessing the secure platform 204 and initiating creation of multiple sandbox areas 310a. Each sandbox area 310a could be associated with a different third party, such as a different integrators or OEMs. The industrial process control and automation system 100 could include equipment supplied, installed, or monitored by or otherwise associated with multiple (and possibly a large number) of integrators, OEMs, or other third parties. One, some, or all of these third parties could have their own sandbox areas 310a.

[0072] Views and templates are defined in the secure platform based on input from the owners/operators of the industrial process control and automation system at step 604. This could include, for example, the secure platform 204 receiving input defining multiple views 304 via the view definition function 306. Each view 304 can define (i) access rights that a user role 302 could have to data stored by the secure platform 204 and
(ii) functions that could be invoked by the user role 302 in the secure platform 204. This could also include the secure platform 204 receiving data defining multiple templates 314 associated with equipment in the industrial process control and automation system 100. The templates 314 can define the structures, properties, relationships, control strategies, or visualizations associated with the equipment. Depending on the owners/operators, one possible use of the templates 314 is to help define common configurations to be used by multiple third parties across various equipment in the control and automation system 100.

[0073] The third parties can access the secure platform, and the secure platform uses the defined views to control the access to the secure platform at step 606. This could include, for example, the secure platform 204 detecting access to a specific sandbox 310a of the secure platform 204 by a specified user. This could also include the secure platform 204 identifying the user role 302 associated with the user and identifying the view 304 associated with that user role 302. The identified view 304 can be used to control which data can be accessed by the user and which functions can be invoked by the user.

[0074] The secure platform can also allow the download of the defined templates to the third parties at step 608. This could include, for example, the secure platform 204 allowing an authorized user to download one or more templates 314 to a third party's computer system. Once downloaded, the third party can use the templates 314 in any suitable manner. For instance, the third party could generate configurations for equipment to be installed in the industrial process control and automation system 100 in line with the template 314 for that equipment. If the same template 314 is used by multiple third parties for the same type of equipment, this can help to standardize the configurations for that equipment across multiple integrators or OEMs.

[0075] The secure platform allows the various entities to exchange data and collaborate via the secure platform generally at step 610. This could include, for example, the secure platform 204 using the views 304 to ensure that third-party users are able to access only allowed data and invoke allowed functions of the secure platform 204. Data uploaded to the secure platform 204 by a third party can be placed into that third party's sandbox area 310a. The owners/operators of the industrial process control and automation system 100 can review the data, make or request changes, and perform other collaborative actions.

[0076] As part of this collaboration, the secure platform can receive content from
the third parties and store the content in the associated sandboxes 310a at step 612. Also, content in the sandboxes can be selectively activated for use in the industrial process control and automation system at step 614. This may include, for example, the secure platform 204 receiving equipment configurations from the third parties and storing the equipment configurations in the sandbox areas 310a. This may also include the owners/operators of the industrial process control and automation system 100 or their agents approving of the equipment configurations and moving the equipment configurations from the sandbox areas 310a to one or more online production areas 310b. The content received from the third parties could comply with the templates 314 previously provided to the third parties.

[0077] As another part of this collaboration, operational data associated with online equipment in the industrial process control and automation system can be provided to one or more of the third parties at step 616. This could include, for example, run-time data, historical data, or other data associated with equipment in the industrial process control and automation system 100 being provided to the third parties via one or more online production areas 310b. This data could be used by the third parties to provide remote monitoring, troubleshooting, or other services to the owners/operators of the industrial process control and automation system 100.

[0078] Note that this represents two examples of the types of collaborations that could occur between personnel associated with an industrial process control and automation system 100 and personnel associated with one or more third parties. Any other or additional collaborations could also occur involving these personnel.

[0079] In this way, third parties are able to engage with the owners/operators of the industrial process control and automation system 100 more effectively and efficiently. The services provided by integrators and OEMs can be expanded in a manner that is cyber-secure and under the full control of the owners/operators, and the owners/operators can standardize equipment and its configuration more easily. The integrators and OEMs can more easily check out the integration of new equipment with an overall system, perform simulated testing before equipment is shipped to a site, and support commissioning and troubleshooting on an ongoing basis. This can all occur regardless of the physical distance between the integrators or OEMs and a site. It can also occur over a prolonged period of time to support functions like incorporating new physical equipment, programming control algorithms, and mapping control to appropriate system graphics,
reports, alarms, and history collections (such as throughout the life of the control and automation system 100).

[0080] Although FIGURE 6 illustrates one example of a method 600 for providing a combined environment for owners/operators and multiple third parties to cooperatively engineer, operate, and maintain an industrial process control and automation system using a secure approach, various changes may be made to FIGURE 6. For example, while shown as a series of steps, various steps in FIGURE 6 could overlap, occur in parallel, occur in a different order, or occur any number of times.

[0081] In some embodiments, various functions described in this patent document are implemented or supported by a computer program that is formed from computer readable program code and that is embodied in a computer readable medium. The phrase "computer readable program code" includes any type of computer code, including source code, object code, and executable code. The phrase "computer readable medium" includes any type of medium capable of being accessed by a computer, such as read only memory (ROM), random access memory (RAM), a hard disk drive, a compact disc (CD), a digital video disc (DVD), or any other type of memory. A "non-transitory" computer readable medium excludes wired, wireless, optical, or other communication links that transport transitory electrical or other signals. A non-transitory computer readable medium includes media where data can be permanently stored and media where data can be stored and later overwritten, such as a rewritable optical disc or an erasable storage device.

[0082] It may be advantageous to set forth definitions of certain words and phrases used throughout this patent document. The terms "application" and "program" refer to one or more computer programs, software components, sets of instructions, procedures, functions, objects, classes, instances, related data, or a portion thereof adapted for implementation in a suitable computer code (including source code, object code, or executable code). The term "communicate," as well as derivatives thereof, encompasses both direct and indirect communication. The terms "include" and "comprise," as well as derivatives thereof, mean inclusion without limitation. The term "or" is inclusive, meaning and/or. The phrase "associated with," as well as derivatives thereof, may mean to include, be included within, interconnect with, contain, be contained within, connect to or with, couple to or with, be communicable with, cooperate with, interleave, juxtapose, be proximate to, be bound to or with, have, have a property
of, have a relationship to or with, or the like. The phrase "at least one of," when used with a list of items, means that different combinations of one or more of the listed items may be used, and only one item in the list may be needed. For example, "at least one of: A, B, and C" includes any of the following combinations: A, B, C, A and B, A and C, B and C, and A and B and C.

[0083] The description in the present application should not be read as implying that any particular element, step, or function is an essential or critical element that must be included in the claim scope. The scope of patented subject matter is defined only by the allowed claims. Moreover, none of the claims invokes 35 U.S.C. § 112(f) with respect to any of the appended claims or claim elements unless the exact words "means for" or "step for" are explicitly used in the particular claim, followed by a participle phrase identifying a function. Use of terms such as (but not limited to) "mechanism," "module," "device," "unit," "component," "element," "member," "apparatus," "machine," "system," "processor," or "controller" within a claim is understood and intended to refer to structures known to those skilled in the relevant art, as further modified or enhanced by the features of the claims themselves, and is not intended to invoke 35 U.S.C. § 112(f).

[0084] While this disclosure has described certain embodiments and generally associated methods, alterations and permutations of these embodiments and methods will be apparent to those skilled in the art. Accordingly, the above description of example embodiments does not define or constrain this disclosure. Other changes, substitutions, and alterations are also possible without departing from the spirit and scope of this disclosure, as defined by the following claims.
WHAT IS CLAIMED IS:

1. A method comprising:
   creating (602), in a secure platform (204), multiple securely-partitioned system sandboxes (310a) under control of at least one user associated with an industrial process control and automation system (100), different system sandboxes associated with different third parties who are not owners or operators of the industrial process control and automation system;
   receiving (612) content from the third parties in the system sandboxes; and
   receiving (614) from the at least one user a selective activation of at least some of the content in the system sandboxes in order to place the at least some of the content into use by the industrial process control and automation system

2. The method of Claim 1, wherein:
   the at least some of the content placed into use by the industrial process control and automation system comprises equipment configurations for equipment (102a-140) associated with the industrial process control and automation system; and
   the equipment configurations comprise control strategies and visualizations for the equipment.

3. The method of Claim 1, wherein the at least some of the content is placed into use by the industrial process control and automation system without requiring an additional file transfer involving the third parties and without requiring re-entry of the content.

4. The method of Claim 1, further comprising:
   receiving (604) templates from the at least one user, each template defining one or more equipment configurations associated with the industrial process control and automation system; and
   providing (608) one or more of the templates to each of the third parties, wherein the content received from each of the third parties is based on the one or more templates provided to that third party.

5. The method of Claim 1, wherein the secure platform supports
collaboration between the owners or operators of the industrial process control and automation system and the third parties independent of personnel and physical automation equipment location.

6. The method of Claim 1, wherein the secure platform allows the at least one user to control access by the third parties to the secure platform in multiple dimensions.

7. The method of Claim 1, further comprising:
   - receiving operational data based on operation of equipment (102a-140) associated with the industrial process control and automation system; and
   - providing (616) the operational data to at least one of the third parties engaging in remote monitoring or troubleshooting for the equipment.

8. An apparatus comprising:
   - at least one processing device (502) configured to:
     - create, in a secure platform (204), multiple securely-partitioned system sandboxes (310a) under control of at least one user associated with an industrial process control and automation system (100), different system sandboxes associated with different third parties who are not owners or operators of the industrial process control and automation system;
     - receive content from the third parties in the system sandboxes; and
     - receive from the at least one user a selective activation of at least some of the content in the system sandboxes in order to place the at least some of the content into use by the industrial process control and automation system

9. The apparatus of Claim 8, wherein:
   - the at least some of the content placed into use by the industrial process control and automation system comprises equipment configurations for equipment (102a-140) associated with the industrial process control and automation system; and
   - the equipment configurations comprise control strategies and visualizations for the equipment.
10. The apparatus of Claim 8, wherein the at least one processing device is configured to place the at least some of the content into use by the industrial process control and automation system without requiring an additional file transfer involving the third parties and without requiring re-entry of the content.

11. The apparatus of Claim 8, wherein the at least one processing device is further configured to:

- receive templates from the at least one user, each template defining one or more equipment configurations associated with the industrial process control and automation system; and
- provide one or more of the templates to each of the third parties, wherein the content received from each of the third parties is based on the one or more templates provided to that third party.

12. The apparatus of Claim 8, wherein the at least one processing device is further configured to support collaboration between the owners or operators of the industrial process control and automation system and the third parties independent of personnel and physical automation equipment location.

13. The apparatus of Claim 8, wherein the at least one processing device is further configured to allow the at least one user to control access by the third parties to the secure platform in multiple dimensions.

14. The apparatus of Claim 8, wherein the at least one processing device is further configured to:

- receive operational data based on operation of equipment (102a-140) associated with the industrial process control and automation system; and
- provide the operational data to at least one of the third parties engaging in remote monitoring or troubleshooting for the equipment.

15. A non-transitory computer readable medium containing computer readable program code that when executed causes at least one processing device (502) to perform the method of any of Claims 1-7.
FIG. 1
FIG. 5

600

START

602
CREATE SANDBOXES IN SECURE PLATFORM FOR THIRD PARTIES RELATED TO INDUSTRIAL CONTROL AND AUTOMATION SYSTEM

604
DEFINE VIEWS AND TEMPLATES BASED ON INPUT FROM SYSTEM OWNERS/OPERATORS

606
CONTROL ACCESS TO SECURE PLATFORM BASED ON VIEWS

608
PROVIDE TEMPLATES TO THIRD PARTIES

612
RECEIVE CONTENT FROM THIRD PARTIES AND STORE CONTENT IN ASSOCIATED SANDBOXES

614
ACTIVATE CONTENT FOR USE IN CONTROL AND AUTOMATION SYSTEM

616
PROVIDE OPERATIONAL DATA FOR EQUIPMENT TO THIRD PARTIES FOR MONITORING/TROUBLESHOOTING

END

FIG. 6
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

G06F 2/53(2013.01)i, G05B 19/418(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 21/53; G06F 11/263; G06F 11/34; G05B 9/02; G06F 21/60; G06Q 10/00; G06F 11/36; G05B 19/418

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: sandbox, control, automation, production, configuration, change, select, activate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>US 2016-0011952 AI (MICROSOFT CORPORATION) 14 January 2016 See paragraphs [0004], [0024]- [0027], [0029H0030] ; and figure 2.</td>
<td>1-15</td>
</tr>
<tr>
<td>Y</td>
<td>US 2012-0209411 AI (AKIRA OGISO et a1.) 16 August 2012 See paragraphs [0033], [0036], [0040], [0056] ; and figure 3.</td>
<td>1-15</td>
</tr>
<tr>
<td>A</td>
<td>US 2014-0007254 AI (DAVID BURK et a1.) 02 January 2014 See paragraphs [0016], [0039] ; and figure 2.</td>
<td>1-15</td>
</tr>
<tr>
<td>A</td>
<td>US 2014-00173355 AI (MICROSOFT CORPORATION) 19 June 2014 See paragraphs [0003], [0051] ; and figure 1.</td>
<td>1-15</td>
</tr>
<tr>
<td>A</td>
<td>EP 2172887 A2 (ROCKWELL AUTOMATION TECHNOLOGIES, INC.) 07 April 2010 See paragraphs [0088], [0233] ; and figure 2.</td>
<td>1-15</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C.

See patent family annex.

Date of the actual completion of the international search
22 August 2017 (22.08.2017)

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

Form PCT/ISA/210 (second sheet) (January 2015)
### INTERNATIONAL SEARCH REPORT

Information on patent family members

<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td>US 2016-0011952 Al</td>
<td>14/01/2016</td>
<td>US 2017-052863 Al</td>
<td>23/02/2017</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 9519557 B2</td>
<td>13/12/2016</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 5689333 B2</td>
<td>25/03/2015</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2013-0150985 Al</td>
<td>13/06/2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 9075410 B2</td>
<td>07/07/2015</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 9354625 B2</td>
<td>31/05/2016</td>
</tr>
<tr>
<td>US 2014-0007254 Al</td>
<td>02/01/2014</td>
<td>US 2014-007263 Al</td>
<td>02/01/2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 8904550 B2</td>
<td>02/12/2014</td>
</tr>
<tr>
<td>US 2014-0173355 Al</td>
<td>19/06/2014</td>
<td>AR 093988 Al</td>
<td>01/07/2015</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 201435364 A</td>
<td>16/09/2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 9588874 B2</td>
<td>07/03/2017</td>
</tr>
<tr>
<td></td>
<td></td>
<td>¥0 2014-093683 Al</td>
<td>19/06/2014</td>
</tr>
<tr>
<td>EP 2172887 A2</td>
<td>07/04/2010</td>
<td>CN 101807265 A</td>
<td>18/08/2010</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1286289 A2</td>
<td>26/02/2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1286289 A3</td>
<td>08/02/2006</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1521152 A2</td>
<td>06/04/2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1521152 A3</td>
<td>02/09/2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2003-0061004 Al</td>
<td>27/03/2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2004-0267395 Al</td>
<td>30/12/2004</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2009-0210081 Al</td>
<td>20/08/2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2010-0306001 Al</td>
<td>02/12/2010</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 6847854 B2</td>
<td>25/01/2005</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 7050873 Bl</td>
<td>23/05/2006</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 7797062 B2</td>
<td>14/09/2010</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 8126574 B2</td>
<td>28/02/2012</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 8417360 B2</td>
<td>09/04/2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 8914300 B2</td>
<td>16/12/2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 9729639 B2</td>
<td>08/08/2017</td>
</tr>
</tbody>
</table>

Form PCT/ISA/2 10 (patent family annex) (January 2015)