



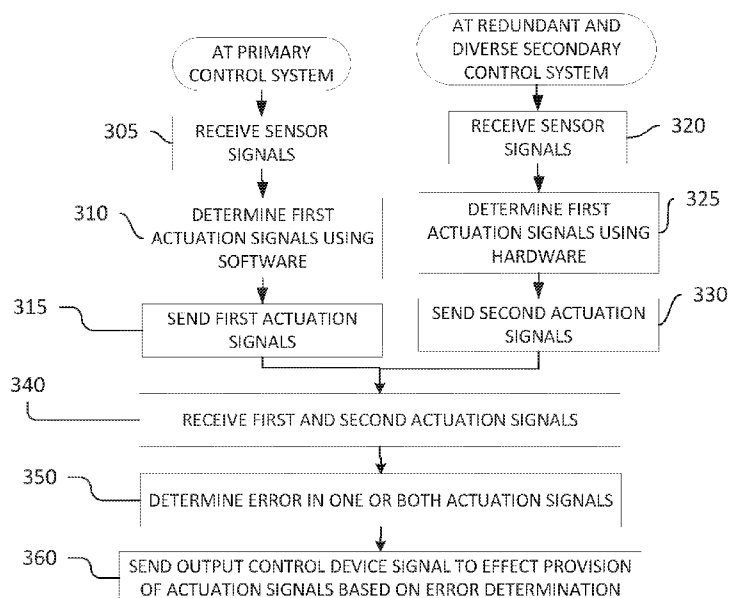
- (51) **International Patent Classification:**
G06F 21/50 (2013.01) *G06F 11/20* (2006.01)
- (21) **International Application Number:**
PCT/US2015/062159
- (22) **International Filing Date:**
23 November 2015 (23.11.2015)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
62/084,671 26 November 2014 (26.11.2014) US
- (71) **Applicant:** HOWARD UNIVERSITY [US/US]; 2400 Sixth Street, N.W., Suite 321, Washington, DC 20059 (US).
- (72) **Inventor:** KIM, Charles J.; 4021 Estabrook Drive, Annandale, Virginia 22003 (US).
- (74) **Agents:** KRATZ, Rudy et al.; Fitch, Even, Tabin & Flannery, LLP, 120 S. LaSalle Street, Suite 1600, Chicago, Illinois 60603 (US).

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

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

Published:

— with international search report (Art. 21(3))

(54) **Title:** COMPUTER CONTROL SYSTEM SECURITY**FIG. 3**

(57) **Abstract:** A redundant and diverse secondary control system mirrors a primary control system but has some fundamental structural difference as compared to the primary control system to prevent a spread of a security breach from the primary control system to the secondary control system. The secondary control system may operate on different hardware built on different software written with different programming language as compared to the primary control system while performing the same function as that of the primary system. By hardware coding the algorithm to produce actuation signals, software based viruses and worms cannot interfere with the secondary control system's operation. A monitor device receives actuation signals from both the primary and secondary controls signals to determine whether an error occurred and to provide correct actuation signals to the controlled system.

COMPUTER CONTROL SYSTEM SECURITY

TECHNICAL FIELD

[0001] This invention relates generally to computer security and more particularly to confirming the security and normal operation of a control system that is computer controlled.

BACKGROUND

[0002] A computer controller is a control system of hardware and software that produces desired output signals to actuators from input signals obtained through sensors. A simple example of the computer controller is a digital thermostat or temperature controller that reads the temperature of a space through temperature sensors and produces a turn-on or turn-off signal to air-conditioner units. More complex computer controllers are engine control systems in cars, programmable logic controllers in manufacturing lines and petrochemical processing plants, and digital relays in unmanned remote power substations.

[0003] Present computer controllers are equipped with high-end microprocessors and network capabilities along with sophisticated software, and thus they are now called intelligent electronic devices. These intelligent devices are getting connected to communication servers which in turn provide, via open networks or the Internet, plant operators, system designers and developers, corporate managers, and vendors with convenient access to them for update, maintenance, and modification of the hardware and software components.

[0004] FIG. 1 illustrates an example of such a prior art control system 100. A field/plant 105 constitutes the process or mechanism being controlled by the control system 100. The field/plant 105 can be any process or mechanism where a computer can automatically control operation of at least a portion of the process or mechanism such as in the non-limiting examples provided above. A computer controller 110 includes hardware 112 and software 114 aspects to perform its control function and may further include various ports to facilitate communication with other devices such as USB drives or other computing devices to allow updating, analysis, or maintenance of the system, which may be performed by outside vendors. The computer controller 110 receives signals from one or more sensors 120 from the field/plant 105 regarding the controlled process or mechanism. Based on those signals, the computer controller 110

automatically controls at least one actuator 130 to effect some change or control in the process or mechanism of the field/plant 105.

[0005] Optionally, the computer controller 110 can connect to a network 140, for example, directly or through a communication server 151. The network 140 can be any network such as a local private network or a public network such as the Internet. Through the network, the computer controller 110 may communicate with a management system 161 that is located, for example, at a corporate level network 170. The management system 161 can update or monitor the computer controller 110.

[0006] The convenience of access to the computer controllers, however, poses cyber vulnerability to the controllers of being maliciously or accidentally modified or operated illegitimately. A virus or worm may penetrate to the computer controllers via the infected computer of a vendor and may shut down the entire operation of the controller. An infected thumb drive (or USB memory stick) of a maintenance person who accesses the communication serve may inadvertently infect the computer controllers and thus cause a wrong operation immediately or latently. A malicious attack from a hacker who is knowledgeable of the hardware and software structure of a computer controller may be able to access through Internet and false authentication and modify the software code for ill-intended operation to cause havoc such as power outage, sewage spillage, nuclear plant shutdown, or contamination in water treatment.

[0007] The current focus on the cyber-security for computer control systems is centered on security measures that include development of security policies, development of access control lists and firewalls and proxy servers, development of event logs to detect malicious cyber activities, and development of updating, upgrading, and patching the software vulnerability. The fundamental problem of the current focus and practice of cyber-security for computer controllers is that it ignores the plain truth that it is impossible to predict cyber events throughout the computer controller's lifecycle, and that the detection and mitigation strategies may be good for old and known malwares and viruses only.

SUMMARY

[0008] Generally speaking, pursuant to these various embodiments, an apparatus and method for providing protection against software based security attacks includes a redundant and

diverse secondary control system that mirrors a primary control system. The secondary system, while keeping the same functional design or algorithm as the primary control system, has some fundamental structural difference as compared to the primary control system to prevent a spread of a security breach (such as a computer virus or worm, for example) from the primary control system to the secondary control system. For example, the secondary control system may operate on different hardware built on different software written with different programming language as compared to the primary control system while performing the same function as that of the primary system. For instance, the secondary control system may have a hardware based system incompatible with the primary control system and configured to run at least one hardware-coded algorithm. By hardware coding the algorithm to produce actuation signals, software based viruses and worms cannot interfere with the secondary control system's operation. The secondary control system receives signals from the same sensor that is used by the primary system, monitors an aspect of the controlled process as done by the primary system, and produces actuation signals that can be compared to actuation signals from the primary control system and/or to stored actuation signals to confirm the proper functioning of the primary control system.

[0009] So configured, computer controllers can be largely immune to and withstand cyber incidents that may originate from malicious cyber attackers, random or design hardware/software problems in the computer controllers, sabotage from a disgruntled employee, or inadvertent mistakes. These and other benefits may become clearer upon making a thorough review and study of the following detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The above needs are at least partially met through provision of the computer control system security approach described in the following detailed description, particularly when studied in conjunction with the drawings, wherein:

[0011] FIG. 1 comprises a block diagram of a prior art computer control system;

[0012] FIG. 2 comprises a block diagram of an example control system as configured in accordance with various embodiments of the invention;

[0013] FIG. 3 comprises a flow diagram of an example method of operation of an example control system as configured in accordance with various embodiments of the invention.

[0014] Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been drawn to scale. For example, the dimensions and/or relative positioning of some of the elements in the figures may be exaggerated relative to other elements to help to improve understanding of various embodiments of the present invention. Also, common but well-understood elements that are useful or necessary in a commercially feasible embodiment are often not depicted in order to facilitate a less obstructed view of these various embodiments. It will further be appreciated that certain actions and/or steps may be described or depicted in a particular order of occurrence while those skilled in the art will understand that such specificity with respect to sequence is not actually required. It will also be understood that the terms and expressions used herein have the ordinary technical meaning as is accorded to such terms and expressions by persons skilled in the technical field as set forth above except where different specific meanings have otherwise been set forth herein.

DETAILED DESCRIPTION

[0015] Referring now to the drawings, and in particular to FIG. 2, an illustrative apparatus providing protection against software based security attacks that is compatible with many of these teachings will now be presented. The apparatus includes a primary control system 202 including an input port 204 configured to receive sensor signals S_i from a sensor 220. Depending on the implementation, the sensor 220 provides a state or status from a controlled system 205 regarding the process or mechanism controlled by the control system. The primary control system 202 also includes an output port 208 configured to send first actuations signals O_i configured to control operation of at least a portion of the controlled system 205. A computer controller 210 includes a hardware component 212 running at least one software 214 based algorithm configured to output the first actuation signals based on the sensor signals. Optionally, the primary control system 202 further includes a communication port 238 configured to provide two-way communication with a communication server 251 or a wide area network 240. The computer controller 210 can connect to the network 240, for example, directly or through the communication server 251. The network 240 can be any network such as a local private network

or a public network such as the Internet. Through the network 240, the computer controller 210 may communicate with a management system 261 that is located, for example, at a corporate level network 270. The management system 261 can update or monitor the computer controller 210 through the network based communication path.

[0016] A redundant and diverse secondary control system 250 includes a second input port 254 configured to receive the sensor signals S_1 from the sensor 220 and a second output port 258 configured to send second actuations signals O_2 configured to control operation of the at least a portion of the controlled system 205. The secondary control system 250 further includes a hardware based system 260 incompatible with the primary control system 202 and configured to run at least one hardware-coded algorithm 262 and to output the second actuation signals O_2 based on the sensor signals S_1 . The second actuation signals O_2 are substantially identical to the first actuation signals O_1 when the primary 202 and secondary 250 control systems operate in an expected manner. In one example, the hardware based system 260 includes a field programmable gate array (FPGA) to implement the logic to create the secondary actuation signals O_2 in response to the sensor signals S_1 such that the system 260 does not include a software component configured to generate the secondary actuation signals O_2 . Such a fixed-purpose hard-wired platform, exemplified in the burned basic input/output system (BIOS) firmware read only memory (ROM) and in programmable/reconfigurable logic devices such as programmable logic array (PLA), programmable array logic (PAL), complex programmable logic device (CPLD), and FPGA, is well known and understood in the art and requires no further description here. Optionally, to further improve security, the secondary control system 250 can be configured to have no two-way communication path with another device.

[0017] The overall apparatus may further include an output control device 280 configured to receive the first actuation signals O_1 and the second actuation signals O_2 and to output either the first actuation signals O_1 or the second actuation signals O_2 to the controlled system 205 to control operation of the controlled system 205. For example, the output control device 280 can be a simple switch set to connect the actuator 230 to either a line carrying the first actuation signals O_1 or a second line carrying the second actuation signals O_2 . The output control device 280 is configured to be controlled by a monitor device 290.

[0018] The monitor device 290 is configured to receive and compare the first actuation signals O_1 and the second actuation signals O_2 , for example, by comparing the expectant actuation signal to one or both of the first actuation signals O_1 and the second actuation signals O_2 , and to determine whether error occurred with respect to one or both of the first and second actuation signals O_1 and O_2 . In one approach, the monitor device 290 accesses a memory 298 configured to store data regarding safe operational parameters including expectant actuation signals based on sensor signals for the controlled system 205 to make the error determination. The memory 298 can be a separate database, an integrated memory device, or other known data storage and access approach. The monitor device 290 sends an output control device signal to the output control device 280 to effect provision of either the first actuation signals O_1 or the second actuation signals O_2 by the output control device 280 based on whether an error occurred with respect to the first actuation signals O_1 . Optionally, the monitor device 290 can be configured to send such error occurrence information via a communication port 292, which may be configured to be a one-way only communication path such that error information can be passed to the management system 261 but incoming traffic, which may include malicious software or hacking attempts, is blocked or otherwise not allowed or possible. Such one-way communication ports are known in the art and need no further elaboration herein. In another approach, the monitor device 290 may instead send the error occurrence information by two way communication.

[0019] To provide additional security, the monitor device 290 can be implemented using a hardware based approach such that it does not include a software component in determining whether error occurred with respect to the first and second actuation signals O_1 and O_2 and generating the output control device signal. One such hardware based approach is implementation of a field programmable gate array embodying the logic used to determine error information and output the control device signal. In short, the monitor device 290 reads from the same sensor and monitors the outputs from the primary and secondary control systems and, based on the normal operational behavior stored in the memory, detects abnormal and different outputs for the same input from the two control systems.

[0020] Those skilled in the art will recognize and understand that such an apparatus may be comprised of a plurality of physically distinct elements as is suggested by the illustration shown in FIG. 2. It is also possible, however, to view this illustration as comprising a logical

view, in which case one or more of these elements can be enabled and realized via a shared platform.

[0021] So configured, any corruption of the primary control system's operation will be detected immediately and accurate output control signals will be provided to the controlled system in lieu of the erroneous controls. Because the secondary system is of a type different from the primary control system, the cause for corruption of the primary control system is unlikely to also corrupt the secondary system. For instance, through implementation of a hardware based processing approach in the secondary system's controller and, optionally, the monitor device, software based malicious attacks and vulnerabilities cannot directly corrupt the control signals provided by the redundant controller. Moreover, the error information can be provided immediately to the management system so that remedial action and repair of the primary control system 202 can be provided as soon as possible. Through this configuration of the diverse secondary control system and the monitor, an intended normal operation of the controller system can be maintained by the correct actuator output selection even when the primary controller is compromised by malicious attacks and other errors.

[0022] Referring to the FIG. 3, a method of controlling a process or system with protection against software based security attacks will be described. The method includes at a primary control system receiving 305 sensor signals from a sensor and determining 310 first actuation signals configured to control operation of at least a portion of a controlled system by using at least one software based algorithm which relies at least in part on the sensor signals. Then the primary control system sends 315 the first actuation signals. Optionally, the method may further include the primary control system conducting two-way communication with a communication server or a wide area network.

[0023] A redundant and diverse secondary control system also receives 320 the sensor signals from the sensor and independently from the primary control system determines 325 second actuation signals configured to control operation of the at least a portion of the controlled system. The secondary control system does so by using a hardware based system incompatible with the primary control system configured to run a hardware-coded control operation relying at least in part on the sensor signals. An example hardware-coded approach includes determining

the secondary actuation signals with a field programmable gate array and without use of a software component configured to generate the secondary actuation signals. When the primary and secondary control systems operate in an expected manner, the second actuation signals are substantially identical to the first actuation signals. The secondary control system sends 330 the secondary actuation signals. To maintain security, the method may include the secondary control system's communicating only in a one-way manner with any other device.

[0024] An output control device receives 340 the first actuation signals and second actuation signals. A monitor device receives and compares the first actuation signals and the second actuation signals. The monitor device determines 350 whether error occurred with respect to one or both of the first and second actuation signals. By one approach, the determination 350 is made using a field programmable gate array and without use of a software component to provide additional security in making the determination. In one aspect, the monitor device may access safe operational data stored in a memory to help with the determination. The safe operational data may include expected actuation signals under a condition or state determined by the received sensor signals that can be utilized to compare to one or both of the primary and secondary actuation signals to determine if there is a deviation from the expected actuation signals, thereby an error indication can be obtained. The method further includes sending 360 from the monitor device an output control device signal to the output control device to effect provision of either the first actuation signals or the second actuation signals by the output control device based on whether an error occurred with respect to the first actuation signals. Optionally, the method may further include sending error occurrence information via the two-way communication between the primary control system and with a communication server or a wide area network or via one-way communication between the monitor device and a communication server or wide area network.

[0025] The strength and resiliency of the described method of cyber security is explained under a typical scenario of attack or inadvertent error. Let us assume that a hacker, with presumed authenticity and login credentials of the communication server using a virtual private network (VPN) of a remote desktop connection across the Internet uploads a new and malicious code to the primary computer based controller. Then the primary controller would behave abnormally for a given input condition, while the duplicate secondary control system would

behave normally. These two different outputs would be detected by the monitor device and the duplicate controller's output would be selected based on the database of normal behavior to control the actuator under the given state or condition of the controlled system determined by the sensor signals.

[0026] Therefore, using the described cyber security method, the duplicate computer controller remains intact even under a cyber-attack resulting in a compromised situation in the existing primary computer controller; in which case the monitor device controls the entire system with normal and designed operation. The monitor device would alert the management system via the uni-directional communication path, and personnel would be dispatched to fix or replace the impacted computer controller and devise countermeasures. The described approaches would similarly be immune to a Stuxnet-like attack because any deliberate change and modification remains only on the existing computer controller; the FPGA based duplicate controller operates normally during and after the incident, and the actuator is correctly controlled by the intervention of the supervising monitor device.

[0027] So configured, strength and resiliency under a cyber-attack is achieved. Thus, even under cyber events of attack or inadvertent error, reliable and continued service of operation for production processes, assembly lines, water or sewage treatment, power and steam generation, electricity supply, or the like can be assured.

[0028] Those skilled in the art will recognize that a wide variety of modifications, alterations, and combinations can be made with respect to the above described embodiments without departing from the scope of the invention. For instance, although the monitor device and output control device are illustrated as separate elements, they could be combined into a single structure functioning as described. Such modifications, alterations, and combinations are to be viewed as being within the ambit of the inventive concept.

What is claimed is:

1. An apparatus providing protection against software based security attacks, the apparatus comprising:

a primary control system comprising:

- an input port configured to receive sensor signals from a sensor,
- an output port configured to send first actuation signals configured to control operation of at least a portion of a controlled system,
- a hardware component running at least one software based algorithm configured to output the first actuation signals based on the sensor signals;

a redundant and diverse secondary control system comprising:

- a second input port configured to receive the sensor signals from the sensor,
- a second output port configured to send second actuation signals configured to control operation of the at least a portion of the controlled system,
- a hardware based system incompatible with the primary control system and configured to run at least one hardware-coded algorithm and to output the second actuation signals based on the sensor signals, wherein the second actuation signals are substantially identical to the first actuation signals when the primary and secondary control systems operate in an expected manner;

an output control device configured to receive the first actuation signals and the second actuation signals and to output either the first actuation signals or the second actuation signals to the controlled system to control operation of the controlled system;

a memory configured to store data regarding safe operational parameters including expectant actuation signals based on sensor signals for the controlled system;

a monitor device configured to:

- receive the sensor signals,
- receive and compare the first actuation signals and the second actuation signals,
- determine whether error occurred with respect to one or both of the first and second actuation signals based on the sensor signals and the stored data for normal operation,

send an output control device signal to the output control device to effect provision of either the first actuation signals or the second actuation signals by the output control device based on whether an error occurred with respect to the first actuation signals.

2. The apparatus of claim 1 wherein the primary control system further comprises a communication port configured to provide two-way communication with a communication server or a wide area network.
3. The apparatus of claim 2 wherein the monitor device is configured to send error occurrence information via the communication port.
4. The apparatus of any of claims 1-3 wherein the secondary control system includes no two-way communication path with another device.
5. The apparatus of any of claims 1-4 wherein:
the secondary control system comprises a field programmable gate array, and
the secondary control system does not include a software component configured to generate the secondary actuation signals.
6. The apparatus of any of claims 1-5 wherein the monitor device further comprises a communication port configured to provide one-way outbound communication with a communication server or a wide area network.
7. The apparatus of any of claims 1-6 wherein:
the monitor device comprises a field programmable gate array, and
the monitor device does not include a software component configured to one or both of
determine whether error occurred with respect to the first and second actuation signals and
generate the output control device signal.
8. The apparatus of any of claims 1-7 wherein the monitor device is configured to determine whether error occurred with respect to one or both of the first actuation signals and the second actuation signals by comparing the expectant actuation signal to one or both of the first actuation signals and the second actuation signals.
9. A method of controlling a process or system with protection against software based security attacks, the method comprising:
at a primary control system:

- receiving sensor signals from a sensor,
 - determining first actuation signals configured to control operation of at least a portion of a controlled system by using at least one software based algorithm which relies at least in part on the sensor signals,
 - sending the first actuation signals;
- at a redundant and diverse secondary control system:
- receiving the sensor signals from the sensor,
 - determining second actuation signals configured to control operation of the at least a portion of the controlled system by using a hardware based system incompatible with the primary control system configured to run a hardware-coded control operation relying at least in part on the sensor signals, wherein the second actuation signals are substantially identical to the first actuation signals when the primary and secondary control systems operate in an expected manner,
 - sending the second actuation signals;
- receiving the first actuation signals and the second actuation signals at an output control device;
- at a monitor device:
- receiving the sensor signals,
 - receiving and comparing the first actuation signals and the second actuation signals,
 - determining whether error occurred with respect to one or both of the first and second actuation signals,
 - sending an output control device signal to the output control device to effect provision of either the first actuation signals or the second actuation signals by the output control device based on whether an error occurred with respect to the first actuation signals;
- outputting from the an output control device either the first actuation signals or the second actuation signals to the controlled system to control operation of the controlled system based on the output control device signal.
10. The method of claim 9 further comprising conducting two-way communication between the primary control system and with a communication server or a wide area network.

11. The method of claim 10 further comprising sending error occurrence information via the two-way communication between the primary control system and with a communication server or a wide area network.

12. The method of any of claims 9-11 further comprising communicating only in a one way manner between the secondary control system and another device.

13. The method of any of claims 9-12 wherein the determining the secondary actuation signals comprises determining the secondary actuation signals with a field programmable gate array and without use of a software component configured to generate the secondary actuation signals.

14. The method of any of claims 9-13 further comprising communicating only in a one way manner between the monitor device and with a communication server or a wide area network.

15. The method of any of claims 9-14 wherein the determining whether error occurred comprises determining whether error occurred using a field programmable gate array and without use of a software component.

16. The method of any of claims 9-15 wherein the determining whether error occurred comprises accessing safe operational data stored in a memory and by comparing expected actuation signals against one or both of the primary and secondary actuation signals.

17. An apparatus providing protection against software based security attacks, the apparatus to be used with a primary control system comprising an input port configured to receive sensor signals from a sensor, an output port configured to send first actuations signals configured to control operation of at least a portion of a controlled system, and a hardware component running at least one software based algorithm configured to output the first actuation signals based on the sensor signals, the apparatus comprising:

a redundant and diverse secondary control system comprising:

- a second input port configured to receive the sensor signals from the sensor,
- a second output port configured to send second actuations signals configured to control operation of the at least a portion of the controlled system,
- a hardware based system incompatible with the primary control system configured to run at least one hardware-coded algorithm and to output the second actuation signals based on

- the sensor signals, wherein the second actuation signals are substantially identical to the first actuation signals when the primary and secondary control systems operate in an expected manner;
- an output control device configured to receive the first actuation signals and the second actuation signals and to output either the first actuation signals or the second actuation signals to the controlled system to control operation of the controlled system;
- a memory configured to store data regarding safe operational parameters including expectant actuation signals based on sensor signals for the controlled system;
- a monitor device configured to:
- receive the sensor signals,
 - receive and compare the first actuation signals and the second actuation signals,
 - determine whether error occurred with respect to the first and second actuation signals by comparing the expectant actuation signal to one or both of the first actuation signals and the second actuation signals based on the sensor signals,
 - send an output control device signal to the output control device to effect provision of either the first actuation signals or the second actuation signals by the output control device based on whether an error occurred with respect to the first actuation signals.
18. The apparatus of claim 17 wherein the secondary control system includes no two-way communication path with another device.
19. The apparatus of any of claims 17-18 wherein:
- the secondary control system comprises a field programmable gate array, and
 - the secondary control system does not include a software component configured to generate the secondary actuation signals.
20. The apparatus of any of claims 17-19 wherein the monitor device further comprises a communication port configured to provide one-way outbound communication with a communication server or a wide area network.
21. The apparatus of any of claims 17-20 wherein:
- the monitor device comprises a field programmable gate array, and

the monitor device does not include a software component configured to one or both of determine whether error occurred with respect to the first actuation signals and generate the output control device signal.

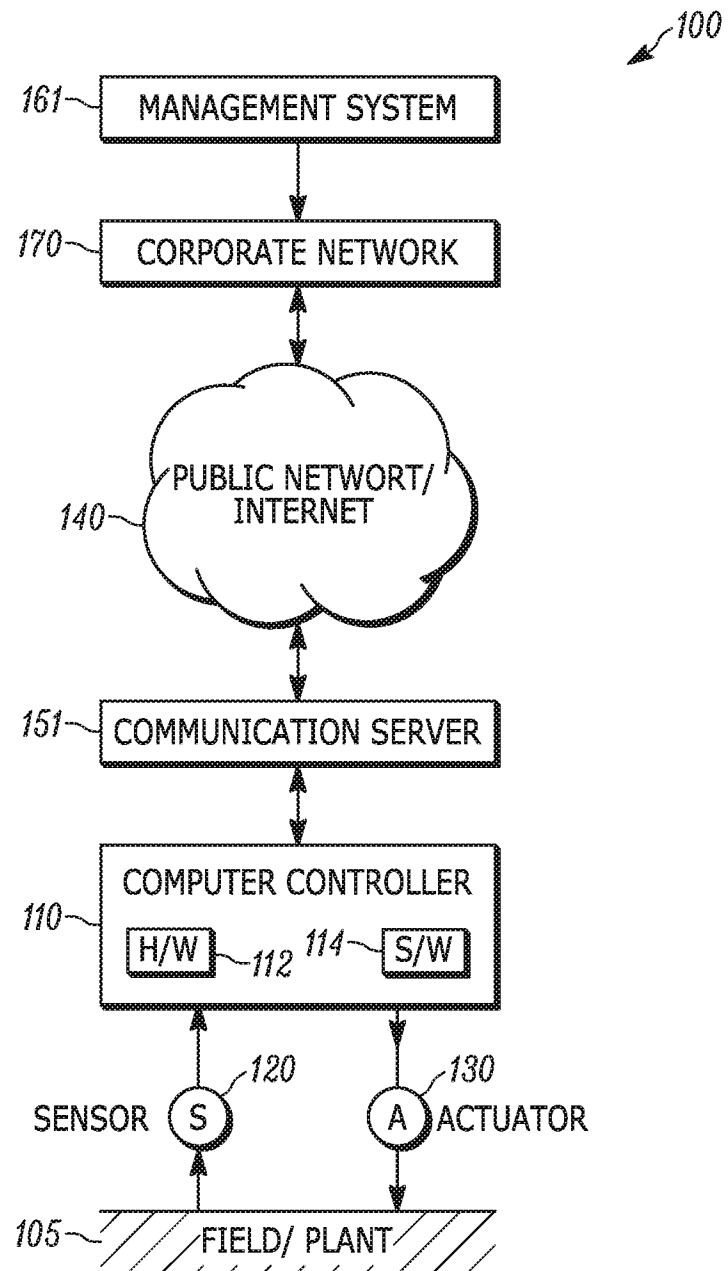


FIG. 1

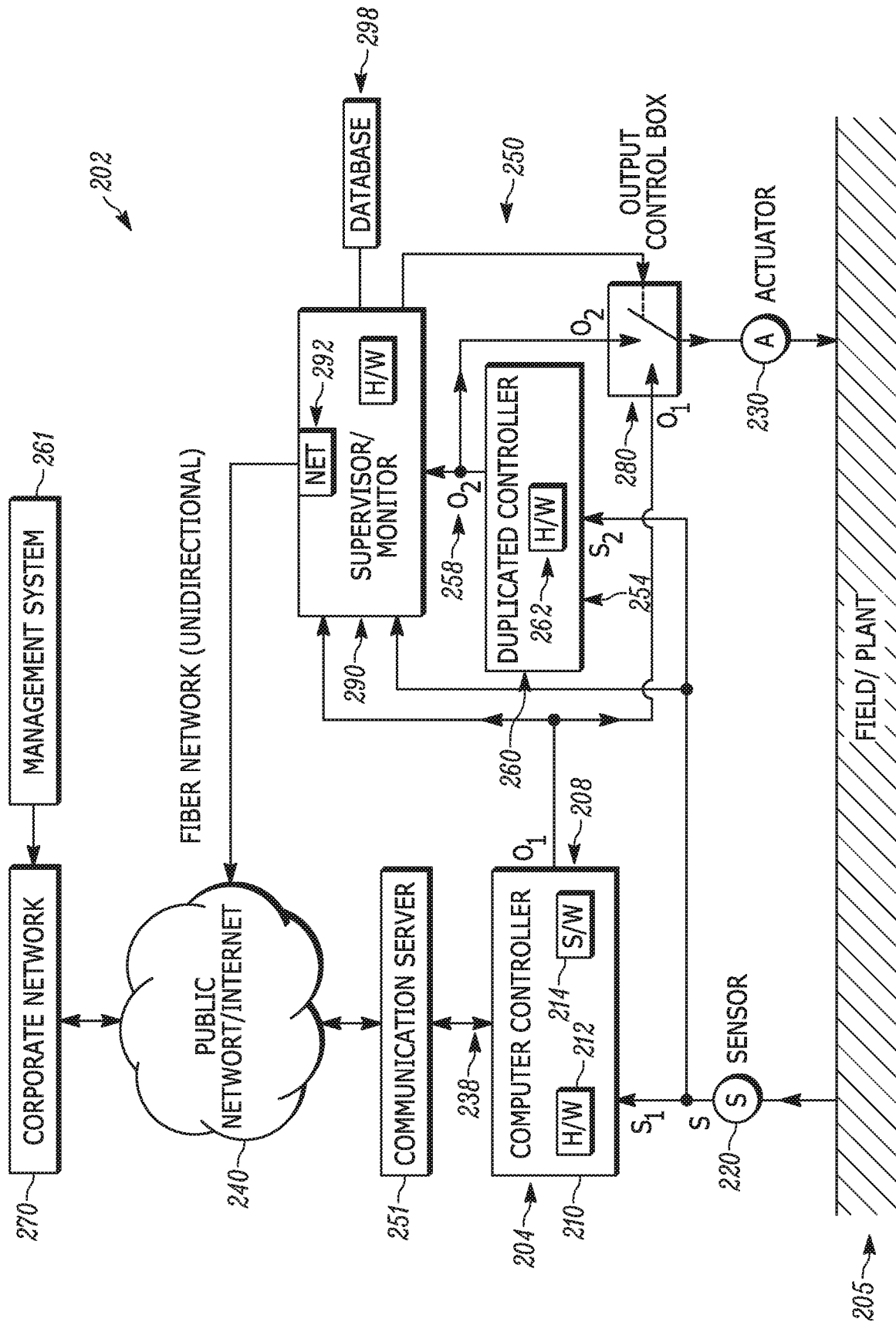
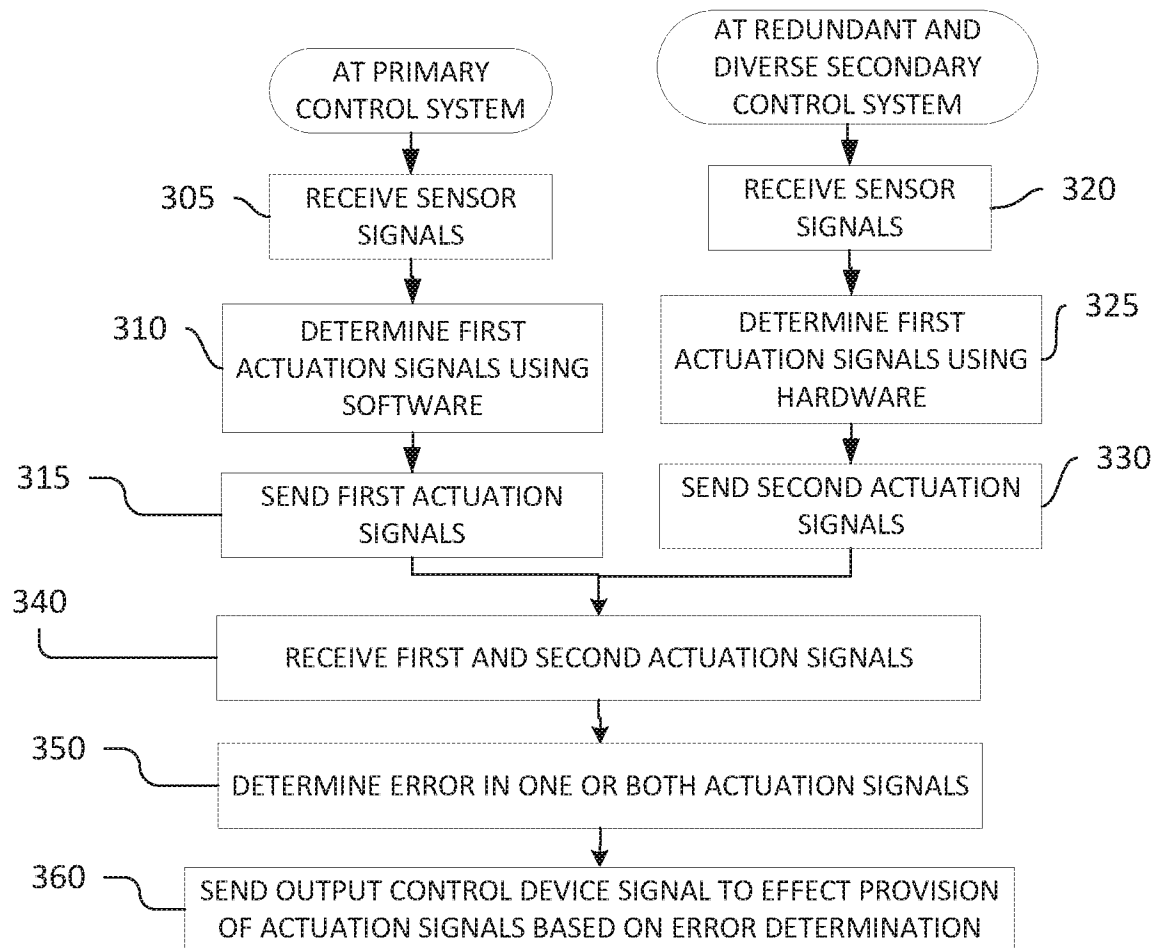


FIG. 2

FIG. 3



INTERNATIONAL SEARCH REPORT

International application No

PCT/US15/62159

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F21/50, G06F11/20 (2016.01)

CPC - G06F21/00, G05B23/0237

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC(8) - G06F21/50, G06F11/20, G05B9/02 (2016.01)

CPC - G06F21/00, G05B23/0237, G06F11/202, G05B9/03, G05B19/00

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

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

PatSeer (US, EP, WO, JP, DE, GB, CN, FR, KR, ES, AU, IN, CA, INPADOC Data); Google/Google Scholar, EBSCO Discovery Service, IEEE

Keywords: Control System, Hardware-coded, Secondary, Redundant, Diverse, Incompatible

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2011/313580 A1 (BAKHMACH, I.) 22 December 2011; abstract, paragraphs [0012], [0016], [0070], [0109]	1-4, 9-12 and 17-19
A	US 2012/0290153 A1 (OLSOE, J. et al.) 15 November 2012; figure 2, paragraphs [0005], [0006], [0020], [0119]	1-4, 9-12 and 17-19
A	US 2011/0264242 A1 (NAKAGAWA, S. et al.) 27 October 2011; paragraphs [0012], [0041], [0043], [0044]	1-4, 9-12 and 17-19

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

☐ See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

25 January 2016 (25.01.2016)

Date of mailing of the international search report

08 FEB 2016

Name and mailing address of the ISA/

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents

P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-8300

Authorized officer

Shane Thomas

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US15/62159

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☒ Claims Nos.: 5-8, 13-16, and 20-21
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

- Remark on Protest**
- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
 - ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
 - ☐ No protest accompanied the payment of additional search fees.