PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: JOSEPH J. HAWKINS
STOEL RIVES LLP
201 SO. MAIN STREET, SUITE 1100
SALT LAKE CITY, UT 84111

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	25 MAR 2020

Applicant's or agent's file reference	FOR FURTHER ACTION
68491-101	See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US 19/63366	26 November 2019 (26.11.2019)	29 November 2018 (29.11.2018)

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

IPC - G06F 21/00 (2020.01)

CPC - H04L 63/1433, H04L 63/14, Y04S 40/24

Applicant BATTELLE ENERGY ALLIANCE, LLC

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	03 March 2020 (03.03.2020)	Lee Young PCT Help Desk Telephone No. 571-272-4300

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 19/63366

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(b)).

3. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:

   a. ☐ forming part of the international application as filed:

      ☐ in the form of an Annex C/ST.25 text file.

      ☐ on paper or in the form of an image file.

   b. ☐ furnished together with the international application under PCT Rule 13*ter*.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.

   c. ☐ furnished subsequent to the international filing date for the purposes of international search only:

      ☐ in the form of an Annex C/ST.25 text file (Rule 13*ter*.1(a)).

      ☐ on paper or in the form of an image file (Rule 13*ter*.1(b) and Administrative Instructions, Section 713).

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 19/63366

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	None	YES
	Claims	1-35, 38-42	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-35, 38-42	NO
Industrial applicability (IA)	Claims	1-35, 38-42	YES
	Claims	None	NO

2. Citations and explanations:
Claims 1-35 and 38-42 lack novelty under PCT Article 33(2) as being anticipated by US 2018/0329593 A1 to Falkonry Inc. (hereinafter 'Falkonry').

As to claim 1, Falkonry teaches a method for securing a control system, comprising: generating a state key comprising cyber key data configured to characterize a cyber state of the control system and physical key data configured to characterize a physical state of the control system (para [0040]-[0049], [0059]-[0064], [0067]-[0073], [0136]-[0149] - "model manager 202 analyzes operating data that describes past operation of machines of a variety of types and, based at least in part on the operating data or other contextual information about the machines, generate and store machine operating models. "Models," in this context, may mean relations, equations, graphs, tables, state machines, or other data stored in computer storage and that describes past or expected future operational behavior of the machines corresponding to states of the machines"; "machine operating models may include patterns such as the snapshots or transitions between snapshots, and each pattern may be associated with a different set of operating states of machines. The patterns may be time series or time-based data, or characteristics thereof, that capture, represent, or are otherwise based on average or persistent measurement (observable) trends for one or more machine parameters over time, such as temperature, pressure, speed, vibration, current, sound, power or resource consumption, movement, torque, or power, resource (refined oil, water, etc.), or byproduct (pollution, carbon dioxide, etc.) output. Some parameters, such as temperature, may trail other parameters, such as engine speed. The operating states may include normal, abnormal, or even failing conditions of machines and/or their components"; "Using graphical representations that correspond to actual machines in the system, optionally shown in a diagram with representations of known physical connections or dependencies between the machines, may create a more readily understood representation of the changing physical state"; "the interface manager 200 and model manager 202 cooperate to provide an adaptive machine health management system that reacts to changing conditions in the system of machines and in the environment surrounding the system and characterizes those conditions"); communicating the state key through the control system, the communicating comprising acquiring validation data corresponding to the state key transmitted through one or more control paths of the control system (para [0026], [0067]-[0073], [0167] - "FIG. 2 illustrates an example computer system for labeling machine health information that is displayed in motion. In an embodiment, interface manager 200 uses stored models 208 and stored interface rules 210 to generate elements of a graphical user interface 214 on server-side computer system(s) 212, which are sent to client-side computer system(s) 216 for presentation to a user"; "the operator may be able to determine the state with little information other than changing value patterns in the most relevant parameters. The user may be assisted by flagging normal or abnormal data, or by marking or coloring data that has been indicated to be associated with a negative state or positive state"); generating a reconstruction of the state key by use of the acquired validation data (para [0040]-[0049], [0067]-[0073], [0125], [0136]-[0149] - "machine operating models, snapshots, or other sequences of values may be used by the interface manager to cause display of observed, average, or expected measurements or states of machines"; "a system monitor, such as one or more computing devices configured to collect data from a system and analyze the data, may detect a current state that is directly or indirectly connected to a fault or abnormal state downstream or upstream. As a result, the system monitor may work backwards or forwards along causally related snapshots of states to determine a source where the state might have started or a potential result of the state. These new possible connections or interactions may be determined based on likelihoods that they appear together, and users may confirm these new possible connections or interactions via the graphical user interface by labeling a display that shows both states as part of the same event, which may correspond to the same cluster"; "a machine health management system may detect deviation from expected behavior of a system, unit, component, sensor, or other machine element, and estimate future state of that element by attributing the deviation to degradation, misuse of the element, a trip of the element, or some other historical state that is known to have produced similar measurements in the past. The state of multiple elements may be estimated and learned from to identify dynamics of hidden degradations and/or faults and how these hidden degradations and/or faults affect different elements"); and determining a cyber-physical health of the control system based on a comparison between the state key and the reconstruction of the state key (para [0040]-[0049], [0067]-[0073], [0097]-[0104], [0108]-[0114] - "If different snapshots have been identified as different states of machines, the interface manager may cause display ofstate information, such as which states the machine is in, instead of or in addition to the observed, average, or expected measurements"; "By displaying values in motion, the interface manager 200 facilitates visualization of states and changes in states in a scalable manner that may utilize previously provided labels. For example, a low-level state such as a sensor-level state, a component-level state, or a unit-level state may be classified by past label input as a normal, abnormal, or failure state. The low-level state may later be labeled as the given state when playing a higher-level state such as a system-level, unit-level, or component-level state. In a particular example, normal states may be labeled as green, abnormal states as yellow, and failure states as red"; "FIG. 3, top pane 300 shows global metrics or parameters 301 and 304 of unit health, and these metrics may be specific to the unit domain or unit type. In this example, a value 305 labeled as thrust efficiency 306 is shown in green text, and a value 302 labeled as fan efficiency 303 is shown in green text, indicating nominal or positive behavior. These metrics or parameters may be selected as those most relevant to the health of the system, unit, component, or sensor of interest").
(See Continuation Box)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 19/63366

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

As drafted by applicant, claims 35-37 are indefinite. Claim 36 and claim 37 appear to have been separately numbered, but should properly be part of claim 35. Consequently, for the purpose of this international search, this authority has interpreted claims 35-37 as a single combined claim under the title of "Claim 35." Consequently, claim numbers 36 and 37 are skipped / not considered herein.

Claim 40, as drafted by applicant depends from claim 37, which for the reasons stated above, appears to be an error by applicant in numbering/drafting. Based on the language of claim 40, it appears this claim should properly depend upon claim 39 to avoid a lack of antecedent basis by otherwise depending from claim 35 (claims 35-37, as drafted by applicant). Consequently, for the purpose of this international search, this authority has interpreted claim 40 as depending from claim 39.

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 19/63366

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:
Box V.2. Citations and explanations:

As to claim 2, Falkonry further teaches further comprising communicating the state key through a control path comprising a physical component operatively coupled to a physical process controlled through the control path (para [0026], [0040]-[0049], [0059]-[0064], [0167], Fig. 2, Fig. 14).

As to claim 3, Falkonry further teaches wherein the control path comprises a cyber path configured to communicatively couple a controller to the physical component (para [0026], [0040]-[0049], [0059]-[0064], [0067]).

As to claim 4, Falkonry further teaches wherein communicating the state key through the control system comprises: splitting the state key into a plurality of fragments, each fragment comprising at least a portion of one or more of the cyber key data and the physical key data; transmitting the fragments of the state key through control paths of the control system; and acquiring validation data corresponding to each fragment (para [0026], [0040]-[0049], [0067]-[0073], [0125], [0136]-[0149]).

As to claim 5, Falkonry further teaches wherein transmitting a fragment of the state key through a control path comprises: communicating the fragment through a first cyber path of the control system; transmitting validation data corresponding to the fragment through a physical control section of the control path; and acquiring the validation data corresponding to the fragment through a second cyber path of the control system (para [0026], [0040]-[0049], [0067]-[0073], [0125], [0136]-[0149]).

As to claim 6, Falkonry further teaches wherein transmitting a fragment of the state key through a control path comprises: sending the fragment to a first physical component coupled to a physical process controlled through the control path; and transmitting validation data corresponding to the fragment to a second physical component through the physical process (para [0026], [0040]-[0049], [0070]-[0074], [0125], [0136]-[0149]).

As to claim 7, Falkonry further teaches wherein the first physical component comprises one or more of an actuator device and a controller (para [0066]-[0071]).

As to claim 8, Falkonry further teaches wherein the second physical component comprises one or more of a sensor device and a controller (para [0066]-[0071]).

As to claim 9, Falkonry further teaches wherein the cyber key data is configured to characterize a cyber state of a selected cyber-physical control element of the control system, the cyber-physical control element comprising a controller configured to implement a control function pertaining to a physical process variable by use of one or more physical devices (para [0066]-[0071]).

As to claim 10, Falkonry further teaches wherein the cyber key data is configured to characterize a cyber state of a cyber node communicatively coupled to one or more of the physical devices (para [0066]-[0071]).

As to claim 11, Falkonry further teaches wherein the cyber key data is configured to characterize a cyber state of a cyber path configured to communicatively couple the controller to one or more of the physical devices (para [0066]-[0071]).

As to claim 12, Falkonry further teaches wherein the physical key data is configured to characterize a physical state of one or more of the physical devices (para [0040]-[0049], [0064], [0066]-[0071]).

As to claim 13, Falkonry further teaches wherein the physical key data is configured to characterize a physical state of one or more of the controller and the physical process variable (para [0040]-[0049], [0064], [0066]-[0071]).

As to claim 14, Falkonry further teaches wherein communicating the state key through the control system comprises communicating the state key through a first group comprising a plurality of cyber-physical components of the control system, the method further comprising: calculating a first error metric quantifying differences between the state key and the reconstruction of the state key; and attributing at least a portion of the first error metric to one or more cyber-physical components of the first group (para [0026], [0040]-[0049], [0067]-[0073], [0125], [0136]-[0149]).

As to claim 15, Falkonry further teaches wherein attributing the error metric comprises: configuring a subsequent state key for communication through a second group of cyberphysical components of the control system that overlaps with the first group, the second group excluding one or more cyber-physical components of the first group; and attributing at least a portion of the first metric to the one or more cyber-physical components excluded from the second group (para [0026], [0040]-[0049], [0070]-[0074], [0097]-[0104], [0125], [0136]-[0149]).

As to claim 16, Falkonry further teaches where attributing the error metric further comprises: calculating a second error metric quantifying differences between the subsequent state key and a reconstruction of the subsequent state key; and attributing a difference between the first error metric and the second error metric to one or more of the cyber-physical components excluded from the second group (para [0040]-[0049], [0070]-[0074], [0097]-[0104], [0108]-[0114], [0125], [0136]-[0149]).

(See Next Continuation Box)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 19/63366

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:
Box V.2. Citations and explanations:

As to claim 17, Falkonry teaches an apparatus for securing a control system, comprising: a security agent comprising a processor (para [0156]-[0158]), comprising: a key module configured to generate keys, each key comprising cyber seed data configured to characterize a cyber state of the control system and physical seed data configured to characterize a physical state of the control system (para [0040]-[0049], [0059]-[0064], [0067]-[0073], [0136]-[0149]); a communication module configured to send keys through control paths of the control system (para [0026], [0067]-[0073], [0167]); a reconstruction module configured to determine key errors resulting from communication of the keys through the control paths (para [0040]-[0049], [0067]-[0073], [0125], [0136]-[0149]); and a security module configured to determine cyber health metrics indicating a cyber health of the control system and physical health metrics indicating a physical health of the control system based on the determined key errors (para [0040]-[0049], [0067]-[0073], [0097]-[0104], [0108]-[0114]).

As to claim 18, Falkonry further teaches wherein the communication module is configured to communicate a key through a selected region of the control system, the selected region comprising cyber-physical components configured to control a physical process variable of the control system (para [0026], [0040]-[0049], [0059]-[0064], [0167], Fig. 2, Fig. 14).

As to claim 19, Falkonry further teaches further comprising a parse module configured to split the key into a plurality of fragments, wherein the communication module is configured to send the fragments through respective control paths of the selected region of the control system (para [0026], [0040]-[0049], [0067]-[0073], [0125], [0136]-[0149]).

As to claim 20, Falkonry further teaches wherein the communication module is configured to send a first fragment of the key to an actuator device coupled to the physical process variable (para [0026], [0040]-[0049], [0061], [0066]-[0073], [0080]-[0082], [0125], [0136]-[0149]).

As to claim 21, Falkonry further teaches wherein the coverage module is configured to acquire validation data corresponding to the first fragment from a sensor device coupled to the physical process variable (para [0026], [0040]-[0049], [0061], [0067]-[0073], [0080]-[0082], [0125], [0136]-[0149]).

As to claim 22, Falkonry further teaches wherein the communication module is further configured to acquire validation data corresponding to communication of each fragment of the key, and wherein the reconstruction module is further configured to determine a reconstruction of the key by use of the acquired validation data (para [0040]-[0049], [0067]-[0073], [0125], [0136]-[0149]).

As to claim 23, Falkonry further teaches wherein the reconstruction module is further configured to determine a key error for the key based on a comparison between the key and the determined reconstruction of the key (para [0040]-[0049]).

As to claim 24, Falkonry further teaches wherein the key error is configured to quantify one or more of an error, a difference, and a distance between the key and the reconstruction of the key (para [0040]-[0049]).

As to claim 25, Falkonry further teaches wherein the key module is configured to generate keys adapted for communication through selected regions of the control system, wherein generating a key adapted for communication through a selected region of the control system comprises the key module: deriving cyber seed data of the key from cyber state metadata pertaining to the selected region of the control system; and deriving physical seed data of the key from physical state metadata pertaining to the selected region of the control system (para [0040]-[0049], [0059]-[0064]).

As to claim 26, Falkonry further teaches wherein the cyber state metadata is configured to characterize one or more of: a state of cyber communication at one or more cyber components, a state of cyber communication at one or more cyber nodes, and state of cyber communication within a control system network (para [0040]-[0049], [0059]-[0064], [0130]-[0133]).

As to claim 27, Falkonry further teaches wherein the physical state metadata is configured to characterize a state of one or more: sensor devices, actuator devices, computational components, and physical process variables (para [0066]-[0071]).

As to claim 28, Falkonry further teaches wherein the communication module is configured to send a first key through first cyber-physical control paths, wherein the first cyber-physical control paths comprising a first group of cyber-physical components of the control system, the reconstruction module is configured to determine a first key error resulting from communication of the first key through the first cyber-physical control paths, and wherein the security module is further configured to attribute at least a portion of the first key error to one or more cyber-physical components of the first group (para [0026], [0040]-[0049], [0067]-[0073], [0125], [0136]-[0149]).

As to claim 29, Falkonry further teaches wherein the security module is further configured to: cause the key module to generate a subsequent key adapted for communication through second cyber-physical control paths, the second cyber-physical control paths comprising a second group of cyber-physical components of the control system, the second group configured to overlap with the first group; determine a difference between the first key error and a second key error resulting from communication of the second key through the second cyber-physical control paths; and assign at least a portion of a difference between the first key error and the second key error to a cyber-physical component included in the first group and excluded from the second group (para [0026], [0040]-[0049], [0070]-[0074], [0097]-[0104], [0125], [0136]-[0149]).

(See Next Continuation Box)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 19/63366

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:
Box V.2. Citations and explanations:

As to claim 30, Falkonry further teaches wherein the communication module is configured to send fragments of a key through respective cyber-physical control paths, each cyber-physical control path involving a respective group of cyber-physical components of the control system, wherein the reconstruction module is configured to determine fragment errors resulting from communication of the fragments of the key through the respective cyberphysical control paths, and wherein the security module is configured to determine differences between the fragment errors and associate the determined differences to one or more cyber-physical components of the control system based on differences between the respective groups of cyber-physical components involved in communication of the fragments through the respective cyber-physical control paths (para [0026], [0040]-[0049], [0070]-[0074], [0097]-[0104], [0125], [0136]-[0149]).

As to claim 31, Falkonry teaches a non-transitory storage medium comprising instructions configured for execution by a computing device, the instructions configured to cause the computing device to implement operations for monitoring a cyber-physical health of a control system, the operations comprising: generating state keys comprising cyber key data corresponding to an acquired cyber state of the control system and physical key data corresponding to an acquired physical state of the control system (para [0040]-[0049], [0059]-[0064], [0067]-[0073], [0136]-[0149]); communicating the state keys through cyber-physical control paths of the control system, the communicating comprising acquiring validation data corresponding to respective state keys in response to sending the respective state keys through the cyberphysical control paths of the control system (para [0026], [0067]-[0073], [0167]); determining error metrics for the state keys, the error metrics quantifying error between the state keys and reconstructions of the state keys, the reconstructions generated from the acquired validation data corresponding to the respective state keys (para [0040]-[0049], [0067]-[0073], [0125], [0136]-[0149]); and determining the cyber-physical health of the control system based on the determined error metrics (para [0040]-[0049], [0067]-[0073], [0097]-[0104], [0108] -[0114]).

As to claim 32, Falkonry further teaches wherein communicating a state key through cyber-physical control paths of the control system comprises: sending the state key to one or more actuator devices; and acquiring validation data corresponding to the state key from one or more sensor devices (para [0026], [0040]-[0049], [0061], [0066]-[0073], [0080]-[0082], [0125], [0136]-[0149]).

As to claim 33, Falkonry further teaches wherein communicating a state key comprises: parsing the state key into a plurality of fragments; and communicating the fragments of the state key through cyber-physical control paths of the control system, each cyber-physical control path comprising a physical control coupling, wherein communicating a fragment comprises: sending the fragment to a correlator of a physical control coupling, and acquiring validation data corresponding to the state key from a receiver of the physical control coupling (para [0026], [0040]-[0049], [0067]-[0073], [0125], [0136]-[0149]).

As to claim 34, Falkonry further teaches wherein the correlator comprises an actuator device operatively coupled to a physical process variable of the physical control coupling, and wherein the receiver comprises a sensor device operatively coupled to the physical process variable (para [0026], [0040]-[0049], [0061], [0066]-[0073], [0080]-[0082], [0125], [0136]-[0149]).

As to claim 35, Falkonry further teaches wherein communicating the fragment through the physical control coupling further comprises: configuring the actuator device to communicate validation data corresponding to the fragment through a medium of the physical control coupling; and configuring the sensor device to acquire the validation data communicated through the medium (para [0026], [0040]-[0049], [0061], [0066]-[0073], [0080]-[0082], [0125], [0136]-[0149]).

As to claim 38, Falkonry further teaches wherein communicating the fragment further comprises: sending the fragment to the correlator through a first cyber path; and receiving the validation data corresponding to the fragment from the receiver though a second cyber path (para [0026], [0040]-[0049], [0067]-[0073], [0125], [0136]-[0149]).

As to claim 39, Falkonry further teaches wherein determining the error metrics for the state key comprises determining a plurality of fragment errors, each fragment error quantifying error introduced during communication of a respective fragment of the state key through a respective cyber-physical control path of the control system (para [0026], [0040]-[0049], [0067]-[0073], [0125], [0136]-[0149]).

As to claim 40, Falkonry further teaches wherein communication of the respective fragments through the respective cyber-physical control paths comprises communicating the respective fragments through respective groups of cyber-physical components of the control system, the operations further comprising: determining differences between the fragment errors; and attributing the determined differences to cyber -physical components of the control system based on differences between the respective groups of cyber-physical components (para [0040]-[0049], [0070]-[0074], [0097]-[0104], [0108]-[0114], [0125], [0136]-[0149]).

As to claim 41, Falkonry further teaches the operations further comprising: determining first error metrics for a first state key, the first error metrics quantifying error introduced during communication of the first state key through a first region of the control system; determining second error metrics for a second state key, the second error metrics quantifying error introduced during communication of the second state key through a second region of the control system, the second region including first cyber-physical components included in the first region and second cyber-physical components not included in the first region; and assigning differences between the second error metrics and the first error metrics to one or more of the first cyber-physical components and the second cyber-physical components (para [0040]-[0049], [0070]-[0074], [0097]-[0104], [0108]-[0114], [0125], [0136]-[0149]).

(See Next Continuation Box)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US 19/63366

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**
Continuation of:
Box V.2. Citations and explanations:

As to claim 42, Falkonry further teaches the operations further comprising: configuring the second state key to overlap with the first state key in response to determining that the first error metrics exceed one or more error thresholds, wherein the assigning comprises one or more of: assigning an increase in the first error metrics relative to the second error metrics to one or more of the first cyber-physical components; and assigning a decrease in the second error metrics relative to the first error metrics to one or more of the second cyber-physical components (para [0026], [0040]-[0049], [0063]-[0064], [0070]-[0074], [0097]-[0104], [0125]-[0126], [0136]-[0149]).

Claims 1-35 and 38-42 have industrial applicability as defined by PCT Article 33(4) because the subject matter can be made or used in industry.