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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 October 2015 (08.10.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/152944 A1

(51) International Patent Classification:
G01F 15/00 (2006.01)

(21) International Application Number:
PCT/US2014/033027

(22) International Filing Date:
4 April 2014 (04.04.2014)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **SICPA SECURITY INKS & SYSTEMS USA, INC.** [US/US]; 8000 Research Way, Springfield, Virginia 22153 (US).

(72) Inventors: **FINKEL, Charles**; 19E 79th Street, Apt. 3, New York, New York 10075 (US). **CAMPBELL, Mark**; Rue de la Tour 21, CH-1004 Lausanne (CH). **VAN NGOC TY, Christophe**; Rue de l'Avenir 16, 1207 Genève (CH). **CASET, Giorgio**; Chemin de l'Esplanade 30, CH-1052 Le Mont-sur-Lausanne (CH).

(74) Agents: **TURK, Arnold** et al.; Greenblum & Bernstein, P.L.C., 1950 Roland Clarke Place, Reston, Virginia 20191 (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, LT, 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, 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,

[Continued on next page]

(54) Title: INTERFACE TO GENERATE DATA COMPATIBLE WITH AN EXTERNAL SYSTEM IN AN OIL AND GAS ASSET SUPPLY CHAIN

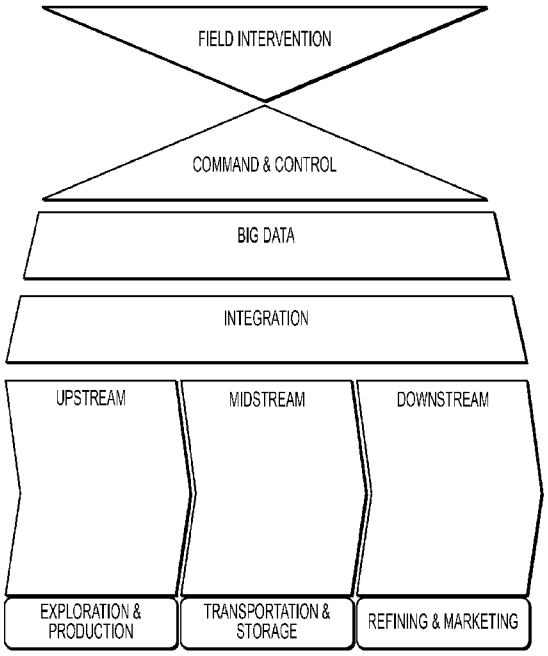


FIG. 4

(57) Abstract: The present disclosure generally relates to an interface system and method of interfacing to generate data compatible with an external system in an oil and gas asset supply chain, and in particular to an interface and interface method for generating secure and verifiable data to prevent tampering, injection of unwanted data resulting from an unauthorized access along a supply chain. An interface generates and transforms data in an oil and gas supply chain for compatibility with external systems. Collected data is captured by an industrial control system sensor or data collector, which is transferred in a secure intermediary hardware platform to interface with a software component. The collected data is then modified using a business rules engine to create enhanced data and events created from the enhanced data.

WO 2015/152944 A1

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))*

INTERFACE TO GENERATE DATA COMPATIBLE WITH AN EXTERNAL SYSTEM IN AN OIL AND GAS ASSET SUPPLY CHAIN

BACKGROUND

1. Field of the Disclosure

[0001] The present disclosure generally relates to a system and method for generating data compatible with an external system in an oil and gas asset supply chain, and in particular to an interface and interface method for generating secure and verifiable data to prevent tampering, or injection of unwanted data resulting from an unauthorized access along a supply chain.

2. Background Information

[0002] The oil and gas industry is typically divided into three sectors: upstream, midstream and downstream, as illustrated in Figure 1. The upstream sector is known as the exploration and production sector. The upstream sector includes the searching and exploration for potential underground or underwater crude oil and natural gas fields (e.g. identification of potential hydrocarbon reserves), drilling of exploratory wells, and subsequently drilling and completion of the wells that recover and bring (produce) the crude oil and/or raw natural gas to the surface. The midstream sector involves the transportation (by pipeline, rail, truck, etc.), storage, and wholesale marketing of crude or refined petroleum products. Pipelines and other numerous transport systems can be used to move crude oil from production sites to refineries and deliver the various refined products to downstream distributors. The downstream sector refers to the refining of petroleum crude oil and the processing and purifying of raw natural gas, as well as the marketing and distribution of products derived from crude oil and natural gas. The downstream sector provides consumers with products such as gasoline or petrol, kerosene, jet fuel, diesel oil, heating, oil, lubricants, waxes, asphalt, natural gas, and liquefied petroleum gas as well as hundreds of petrochemicals.

[0003] In recent years, there has been a major increase of illegal activities related to oil and gas assets. For example, the number of oil and gas thefts in areas such as Texas and Mexico has increased nearly ten times in the past ten years. Corruption, theft, tampering, stealing and other such illegal activities occur along all phases and sectors of supply chain, including upstream, midstream and downstream. Pipeline taps, crude oil diversion, trucking hijacks, underground tunnels and stealing oil in refineries are just a few examples of the types of illegal activities that have become too prevalent within the industry. With this uptick in activity, there are several challenges faced by the oil and gas industry. For example, events that occur are not always related to one another geographically or otherwise, and provide a chain of fragmented events and incidents. Currently, many different solutions and technologies exist to assist in management,

but they are not homogenous or compatible systems. A lack of coordinated communication and transparency among regions, functions and teams provides various challenges, and a lack of recordability and traceability of events stymies accountability. Thus, it becomes difficult to respond to such events and incidents in a timely manner, if at all.

[0004] As such, there exists a need to provide an intelligent management system that can address the need of monitoring and reporting or alerting illegal activities on oil and gas assets while at the same time increasing reliability, safety, regulatory compliance and environmental responsibility. Additionally, there is a need for a system that prescribes actions on the assets in the upstream, midstream and downstream sectors by remotely monitoring, analyzing, predicting events on this asset, and providing data as an alert to allow for decision making from any location. The term asset, as defined herein, includes all oil and gas products and infrastructure.

SUMMARY OF THE DISCLOSURE

[0005] The present disclosure, through one or more of its various aspects, embodiments, and/or specific features or sub-components, provides various systems, servers, methods, media, and programs for interfacing compiled codes, such as, for example, Java or data mining algorithms or mix of hardware and software elements to generate data with additional attributes useful in a Global Management System (GMS) related to management of oil and gas assets. The data with additional attributes are enhanced data which are used to create events useful to create in a specific module of the GMS clustered events.

[0006] The present disclosure generally relates to a system and method for collecting data from industrial control systems (ICS) and generating data compatible with an external system in an oil and gas asset supply chain, and in particular to an interface and interface method for generating secure and verifiable data to prevent tampering, or injection of unwanted data resulting from an unauthorized access along a supply chain.

[0007] In one embodiment, there is a method of generating data in an oil and gas supply chain for compatibility with external systems, including capturing collected data from at least one of an industrial control system, sensor and data collector; signing and storing the collected data in a secure intermediary hardware platform to interface with at least one software component; and adding attributes to the collected data using a business rules engine to create enhanced data.

[0008] In another embodiment, there is an interface generating data in an oil and gas supply chain for compatibility with external systems, including at least one of an industrial control system, sensor and data collector to capture collected data; a secure intermediary hardware platform signing and storing the collected data to interface with at least one software

component; and a business rules engine adding attributes to the collected data to create enhanced data.

[0009] In still another embodiment, there is a non-transitory computer readable medium storing a program to generate data in an oil and gas supply chain for compatibility with external systems, the program when executed by a processor, including capturing collected data from at least one of an industrial control system, sensor and data collector; signing and storing the collected data in a secure intermediary hardware platform to interface with at least one software component; and adding attributes to the collected data using a business rules engine to create enhanced data.

[0010] In one aspect, the collected data is collected from at least one of an industrial control system, sensor and data collector.

[0011] In another aspect, the collected data is redundantly checked or acquired several times and averaged and verified from at least one of an industrial control system, sensor and data collector to confirm the accuracy of information in the collected data prior to being transferred to the secure intermediary hardware platform.

[0012] In still another aspect, the secure intermediary hardware platform is secured from at least one of tampering, injection of unwanted data and unauthorized access.

[0013] In yet another aspect, the additional attributes of the enhanced data include at least one of a secure attribute, allowing detection of modification or corruption and authentication.

[0014] In another aspect, at least one software component sends the enhanced data with the additional attributes to a data integration module in a secure manner.

[0015] In still another aspect, the business rules engine stores and queues the enhanced data, including the additional attributes, in an encrypted and persistent data storage.

[0016] In one aspect, the enhanced data with additional attributes interfaces with an external system.

[0017] In yet another aspect, the enhanced data could be received directly at a data integration module, from the plurality of industrial control systems and then collected and/or organized into clustered events in a global management system; in the part of the global management system preferably at a control center at least one of monitoring alerts is performed, creating alerts and decisions are provided based on the clustered events generated from the data managements system; at the control center, a visualization of the clustered events is displayed; and via the control center and communication with at least one of the data integration module, external operational support and personnel and resources can or will be performed.

[0018] In one aspect, the capturing and transferring of collected data uses system drivers to collect data from at least one of a physical source, programmable logic control and remote terminal units.

[0019] In still another aspect, the industrial control systems are for an upstream, midstream and downstream portion of a supply chain for the oil and gas assets.

[0020] In another aspect, each of the industrial control systems for the upstream, midstream and downstream portions are grouped as a single repository.

[0021] In yet another aspect, the collected data from each of the industrial control systems is provided to the secure intermediary platform in the form of at least one of: non-secure data, secure data, separately formatted data, commonly formatted data, data with secure attributes, read only data, and non-forgeable data.

[0022] In another aspect, interfacing includes communicating the collected data from the industrial control system to the data integration module via the secure intermediary hardware platform in a secure communication to ensure integrity of the collected data.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] The present disclosure is further described in the detailed description which follows, in reference to the noted plurality of drawings, by way of non-limiting examples of preferred embodiments of the present disclosure, in which like characters represent like elements throughout the several views of the drawings.

[0024] Figure 1 is an exemplary supply chain for use in the oil and gas industry.

[0025] Figure 2 is an exemplary system for use in accordance with the embodiments described herein.

[0026] Figure 3 is an exemplary diagram of a global management system in accordance with an embodiment of the disclosure.

[0027] Figure 4 is another exemplary diagram of a global management system in accordance with an embodiment of the disclosure.

[0028] Figure 5 illustrates an exemplary embodiment of communication between the data management system and the control center in accordance with an embodiment of the disclosure.

[0029] Figure 6 is an exemplary diagram of a global management system in accordance with an embodiment of the disclosure.

[0030] Figure 7 illustrates an exemplary diagram of an interface in accordance with one embodiment of the disclosure.

[0031] Figure 8A – 8D show an exemplary sequence of events in which the captured data occurs over time to determine a probability.

[0032] Figure 9 is an exemplary diagram of an interface in accordance with one embodiment of the disclosure.

[0033] Figure 10 is an exemplary embodiment of a process flow of the interface in accordance with one embodiment of the disclosure.

DETAILED DESCRIPTION

[0034] The present disclosure, through one or more of its various aspects, embodiments and/or specific features or sub-components, is thus intended to bring out one or more of the advantages as specifically noted below.

[0035] Figure 2 is an exemplary system for use in accordance with the embodiments described herein. The system 100 is generally shown and may include a computer system 102, which is generally indicated. The computer system 102 may operate as a standalone device or may be connected to other systems or peripheral devices. For example, the computer system 102 may include, or be included within, any one or more computers, servers, systems, communication networks or cloud environment.

[0036] The computer system 102 may operate in the capacity of a server in a network environment, or the in the capacity of a client user computer in the network environment. The computer system 102, or portions thereof, may be implemented as, or incorporated into, various devices, such as a personal computer, a tablet computer, a set-top box, a personal digital assistant, a mobile device, a palmtop computer, a laptop computer, a desktop computer, a communications device, a wireless telephone, a personal trusted device, a web appliance, or any other machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that device. Further, while a single computer system 102 is illustrated, addition embodiments may include any collection of systems or sub-systems that individually or jointly execute instructions or perform functions.

[0037] As illustrated in Figure 2, the computer system 102 may include at least one processor 104, such as, for example, a central processing unit, a graphics processing unit, or both. The computer system 102 may also include a computer memory 106. The computer memory 106 may include a static memory, a dynamic memory, or both. The computer memory 106 may additionally or alternatively include a hard disk, random access memory, a cache, or any combination thereof. Of course, those skilled in the art appreciate that the computer memory 106 may comprise any combination of known memories or a single storage.

[0038] As shown in Figure 2, the computer system 102 may include a computer display 108, such as a liquid crystal display, an organic light emitting diode, a flat panel display, a solid state display, a cathode ray tube, a plasma display, or any other known display.

[0039] The computer system 102 may include at least one computer input device 110, such as a keyboard, a remote control device having a wireless keypad, a microphone coupled to a speech recognition engine, a camera such as a video camera or still camera, a cursor control device, or any combination thereof. Those skilled in the art appreciate that various embodiments of the computer system 102 may include multiple input devices 110. Moreover, those skilled in the art further appreciate that the above-listed, exemplary input devices 110 are not meant to be exhaustive and that the computer system 102 may include any additional, or alternative, input devices 110.

[0040] The computer system 102 may also include a medium reader 112 and a network interface 114. Furthermore, the computer system 102 may include any additional devices, components, parts, peripherals, hardware, software or any combination thereof which are commonly known and understood as being included with or within a computer system, such as, but not limited to, an output device 116. The output device 116 may be, but is not limited to, a speaker, an audio out, a video out, a remote control output, or any combination thereof.

[0041] Each of the components of the computer system 102 may be interconnected and communicate via a bus 118. As shown in Figure 2, the components may each be interconnected and communicate via an internal bus. However, those skilled in the art appreciate that any of the components may also be connected via an expansion bus. Moreover, the bus 118 may enable communication via any standard or other specification commonly known and understood such as, but not limited to, peripheral component interconnect, peripheral component interconnect express, parallel advanced technology attachment, serial advanced technology attachment, etc.

[0042] The computer system 102 may be in communication with one or more additional computer devices 120 via a network 122. The network 122 may be, but is not limited to, a local area network, a wide area network, the Internet, a telephony network, or any other network commonly known and understood in the art. The network 122 is shown in Figure 2 as a wireless network. However, those skilled in the art appreciate that the network 122 may also be a wired network.

[0043] The additional computer device 120 is shown in Figure 2 as a personal computer. However, those skilled in the art appreciate that, in alternative embodiments of the present application, the device 120 may be a laptop computer, a tablet PC, a personal digital assistant, a mobile device, a palmtop computer, a desktop computer, a communications device, a wireless telephone, a personal trusted device, a web appliance, a television with one or more processors

embedded therein and / or coupled thereto, or any other device that is capable of executing a set of instructions, sequential or otherwise, that specify actions to be taken by that device. Of course, those skilled in the art appreciate that the above-listed devices are merely exemplary devices and that the device 120 may be any additional device or apparatus commonly known and understood in the art without departing from the scope of the present application. Furthermore, those skilled in the art similarly understand that the device may be any combination of devices and apparatuses.

[0044] Of course, those skilled in the art appreciate that the above-listed components of the computer system 102 are merely meant to be exemplary and are not intended to be exhaustive and/or inclusive. Furthermore, the examples of the components listed above are also meant to be exemplary and similarly are not meant to be exhaustive and/or inclusive.

[0045] Figure 3 is an exemplary diagram of a global management system in accordance with an embodiment of the disclosure. The global management system GMS includes, but is not limited to, a control center CCC, a data management system, and sensors used for secure measurement. The global management system GMS manages oil and gas assets in a secure manner (or non-secure manner, if desirable) by monitoring for illegal activities on the supply chain, alerting authorities and/or authorized personnel and responding to the illegal activities in an appropriate manner. For example, the system may alert authorities and/or authorized personnel, provide a written report to police or emergency service personnel, forecast or predict data, provide recommendations and/or respond automatically. It is appreciated that the examples provided are non-limiting and that any number of responses may be provided as understood in the art. It is also appreciated that the global management system GMS is not limited to management of illegal activities, but may also be employed during emergencies, accidents, intervention or any other use typically contemplated by a management system. Additionally, as explained in detailed below, the control center CCC utilizes data over time to detect and calculate trends and future events in the clustered events. In this regard, personnel in the control center CCC may be alerted before such events occur when a specified level of probability is reached. Also, as discussed in more detail below, the control center CCC displays (e.g. LCD display) alerts (in addition to normal activity) which reflect events or incidents that are being monitored. The alerts may be used by personnel to contact emergency personnel or provide field intervention, and may by automatically supplied by the control center CCC if authorized personnel do not respond to such alerts within a given time period or after reoccurring alerts.

[0046] The global management system GMS is provided information from sensor(s) and data collector(s) located at various geographical positions and regions, and are in the form of any well known sensor or data collector capable of sensing or collecting data given the nature of the

data that it is intending to capture. The sensors are configured to capture and collect data associated with the oil and gas assets traversing a supply chain, the data including, but not limited to, at least one of temperature, density, humidity, volume, gravity, chemical composition, pressure, weight, pressure variation of a pipeline, difference in weight of a vehicle or fuel volume, GPS localization, timing of a vehicle location, geographical region, flow rate, conductivity, rheology, turbidity, imaging, thermal imaging. Additionally the sensors may sense and collect, sensor status (i.e. fault functioning, disconnect, etc.), strain gauges, weather related data, traffic, vehicle or road condition, wind speed, barometric conditions, rainfall, maintenance data or maintenance date, personal position information (e.g. location of closest fireman or police facilities) radar, motion detectors, RF data, acoustic data, GPS position, data extracted from drones, stock value of petrol, etc. Information may also be collected by data collectors. For example, information and data contained in an SAP™ or Oracle™ repository which could be any data, forecast, purchase of products, tax value, etc.

[0047] Sensors and data collectors (sensing and collecting data in the form of secure measurements) may be located in the upstream sector, midstream sector and/or downstream sector of the oil and gas asset supply chain. The data are collected and sent to the gateway (Fig. 6). The gateway is a collector of data from a variety of sources (e.g. ICS such as SCADA, said ICS using protocols such as MODBUS, AS-iOPC, EtherCAT, etc.) and includes a business rules engine (BRE). The gateway may also collect data directly from the sensor, data collectors or any device providing data within the upstream, midstream and downstream sectors. The collected data may be transformed into secure (or additional secured) data that includes, for example, a timestamp and various attributes. Once the data is transformed by the gateway, the data is sent (preferably securely) to the data integration module. Additionally or alternatively, the collected data may be stored in a repository or multiple repositories and then sent the global management system GMS, where the clustered events will be generated from the data. It is also appreciated that the collected data need not come from the sources listed above, but may come from any internal or external source of data.

[0048] The data integration module includes a data management system that stores the data, acquires the data from storage, and creates a key value data structure from the data, sorts the structure data and analyzes the structured data using computational models and algorithms to identify events. The data is also checked for integrity of the structured data and the secureness of the structured data to prevent tampering. The clustered events are generated by the data management system for use by the control center CCC. The control center CCC (which may comprise processor(s), software, an interface(s), and multiple displays, and/or personnel to control and command information on the global management system GMS, and or, for example,

any of the components described in Figure 2, and which may be provided locally or remotely at any geographical location, mobile or otherwise) performs monitoring of events and alerts, creates alerts and provides decisions based on the clustered events generated from the data management system. The control center also provides communication with external operational support and personnel and resources.

[0049] The computations models and algorithms used in the global management system GMS are not limited to any particular model or algorithm. Rather, it is appreciated that any number of solutions may be used in this system. However, as an example, a data mining algorithm that is a set of heuristics and calculations that creates a data mining model from data. To create a model, the algorithm first analyzes the data provided and looks for types of patterns or trends. The algorithm uses the results of the analysis to define optimal parameters for creating the mining model. These parameters are then applied across the entire data set to extract actionable patterns and detailed statistics. The mining model that an algorithm creates from collected data can take various forms, including: a set of clusters (e.g. clustered events) that describe how the cases (e.g. events) in a dataset are related; a decision tree that predicts an outcome, and describes how different criteria affect that outcome. Using the data mined by the algorithms, the system is able to utilize historical data and improve accuracy over time. The accuracy may also be supplemented by human or drone verification at the location an event occurs, and using the alerts generated by the system.

[0050] Figure 4 is another exemplary diagram of a global management system in accordance with an embodiment of the disclosure. The diagram illustrates a flow of data from the initial sensing and collecting of data at the upstream, midstream and downstream sectors all the way through any necessary field intervention that may occur as a result of the monitoring and alerts provided by the control center CCC. Within each stream (sector), there are multiple technologies, assets and generations of assets. These technologies are not consolidated and therefore not monitored together. The integration of the collected data interfaces between the various technologies and systems, provides communication between the technologies and systems that have different protocols and integrates external systems, such as ERPs and the like. The integrated data is formatted, stored and analyzed for use by the (command and) control center CCC. The control center CCC provides an overview of the collected data by monitoring the data provided by the data management system, alerting at the level of the control center (and personnel when necessary) of events or sequences of events and diagnosing and analyzing the data. To the extent necessary, intervention from security and emergency personnel, drones, remote cameras and any other resource capable of intervening or providing intervening measures

will be contacted and informed of the control center CCC results. Data gathered and extracted by drones or videos cameras is stored in the repository(ies) of the system for use in future analysis.

[0051] Figure 5 illustrates an exemplary embodiment of communication between the data management system and the control center in accordance with an embodiment of the disclosure. The data management system provides real-time data, event classification and recommendations to the control center CCC based on collected data that has been analyzed, as described above and further below. The control center CCC confirms the event classifications and responds with a notification to the data management system, which may be securely logged with a timestamp. The control center CCC also performs monitoring of events and alerts, creates alerts and provides decisions based on the clustered events generated from the data management system. Notifications and alerts may be presented to, for example, personnel located at the control center CCC or remotely located using any number of interfaces. Interfaces can convey information as visual information, audible information, or in any other form, and may be conveyed using mobile devices as well as non-mobile devices. The control center also provides communication with external operational support and personnel and resources. For example, external operational support and personnel can provide field of intervention to verify whether alerts are accurate (e.g. whether an explosion occurs, material is stolen), and drones can be mobilized and sent to a specific region related to the alerts to verify and can provide visualization to enhance the value of the analysis of the clustered events.

[0052] Figure 6 is an exemplary diagram of a global management system in accordance with an embodiment of the disclosure. The global management system GMS includes, but is not limited to, a control center CCC, a data management system, a data integration module, a user interface, a gateway interface, and sensors or data collectors used for capturing data from upstream, midstream and downstream. The global management system GMS may also include or extend to external resources such as ERPs, field and resource management, predictive and prescriptive applications, evidence based event management and existing legacy systems. It is appreciated that the global management system GMS is not limited to the disclosed components, nor must it include each of the components illustrated in the non-limiting and exemplary embodiment. For example, a supervisory control and data acquisition (ICS such as SCADA) system may replace the collection of data instead of the gateway interface. As noted above, data may be stored in a single repository or multiple repositories.

[0053] The global management system GMS manages oil and gas assets in a secure manner (or non-secure manner, if desirable) by monitoring for illegal activities on the supply chain, alerting authorities and/or authorized personnel and responding to the illegal activities in an appropriate manner. The global management system GMS collects the heterogeneous,

unstructured and fragmented data from sensors, data collectors and monitoring sub-systems in the upstream, midstream and downstream oil and gas infrastructure (pipelines), to store and process the collected data using knowledge of the oil and gas infrastructure systems. The data is structured for additional processing and analysis, and the integrity of the structured data is verified and secured to prevent tampering. Eventually, as described above, the data is sent to the control center CCC for personnel to respond to theft or similar operational incidents. This process allows for a more rapid response than compared to current systems, as well as provide an evidential basis that constitutes material proof admissible in a court of law to support prosecution of criminal offenders. For example, drones may be used to provide on site evidence that an event has occurred.

[0054] More specifically, collected data will be acquired and processed in real-time and routed to the control center CCC (which may be in form of a physical command control center and/or an application operationally independent from personnel, or any combination thereof) for appropriate display to command center personnel. Structured data will be analyzed according to computational models and/or algorithms to identify events, where the events can be operational incidents such as those illegal activities described above and also operational problems, which may be identified and displayed to operators in real-time. In parallel (or at another time), the structured data and events may be entered into a prediction and prescriptive analysis module (predictive and prescriptive application) that uses machine learning, as described above, to identify sequences of measurements (Figure 8A) or computed data that are classified as "events" that require some form of action and/or reporting. The classification of an event, previously supplied by the data management system, can be confirmed (by a human operator or machine) and the results sent to the prediction and prescription module to improve the training set for the learning algorithm, allowing it to "learn" over the course of time. Using machine learning, the global management system GMS will learn which series of event measurements taken together will indicate that a certain event or cluster of events has occurred. Using the "learned" events, the system is able to utilize historical data and improve accuracy over time. The accuracy may also be supplemented by human or drone verification at the location an event occurs, and using the alerts generated by the system.

[0055] The data management system, similar to the control center CCC, may also be in communication with the prediction and prescription module, which will use machine learning on structured data and events as learning sets to classify events, which can be understood as sequences of measurements. The prediction and prescription module provides information to identify probable events (at varying degrees) in the future, or events in progress that may be sent as events to the control center CCC. The prediction and prescription module can also prescribe

the event response most likely to result in a positive outcome based on the history of events. Similarly, recognized (or known) trends that occur over the course of time may be used to improve the clustered events to more accurately generate the alerts in the control center CCC.

[0056] Figure 7 illustrates an exemplary diagram of an interface in accordance with one embodiment of the disclosure. As illustrated, the interface (gateway) receives data from one or more of a variety of sources. For example, the data collected from the upstream, midstream and downstream sensors that are processed by the SCADA systems is passed along to the gateway interface. In an alternative embodiment, the gateway replaces the industrial control system (such as SCADA) and collects data directly from the upstream, midstream and downstream sensors (Figure 6). The gateway interface transforms (e.g. sorts, formats and modifies) the collected data into secure and formatted data that is compatible with the system, and in particular the data integration module, prior to being sent to the data management system for analysis by the global management system GMS.

[0057] Figures 8A – 8D illustrate exemplary sensor measurements and sensors collecting data along a supply chain in accordance with an embodiment of the disclosure. The control center CCC through the interface to the field and resource management (Figure 6) can take a number of actions based on the real-time data and events received from the data management system. Once a particular sequence of measurements (or sequence of events) associated with an event description is known (i.e. learned by the prediction and prescription application, events can be flagged in real-time and sent to the control center CCC along with a probability score indicating the likelihood that a sequence of measurements unfolding will result in an identified event. In the figures, the shaded boxes represent the values received from a given sensor. Figure 8A shows an exemplary number of sensors 1...m that are configured to capture a sequence of events. Figures 8B, 8C and 8D show an exemplary sequence of events in which the captured data over the course of time t represents a weak probability, a medium probability and a high probability, respectively, of the event having occurred (termed here, the event probability).

[0058] The event probability is sent to the control center CCC along with a recommendation, such as "Theft possible in Pipeline Section 452, send intervention team to Sector D." The control center CCC may respond in any number of ways, including, but not limited to, the following: request additional data display for the indicated area in which the event (incident) has occurred; direct drones (UAVs) to the affected area for surveillance or capturing information or for visualization; dispatch intervention teams or humans (such as police, fireman...) to the area to check out the event or what happens in the field; or order an evacuation of personnel in the field depending on what happens (for example explosion on site during petrol extraction).

[0059] To improve efficiency, using the predictive and prescriptive module, based on past events contained in historical data of measurements and events, patterns may be generated and used from the historical data to assist in predicting future events (incidents) before the sensors and data collectors begin to register data. Using this predictive data, the control center CCC and personnel operating the control center CCC could be alerted to predicted "hot areas" for theft identified by the system using data in the system, such as time of day, day of week, month or specific dates, weather conditions, previous event sequences, and the like. For example, based on a predicted "hot area," UAVs could be deployed to capture and display video, and intervention teams could be stationed nearby so that the event may be prevented. Or, if the event occurs, the intervention time will be reduced because the relevant resources are nearby. Additionally, the data management system may instruct the control center CCC to automatically display data from the "probable" areas where events are likely to occur, so that personnel may inspect the data and video from those areas to detect anomalies and activities in advance of any occurrence. The global management system GMS may also use a mix of data mining algorithms and human action to update system data based on events and analysis, with confirmation by personnel on the field or where problems have occurred.

[0060] It is appreciated from the above that that the global management system GMS is capable of recording the evolution of events, and link them together for providing a history to analyze and improve the data analysis in the data management system. Based on the prior knowledge of events having occurred in the past, historical data and verification that the events actually occurred, such as a hole being made in a pipeline such that fuel may be stolen, future events can be more accurately predicted and the events themselves may be better interpreted during monitoring and analysis. Additionally, the global management system GMS by virtue of its predictive and prescriptive nature is able to mitigate corruption by people, for example operating personnel in the control center CCC. Accordingly, it becomes increasingly difficult, for people involved with the illegal activities to avoid detection by deleting data, changing data, paying off personnel monitoring the data, etc.

[0061] Significantly, to avoid these types of situations from occurring, the global management system provides: secure and unforgeable data which may not be deleted, alerts based on the correlation of clustered events that give a high probability of illegal activity, which activity may be displayed to an operator and recorded as alerts that are also unforgeable and may not be deleted. Alternatively or additionally, the system itself may intervene in place of personnel to identify and send urgent information to external authorities such as police, fireman, etc. Accordingly, a part of the system is to supply an alternative to human error and inadequacies.

[0062] Further non-limiting examples of the global management system GMS, are provided below with respect to the midstream and downstream sectors. In the midstream sector, illegal activities typically occur by diverting or stealing materials. For example, in the pipeline of a supply chain, a hole can be made to pump petrol along the pipeline in an effort to steal, often successfully, the petrol. As countermeasures and in accordance with the objectives of the global management system GMS, the pipeline may be lined with several sensors and/or data collectors that will monitor and collect data from the pipelines. For example, speed of the flow, temperature, pressure, volume, etc. may be monitored and data collected. The collected data from the sensors and data collectors will be sent to the corresponding gateway (Figure 6) or industrial control system ICS, and escalated to the data management system and on to the control center CCC, as described herein above. Additionally, the collected data should be updated in a manner that it may be interpreted to provide conclusions and recommendations. For example, if the sensor(s) or data collector(s) only measure the pressure in the pipeline every hour, when the fuel or crude oil is being illegally extracted, the sensor(s) and data collector(s) may not capture the illegal activity. If, on the other hand, the pressure in the pipeline is measured each minute, the sensor(s) and data collector(s) will be able to measure any increase or decrease in the pressure (or any other type of data, such as volume decrease, chemical presence of air or water) indicating that illegal activities are occurring. Linked with the localization of the sensor(s) and data collector(s), a drone or personnel could be sent automatically to the regional location, images could be captured from a local camera, and the police or emergency response personnel could be notified that the activities are underway.

[0063] Another non-limiting example of data in the midstream is a tanker truck transporting crude oil and petroleum. In this example, the collected data is GPS information generated by the trip made by the truck, and the volume of the content of the truck's tank. If the data collected over time indicates, for example, that the truck is stopping at a location longer than anticipated, or there is a variation of volume of the content of the tank, this may indicate that illegal activities are occurring or have occurred. In another example, the truck can be stopped at an overnight rest area. Since these areas are a known, regular stop for an extended period, volume sensors on the truck may be activated to monitor variations in the content of the tank. In a particular, it may be known that the particular region is known to have illegal activities. Together, any change in variation detected by the sensors can be escalated through the data management system to the control center CCC after the data has been analyzed. Authorities can be sent to the location if necessary, and the system's learning engines will become aware of the region and expectation of illegal activities in the area, and apply such knowledge in further

analysis. The content (assets) could also be marked by chemical or forensic markers to retrieve them when for example, detected in a retail shop or by authorities.

[0064] In the downstream sector, a non-limiting example is provided in which collected data includes the volume produced in a refining factory. The volume data may be linked, for example, with the number of trucks required to transport the truck's content (fuel) to retails shops. As understood, once the fuel reaches the retail shops, it is unloaded into shop tanks for storage. Here, the volume is transferred and the fuel is distributed. Sensors and data collectors may then be used to measure the corresponding volumes exchanged, and cash generated by the sale of fuel. If the volumes and sales do not match, this could indicate illegal activities, such as embezzlement. This information may also be useful for tax recollection or reconciliation, to estimate the amount of fuel required in a particular region, etc. As appreciate, the data is not only collected, but also stored in a repository and transformed into a sum of clustered events that may be linked, used or analyzed for prescriptive or predictive action.

[0065] Figure 9 is an exemplary diagram of an interface in accordance with one embodiment of the disclosure. The interface, in this application also referred to as the Gateway or Gateway interface, interfaces the data sensors that are positioned along the upstream, midstream and downstream sectors to external sources, such as an enterprise service bus ESB or the data global management system GMS via the data integration module. As illustrated, the gateway is divided into three layers including: (1) the compturer (for signing and storing) which communicate with industrial control systems (such as SCADA, OPC, AS-i MODBUS and Ethercat). The drivers may be a combination of physical interfaces and software, (2) the business rules engine (BRE) which correlates, secures, authenticates, filters, reconciles, provides unforgeability, and creates key value data. The BRE will also from the data collected, make association of data collected into objects, create events based on non-integrity of objects, create events-based alert or events-based on thresholds or on business rules or on trends , and (3) the interfaces that interface with the external systems using, for example, HTTPS, SSL or any other known software or hardware protocol.

The gateway interface provides, among other features, a mechanism to manage the collected the data into a format that is further secured and which is compatible with the external system to which the transformed data or objects or events or alerts created in the Gateway will be sent. For example, the gateway interface will secure the collected data from the sensors and/or data collectors as well as formatting the collected data to be compatible with the data integration system before being used in the global management system GMS especially at the Data Management System (DMS) level. The gateway interface interfaces with external systems using, for example, protocols such as HTTPS, SSL, etc. External interfaces include, but are not

limited to, an enterprise service bus ESB or an industrial control system ICS, such as the gateway management system GMS described herein.

[0066] At the driver layer, the drivers which communicate with external systems, such as the ICS system, may be hardware, software or any combination therefore. The hardware and software is preferably tamper resistant and secure in order to avoid attacks on the physical hardware as well as malicious attacks on the software, for example by hackers, injection of unwanted data or the like. The data that will be generated and created in the gateway interface will be more secure and provide enhanced properties in addition to those collected from the various repositories of data, such as the SCADA or ICS. The secure and enhanced data will then be provided to the global management system GMS and assist in creating the clustered events. The gateway will also verify that data being received from the sensor(s) and data collector(s) are authentic data and have not been corrupted by external sources or otherwise. That is, the gateway will first have the capability to authenticate data being received before securing the data and adding additional properties. This will ensure that the data to be secured and enhanced is authenticated prior to being passed to the global management system GMS, and will avoid corrupted data being sent to the global management system GMS. One weakness of existing systems in the oil and gas supply chain is the incredibly large volume of data. If the system becomes contaminated or infected with fake, counterfeit, fabricated or inaccurate data, the data captured will not be reliable and any events or clustered events created in the global management system GMS may potentially compromise the alerts generated from the clustered events. Accordingly, any data to be accessed or used in the global management system GMS (via the data integration module), using the gateway, should be as secure and accurate as possible. An example of authenticating the data that will be inserted in the gateway, is to capture from the sensors, several times the information it is supposed to capture and in a short period of time and verifying that the data collected is always of the same nature (e.g. the temperature is captured ten times during 30 seconds and the value is quite the same, then the data seems to be correct). Another example of authenticating or being sure that the data is accurate is to add to the sensor an electronic system or mechanism that protect him from tampering or diversion and protect the access to the sensor by any means, the data collected from the sensor and then send to the gateway will be accurate as possible.

[0067] The gateway interface collects data either via the physical interfaces to industrial sensors utilizing industrial communication protocols, such as OPC or Ethercat, or via virtual (i.e. software) interfaces to existing monitoring or control systems, such as SCADA. The interfaces are powered, for example, using software drivers which can be dynamically loaded or unloaded depending on the physical or virtual requirements. For example, if there are three OPC powered

devices and an Ether cat device physically attached, then there would be three OPC drivers and a single Ethercat driver.

[0068] Once the data reaches the gateway interface, the Business Rules Engine BRE create new monitoring data by correlating captured data, filtering irrelevant data, for example non--security related events, validating read/write access to/from the driver layer to the integration layer (in both directions), and applying security/access/authentication rules, using an external system if necessary. It is appreciated, however, that these functions are only exemplary and the BRE is not limited to such functions.

[0069] At the interface layer, the software in the gateway interface may also interact with external systems based on the monitoring requirements. For example, the interface may include an email interface, a web interface, etc. The interface layer may also interface with the enterprise service bus ESB as a messaging system (for example, utilizing a protocol such as REST over HTTPS) to integrate data from all gateway interfaces and external systems into the data storage component of the global management system GMS. It is also appreciated that although the diagram illustrates an interface to the gateway interface, the gateway interface may also be directly connected or a part of global management system GMS.

[0070] The enterprise service bus ESB software is a messaging system similar to the IBM™ products MQueue Series and BMC Control. The ESB software, which in the instant embodiment is referred to as the data integration module part of the global management system GMS (although it is appreciated that the ESB could also be a separate entity), could be application such as Open ESB developed by Sun Microsystems™ or WSO2 ESB. A JAVA based programming language may be used as the programming language to achieve such software.

[0071] The Business Rules Engine BRE, the second layer, acts as the transformation processing of the captured data and applies rules which can be configured to represent a particular element of interest, such as a potential security incident. The BRE monitors all activities and measuring points of all the drivers loaded, along with any physically or virtually connected devices. By accessing all of these measuring points in real time, the BRE can create new measuring points or data useful to create clustered events in the global management system GMS. The BRE will also from the data collected, make association of data collected into objects, create events based on non-integrity of objects, create events-based alert or events-based on thresholds or on business rules or on trends . For example, measuring point A on a physically connected device (such as a temperature sensor) and measuring point B (such as a variable from an external software SCADA system) under specific thresholds can create new data based on both measuring point A and measuring point B. For example new data C may be created, where

the new C data is an appendage of measuring points A and B and which can constitutes an event. This enables the BRE to correlate data for a better understanding of events as they occur. The events generated in the Gateway are based on the data collected from sensors, data collector or ICS systems. To these data which have been checked in their accuracy before entering in the Gateway, addition of attributes to the data to obtain enhanced data is made.

[0072] Another possibility, if the sensors, data collectors or ICS systems are not reliable or able to check the accuracy of the data, this step of checking is made in the Gateway. The events created in the Gateway will be useful in the DMS of the GMS to create the clustered events. Said clustered events are used in the GMS to create and/or display alerts at the CCC level and will allow in the context of the present invention to mobilize efficiently the corresponding field intervention (i.e., police when theft of material, fireman if explosion....) .

[0073] The BRE may also act autonomously if enough physical and/or virtual information is available to determine, based on data collected events useful for creating in the global management system GMS clustered events without reliance on any external system, the clustered events will be useful to determine actions such as notifications to identify or alert security incidents and other actions. Definition(s) of the clustered events is managed via the data management module of the global management system GMS as part of the "learning" nature of the system. The BRE stores and queues, when necessary, these data and encrypts or signs each data to ensure the data is complete, authentic, accountable, non-repudiated, and protected from external access, modification, disruption and destruction. It is appreciated that any one or more, none or all of these features may be used, in addition to another form of functionality. The encrypted data may then be accessed by external systems based on, for example, security profiles of the system requesting the information.

[0074] Figure 10 is an exemplary embodiment of a process flow of the interface in accordance with one embodiment of the disclosure. The drivers of the gateway interface collect data from a variety of sources including, but not limited to, physical sources, programmable logic control (PLC) and remote terminal units (RTU) and any other type of source. The business rules engine BRE processes the data, correlates the data and creates from the data events or a sequence of events, as described in detail above. The data and events are optionally signed by a Hardaware or software security module (HSM or SSM) Events and enhanced data may be stored in a secure repository or data storage. The gateway then checks to determine where the data will be sent (GMS available), for example to the global management system GMS or another external

system. If the global management system GMS is available, then the data or events are formatted and validated for use by the global management system. Data going to an external system may or may be formatted and validated depending on the external system requirements. Data or events being passed to the global management system GMS is sent to the data integration module, which stores the data or the events, acquires the data from storage, creates for example a key value data structure from the data, sorts the structure data and analyzes the structured data using computational models and algorithms to identify correlation between data useful for the creation of clustered events in the global management system GMS. The data is also checked for integrity of the structured data and the security of the structured data to prevent tampering. The data interface may be an independent interface or part of the data management system. If separate, the data is then passed along to the data management system for processing in accordance with the embodiments described above.

[0075] Accordingly, the present disclosure provides various systems, servers, methods, media, and programs. Although the disclosure has been described with reference to several exemplary embodiments, it is understood that the words that have been used are words of description and illustration, rather than words of limitation. Changes may be made within the purview of the appended claims, as presently stated and as amended, without departing from the scope and spirit of the disclosure in its aspects. Although the disclosure has been described with reference to particular means, materials and embodiments, the disclosure is not intended to be limited to the particulars disclosed; rather the disclosure extends to all functionally equivalent structures, methods, and uses such as are within the scope of the appended claims.

[0076] While the computer-readable medium may be described as a single medium, the term "computer-readable medium" includes a single medium or multiple media, such as a centralized or distributed database, and/or associated caches and servers that store one or more sets of instructions. The term "computer-readable medium" shall also include any medium that is capable of storing, encoding or carrying a set of instructions for execution by a processor or that cause a computer system to perform any one or more of the embodiments disclosed herein.

[0077] The computer-readable medium may comprise a non-transitory computer-readable medium or media and/or comprise a transitory computer-readable medium or media. In a particular non-limiting, exemplary embodiment, the computer-readable medium can include a solid-state memory such as a memory card or other package that houses one or more non-volatile read-only memories. Further, the computer-readable medium can be a random access memory or

other volatile re-writable memory. Additionally, the computer-readable medium can include a magneto-optical or optical medium, such as a disk or tapes or other storage device to capture carrier wave signals such as a signal communicated over a transmission medium. Accordingly, the disclosure is considered to include any computer-readable medium or other equivalents and successor media, in which data or instructions may be stored.

[0078] Although the present application describes specific embodiments which may be implemented as code segments in computer-readable media, it is to be understood that dedicated hardware implementations, such as application specific integrated circuits, programmable logic arrays and other hardware devices, can be constructed to implement one or more of the embodiments described herein. Applications that may include the various embodiments set forth herein may broadly include a variety of electronic and computer systems. Accordingly, the present application may encompass software, firmware, and hardware implementations, or combinations thereof.

[0079] Although the present specification describes components and functions that may be implemented in particular embodiments with reference to particular standards and protocols, the disclosure is not limited to such standards and protocols. Such standards are periodically superseded by faster or more efficient equivalents having essentially the same functions. Accordingly, replacement standards and protocols having the same or similar functions are considered equivalents thereof.

[0080] The illustrations of the embodiments described herein are intended to provide a general understanding of the various embodiments. The illustrations are not intended to serve as a complete description of all of the elements and features of apparatus and systems that utilize the structures or methods described herein. Many other embodiments may be apparent to those of skill in the art upon reviewing the disclosure. Other embodiments may be utilized and derived from the disclosure, such that structural and logical substitutions and changes may be made without departing from the scope of the disclosure. Additionally, the illustrations are merely representational and may not be drawn to scale. Certain proportions within the illustrations may be exaggerated, while other proportions may be minimized. Accordingly, the disclosure and the figures are to be regarded as illustrative rather than restrictive.

[0081] One or more embodiments of the disclosure may be referred to herein, individually and/or collectively, by the term "invention" merely for convenience and without intending to

voluntarily limit the scope of this application to any particular invention or inventive concept. Moreover, although specific embodiments have been illustrated and described herein, it should be appreciated that any subsequent arrangement designed to achieve the same or similar purpose may be substituted for the specific embodiments shown. This disclosure is intended to cover any and all subsequent adaptations or variations of various embodiments. Combinations of the above embodiments, and other embodiments not specifically described herein, will be apparent to those of skill in the art upon reviewing the description.

[0082] The Abstract of the Disclosure is provided to comply with 37 C.F.R. §1.72(b) and is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, various features may be grouped together or described in a single embodiment for the purpose of streamlining the disclosure. This disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter may be directed to less than all of the features of any of the disclosed embodiments. Thus, the following claims are incorporated into the Detailed Description, with each claim standing on its own as defining separately claimed subject matter.

The above disclosed subject matter is to be considered illustrative, and not restrictive, and the appended claims are intended to cover all such modifications, enhancements, and other embodiments which fall within the true spirit and scope of the present disclosure. Thus, to the maximum extent allowed by law, the scope of the present disclosure is to be determined by the broadest permissible interpretation of the following claims and their equivalents, and shall not be restricted or limited by the foregoing detailed description.

What is claimed is:

1. A method of generating data in an oil and gas supply chain for compatibility with external systems, comprising:

capturing collected data from at least one of an industrial control system, sensor and data collector;

signing and storing the collected data in a secure intermediary hardware platform comprising at least one software component; and

adding attributes to the collected data using a business rules engine to create enhanced data.

2. The method according to claim 1 wherein at least part of the enhanced data created using a business rules engines are transformed into events.

3. The method according to claim 1 or 2 wherein the signing of the enhanced data or the events-based on enhanced data are signed or encrypted with at least one of hardware or software security module(s).

4. The method according to any of the preceding claims , further comprising securely collecting the collected data from at least one of an industrial control system, sensor and data collector.

5. The method according to any of the preceding claims, further comprising redundantly checking or acquired several times and averaged and verifying collected data from at least one of an industrial control system, sensor and data collector to confirm the accuracy of information in the collected data prior to being transferred to the secure intermediary hardware platform.

6. The method according to any of the preceding claims, further comprising protecting the secure intermediary hardware platform from at least one of tampering, injection of unwanted data and unauthorized access.

7. The method according to any of the preceding claims, wherein the additional attributes of the enhanced data include at least one of a secure attribute, allowing detection of modification or corruption and authentication.

8. The method according any of the preceding claims, wherein at least one software component sends the enhanced data with the additional attributes to a data integration module in a secure manner.

9. The method according to any of the preceding claims, wherein the business rules engine stores and queues the enhanced data in an encrypted and persistent data storage.

10. The method according to any of the preceding claims, wherein the enhanced data with additional attributes interfaces with an external system.

11. The method according to any of the preceding claims, further comprising:

receiving the enhanced data, at a data integration module, from the plurality of industrial control systems and collecting and/or organizing the enhanced data and the events created from the enhanced data into clustered events in a global management system;

performing, at a control center, at least one of monitoring alerts, creating alerts and providing decisions based on the clustered events generated from the data managements system;

displaying, at the control center, a visualization of the clustered events; and

interfacing, via the control center, to communicate with at least one of the data integration module, external operational support and personnel and resources.

12. The method according to any of the preceding claims, wherein the capturing and transferring of collected data uses system drivers to collect data from at least one of a physical source, programmable logic control and remote terminal units.

13. The method according to any of the preceding claims, wherein the industrial control systems are for an upstream, midstream and downstream portion of a supply chain for the oil and gas assets.

14. The method according to claim 4 or 5, wherein the each of the industrial control systems for the upstream, midstream and downstream portions are grouped as a single repository.

15. The method according to claim 4 or 5, wherein the collected data from each of the industrial control systems is provided to the secure intermediary platform in the form of at least one of non-secure data, secure data, separately formatted data, commonly formatted data, data with secure attributes, read only data, and non-forgeable data.

16. The method according to claim 10, wherein interfacing includes communicating the collected data from the industrial control system to the data integration module via the secure intermediary hardware platform in a secure communication to ensure integrity of the collected data.

17. An interface generating data in an oil and gas supply chain for compatibility with external systems, comprising:

at least one of an industrial control system, sensor and data collector to capture collected data;

a secure intermediary hardware platform signing and storing the collected data to interface with at least one software component; and

a business rules engine adding attributes to the collected data to create enhanced data.

18. An interface according to claim 17 wherein enhanced data created using a business rules engines are transformed into events.

19. An interface according to any of claims 17 or 18 wherein the signing of the enhanced data or the events-based on enhanced data are signed or encrypted with at least one of hardware or software security module(s).

20. The interface according to claims 17 to 19, wherein collected data from at least one of an industrial control system, sensor and data collector are collected in a secure manner.

21. The interface according to claims 17 to 20, wherein collected data from at least one of an industrial control system, sensor and data collector are redundantly checked or acquired several times and averaged and verified to confirm the accuracy of information in the collected data prior to being transferred to the secure intermediary hardware platform.

22. The interface according to claims 17 to 21, wherein the secure intermediary hardware platform is protected from at least one of tampering, injection of unwanted data and unauthorized access.

23. The interface according to claims 17 to 22, wherein the additional attributes of the enhanced data include at least one of a secure attribute, allowing detection of modification or corruption and authentication.

24. The interface according to claims 17 to 23, wherein at least one software component sends the enhanced data with the additional attributes to a data integration module in a secure manner.

25. The interface according to claims 17 to 24, wherein the business rules engine stores and queues the enhanced data in an encrypted and persistent data storage.

26. The interface according to claims 17 to 24 wherein the business rules engine stores and queues the events created from the enhanced data, in an encrypted and persistent data storage

27. The interface according to claim 17 to 26, wherein the enhanced data with additional attributes interfaces with an external system.

28. The interface according to claim 17 to 27 wherein the events created from the enhanced data interfaces with an external system.

29. The interface according to claim 17 to 28, further comprising:

a data integration module receiving the enhanced data from the plurality of industrial control systems collecting and/or organizing the enhanced data and the events created from the enhanced data into clustered events in a global management system; and

a control center performing at least one of monitoring alerts, creating alerts and providing decisions based on the clustered events generated from the data managements system,

the control center displaying a visualization of the clustered events, and

the control center interfacing to communicate with at least one of the data integration module, external operational support and personnel and resources.

30. The interface according to claim 17 to 29, wherein the capturing and transferring of collected data uses system drivers to collect data from at least one of a physical source, programmable logic control and remote terminal units.

31. The interface according to claim 17-30, wherein the industrial control systems are for an upstream, midstream and downstream portion of a supply chain for the oil and gas assets.

32. The interface according to claim 20, wherein the each of the industrial control systems for the upstream, midstream and downstream portions are grouped as a single repository.

33. The interface according to claim 20, wherein the collected data from each of the industrial control systems is provided to the secure intermediary platform in the form of at least one of: non-secure data, secure data, separately formatted data, commonly formatted data, data with secure attributes, read only data, and non-forgeable data.

34. The interface according to claim 27, wherein interfacing includes communicating the collected data from the industrial control system to the data integration module via the secure intermediary hardware platform in a secure communication to ensure integrity of the collected data.

35. A non-transitory computer readable medium storing a program to generate data in an oil and gas supply chain for compatibility with external systems, the program when executed by a processor, comprising:

capturing collected data from at least one of an industrial control system, sensor and data collector;

signing and storing the collected data in a secure intermediary hardware platform to interface with at least one software component; and

adding attributes to the collected data using a business rules engine to create enhanced data.

36. An non-transitory computer readable medium according to claim 35 wherein enhanced data created using a business rules engines are transformed into events.

37. An non-transitory computer readable medium according to any of claims 35 or 36 wherein the signing of the enhanced data or the events-based on enhanced data are signed or encrypted with at least one of hardware or software security module(s).

38. The non-transitory computer readable medium according to claim 35, further comprising securely collecting the collected data from at least one of an industrial control system, sensor and data collector.

39. The non-transitory computer readable medium according to claim 35 to 38, further redundantly checking or acquired several times and averaged and verifying collected data from at least one of an industrial control system, sensor and data collector to confirm the accuracy of information in the collected data prior to being transferred to the secure intermediary hardware platform.

40. The non-transitory computer readable medium according to claim 35 to 39, further comprising protecting the secure intermediary hardware platform from at least one of tampering, injection of unwanted data and unauthorized access.

41. The non-transitory computer readable medium according to claim 35 to 40, wherein the additional attributes of the enhanced data include at least one of a secure attribute, allowing detection of modification or corruption and authentication.

42. The non-transitory computer readable medium according to claim 35 to 41, wherein at least one software component sends the enhanced data with the additional attributes and events created from enhanced data to a data integration module in a secure manner.

43. The non-transitory computer readable medium according to claim 35 to 42, wherein the business rules engine stores and queues the enhanced data and the events created from the enhanced data, in an encrypted and persistent data storage.

44. The non-transitory computer readable medium according to claim 35 to 43, wherein the enhanced data and the events created from the enhanced data interfaces with an external system.

45. The non-transitory computer readable medium according to claim 35 to 44, further comprising:

receiving the enhanced data and the events created from enhanced data, at a data integration module, from the plurality of industrial control systems collecting and/or organizing the enhanced data into clustered events in a global management system;

performing, at a control center, at least one of monitoring alerts, creating alerts and providing decisions based on the clustered events generated from the data managements system;

displaying, at the control center, a visualization of the clustered events; and

interfacing, via the control center, to communicate with at least one of the data integration module, external operational support and personnel and resources.

46. The non-transitory computer readable medium according to claim 35, wherein the capturing and transferring of collected data uses system drivers to collect data from at least one of a physical source, programmable logic control and remote terminal units.

47. The non-transitory computer readable medium according to claim 35, wherein the industrial control systems are for an upstream, midstream and downstream portion of a supply chain for the oil and gas assets.

48. The non-transitory computer readable medium according to claim 38, wherein the each of the industrial control systems for the upstream, midstream and downstream portions are grouped as a single repository.

49. The non-transitory computer readable medium according to claim 38, wherein the collected data from each of the industrial control systems is provided to the secure intermediary platform in the form of at least one of: non-secure data, secure data, separately formatted data, commonly formatted data, data with secure attributes, read only data, and non-forgeable data.

50. The non-transitory computer readable medium according to claim 44, wherein interfacing includes communicating the collected data from the industrial control system to the data integration module via the secure intermediary hardware platform in a secure communication to ensure integrity of the collected data.

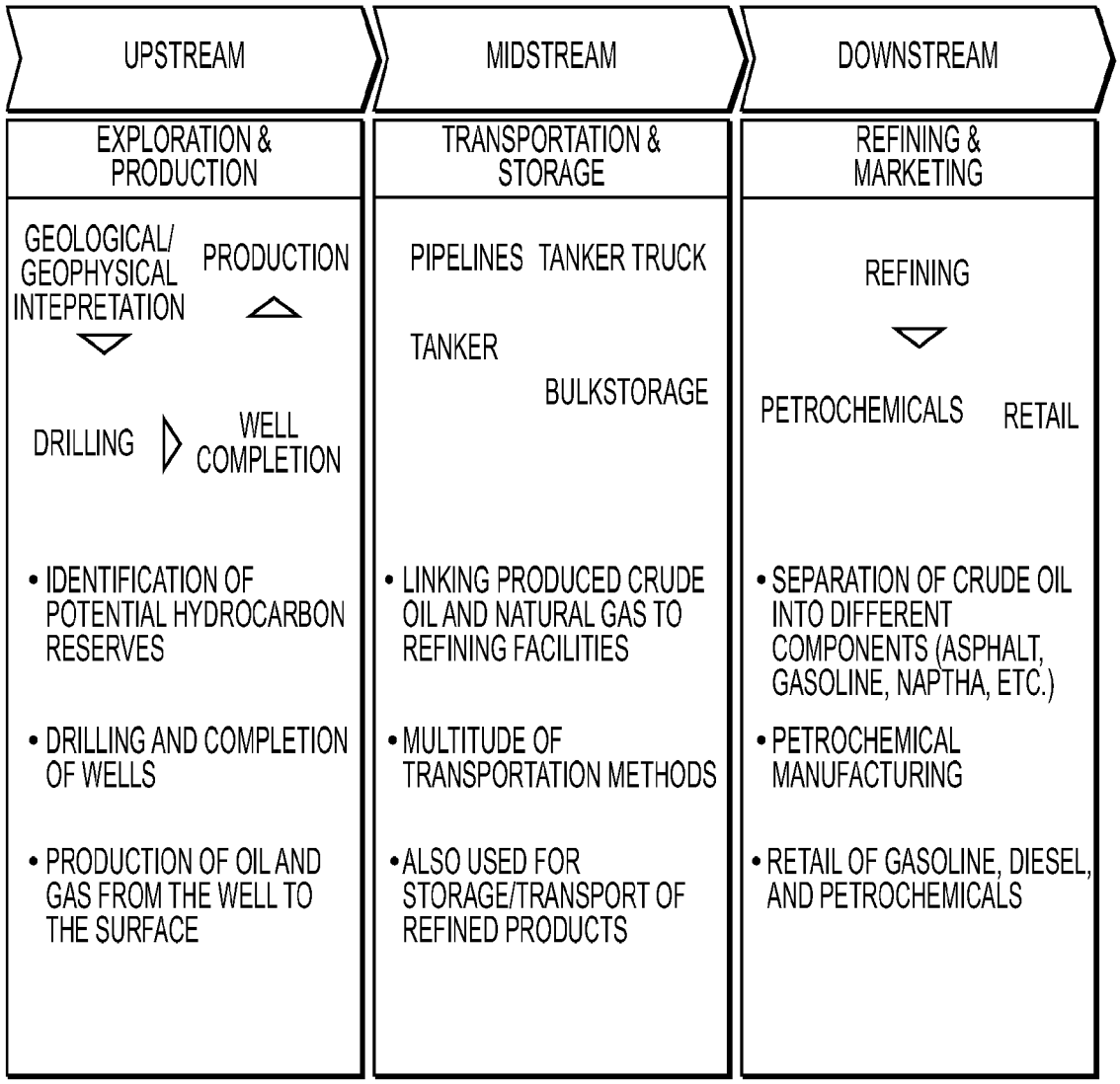

UPSTREAM
MIDSTREAM
DOWNSTREAM
EXPLORATION & PRODUCTION
TRANSPORTATION & STORAGE
REFINING & MARKETING
GEOLOGICAL/ GEOPHYSICAL INTEPRETATION
PRODUCTION
DRILLING
WELL COMPLETION
PIPELINES
TANKER TRUCK
TANKER
BULKSTORAGE
REFINING
PETROCHEMICALS
RETAIL
• IDENTIFICATION OF POTENTIAL HYDROCARBON RESERVES
• DRILLING AND COMPLETION OF WELLS
• PRODUCTION OF OIL AND GAS FROM THE WELL TO THE SURFACE
• LINKING PRODUCED CRUDE OIL AND NATURAL GAS TO REFINING FACILITIES
• MULTITUDE OF TRANSPORTATION METHODS
• ALSO USED FOR STORAGE/TRANSPORT OF REFINED PRODUCTS
• SEPARATION OF CRUDE OIL INTO DIFFERENT COMPONENTS (ASPHALT, GASOLINE, NAPTHA, ETC.)
• PETROCHEMICAL MANUFACTURING
• RETAIL OF GASOLINE, DIESEL, AND PETROCHEMICALS

FIG. 1

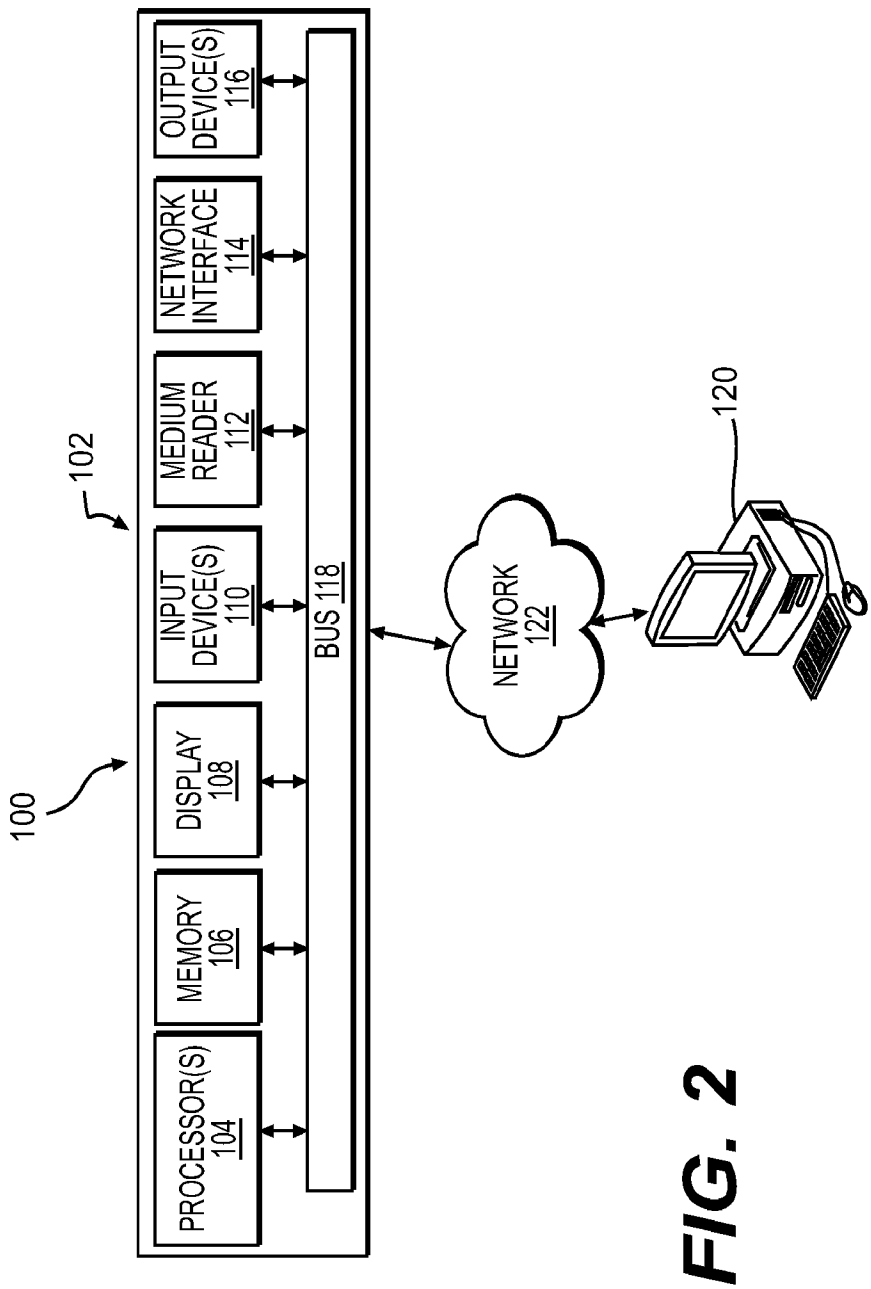

100
102
PROCESSOR(S) 104
MEMORY 106
DISPLAY 108
INPUT DEVICE(S) 110
MEDIUM READER 112
NETWORK INTERFACE 114
OUTPUT DEVICE(S) 116
BUS 118
NETWORK 122
120

FIG. 2

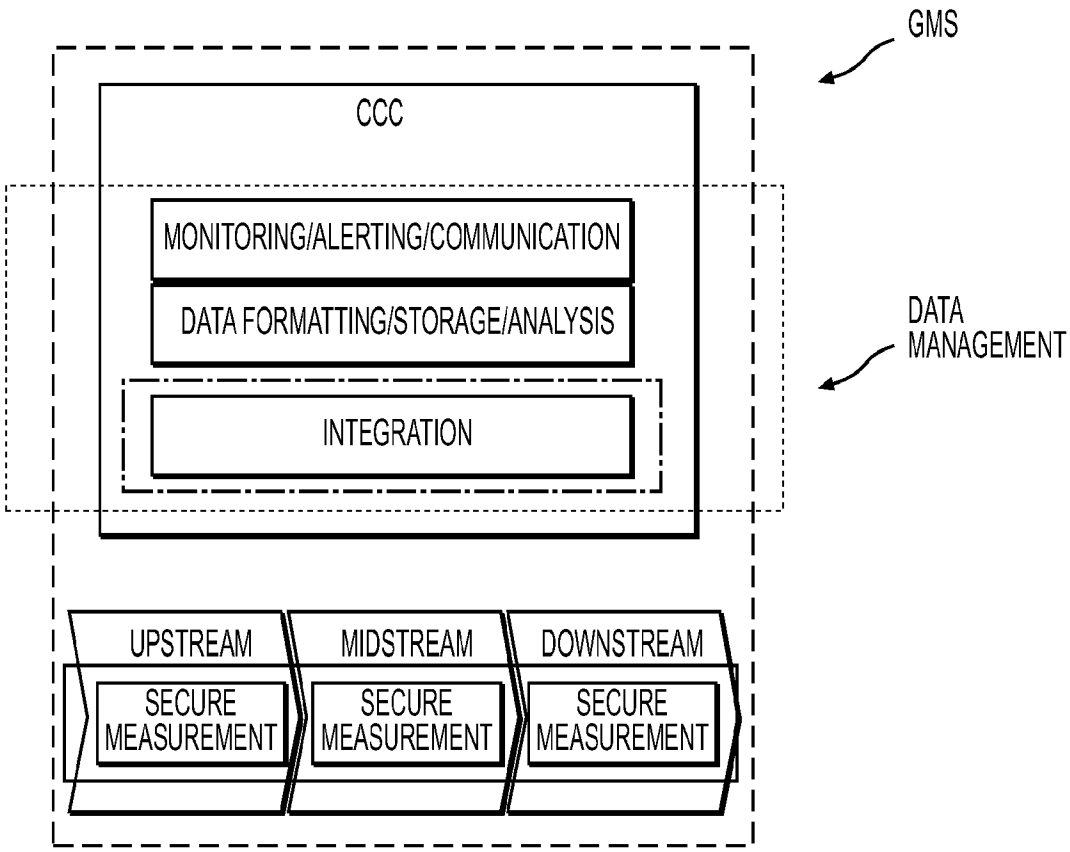

GMS
CCC
MONITORING/ALERTING/COMMUNICATION
DATA FORMATTING/STORAGE/ANALYSIS
INTEGRATION
DATA MANAGEMENT
UPSTREAM
MIDSTREAM
DOWNSTREAM
SECURE MEASUREMENT
SECURE MEASUREMENT
SECURE MEASUREMENT

FIG. 3

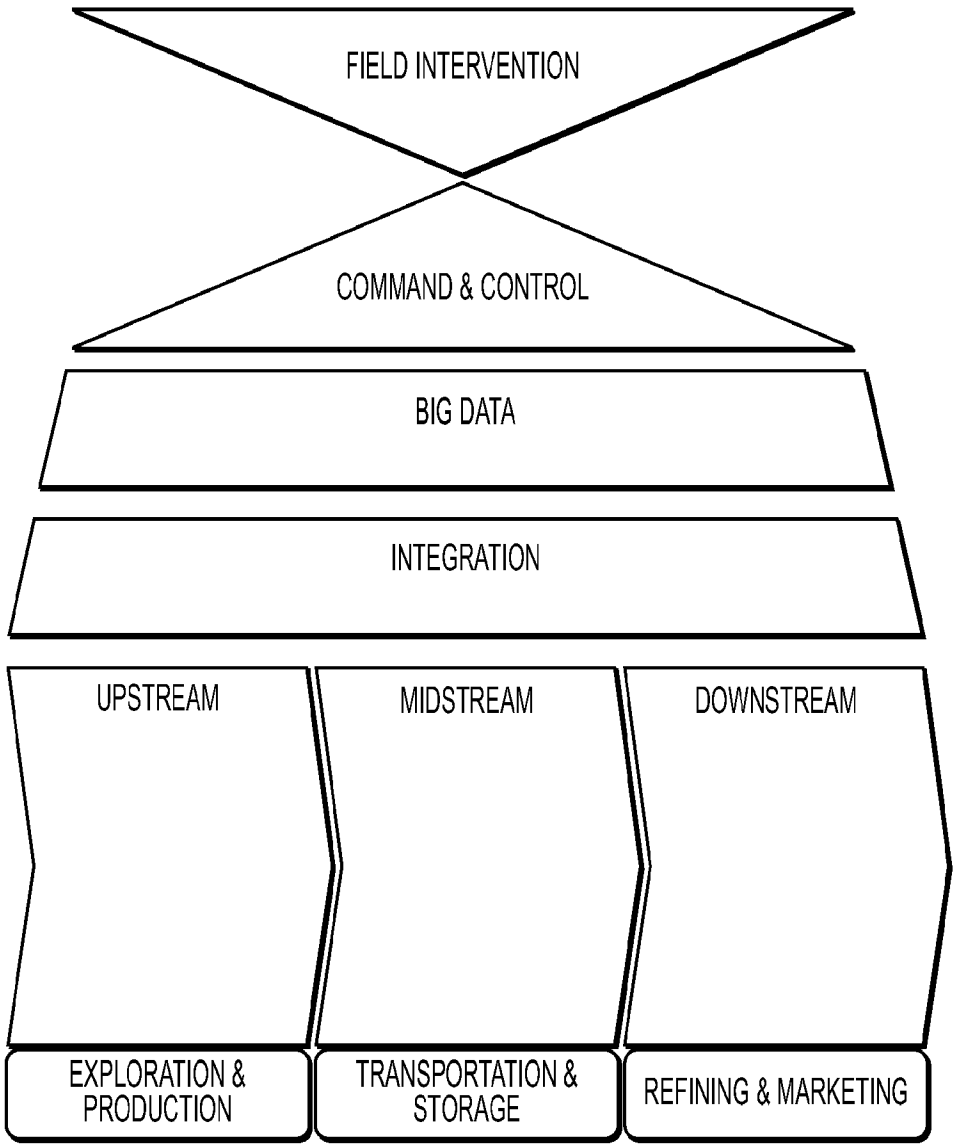

FIELD INTERVENTION
COMMAND & CONTROL
BIG DATA
INTEGRATION
UPSTREAM
MIDSTREAM
DOWNSTREAM
EXPLORATION & PRODUCTION
TRANSPORTATION & STORAGE
REFINING & MARKETING

FIG. 4

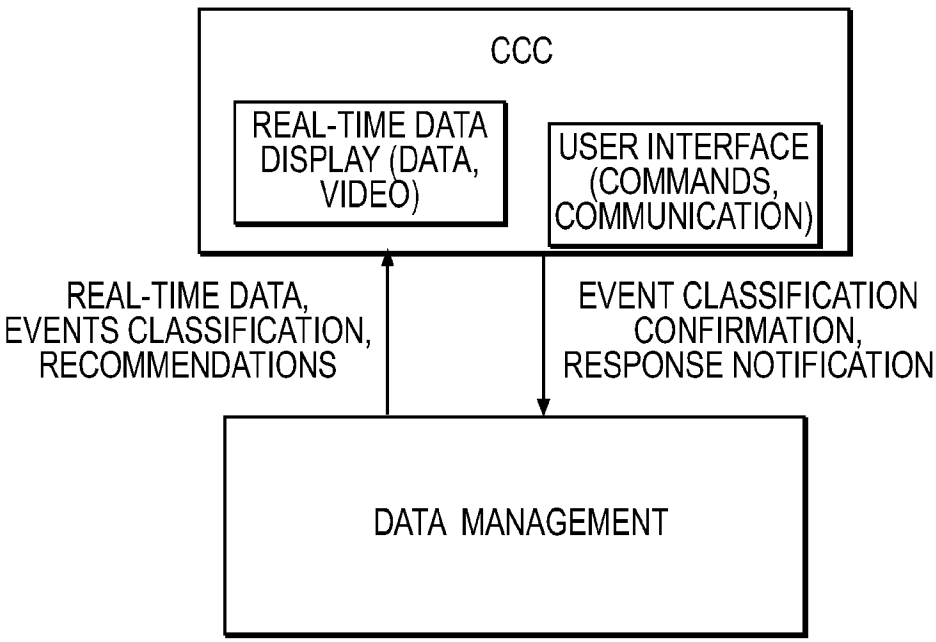

CCC
REAL-TIME DATA DISPLAY (DATA, VIDEO)
USER INTERFACE (COMMANDS, COMMUNICATION)
REAL-TIME DATA, EVENTS CLASSIFICATION, RECOMMENDATIONS
EVENT CLASSIFICATION CONFIRMATION, RESPONSE NOTIFICATION
DATA MANAGEMENT

FIG. 5

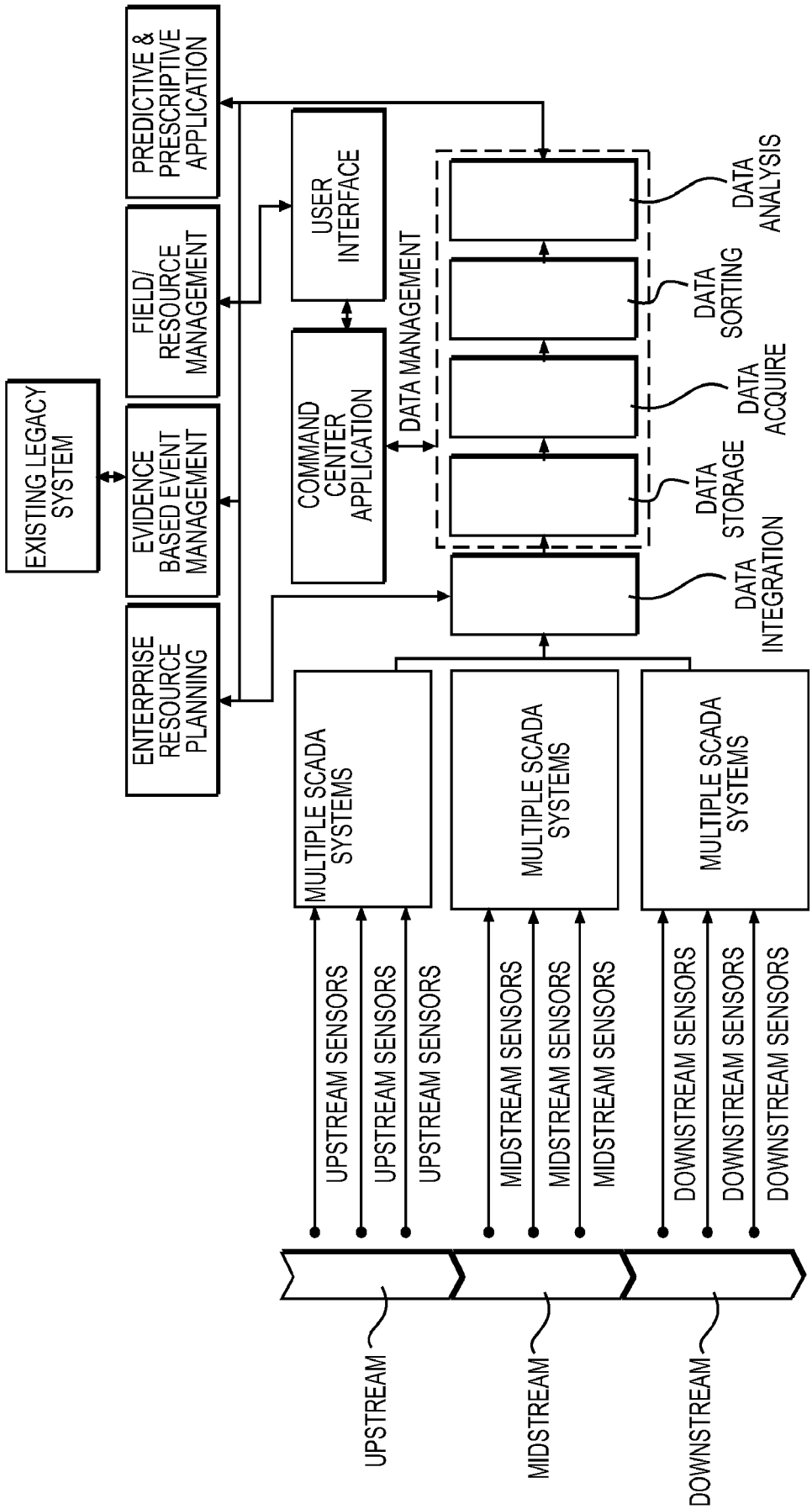

PREDICTIVE & PRESCRIPTIVE APPLICATION
FIELD/ RESOURCE MANAGEMENT
EVIDENCE BASED EVENT MANAGEMENT
ENTERPRISE RESOURCE PLANNING
EXISTING LEGACY SYSTEM
USER INTERFACE
COMMAND CENTER APPLICATION
DATA MANAGEMENT
DATA ANALYSIS
DATA SORTING
DATA ACQUIRE
DATA STORAGE
DATA INTEGRATION
MULTIPLE SCADA SYSTEMS
MULTIPLE SCADA SYSTEMS
MULTIPLE SCADA SYSTEMS
UPSTREAM SENSORS
UPSTREAM SENSORS
UPSTREAM SENSORS
MIDSTREAM SENSORS
MIDSTREAM SENSORS
MIDSTREAM SENSORS
DOWNSTREAM SENSORS
DOWNSTREAM SENSORS
DOWNSTREAM SENSORS
UPSTREAM
MIDSTREAM
DOWNSTREAM

FIG. 6

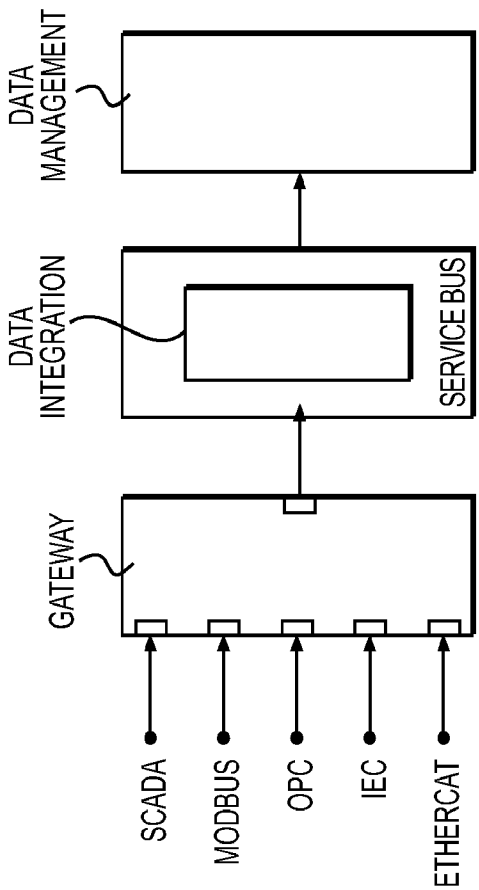

DATA MANAGEMENT
DATA INTEGRATION
SERVICE BUS
GATEWAY
SCADA
MODBUS
OPC
IEC
ETHERCAT

FIG. 7

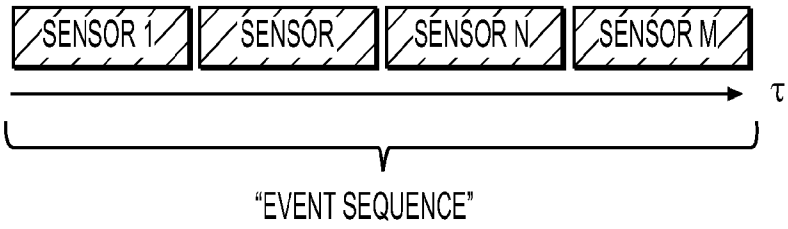


FIG. 8A

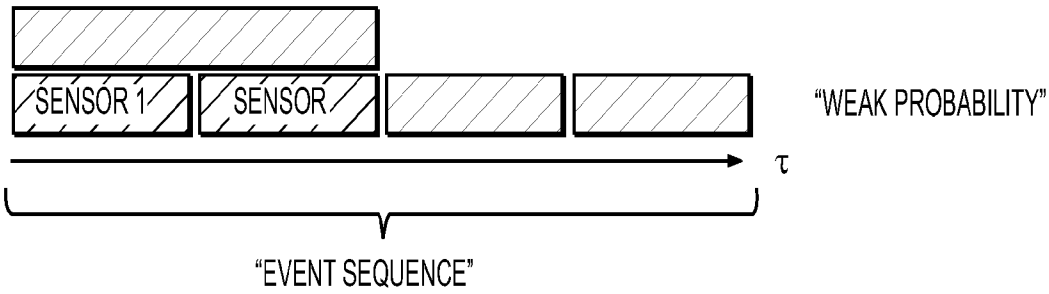


FIG. 8B

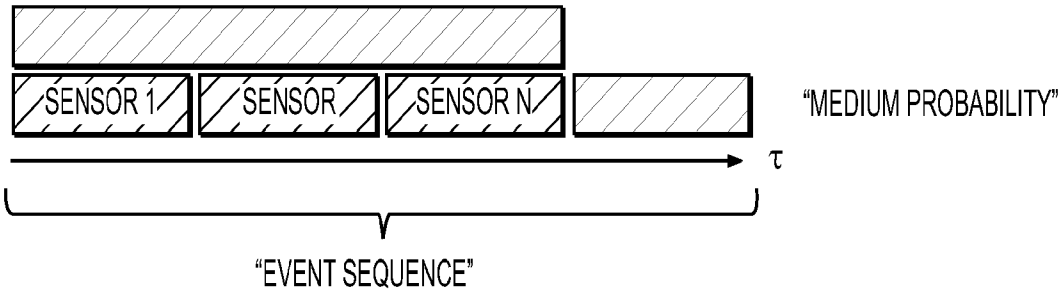


FIG. 8C

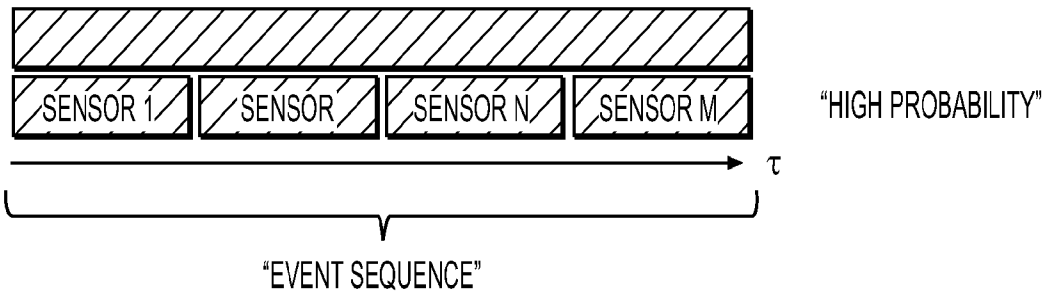


FIG. 8D

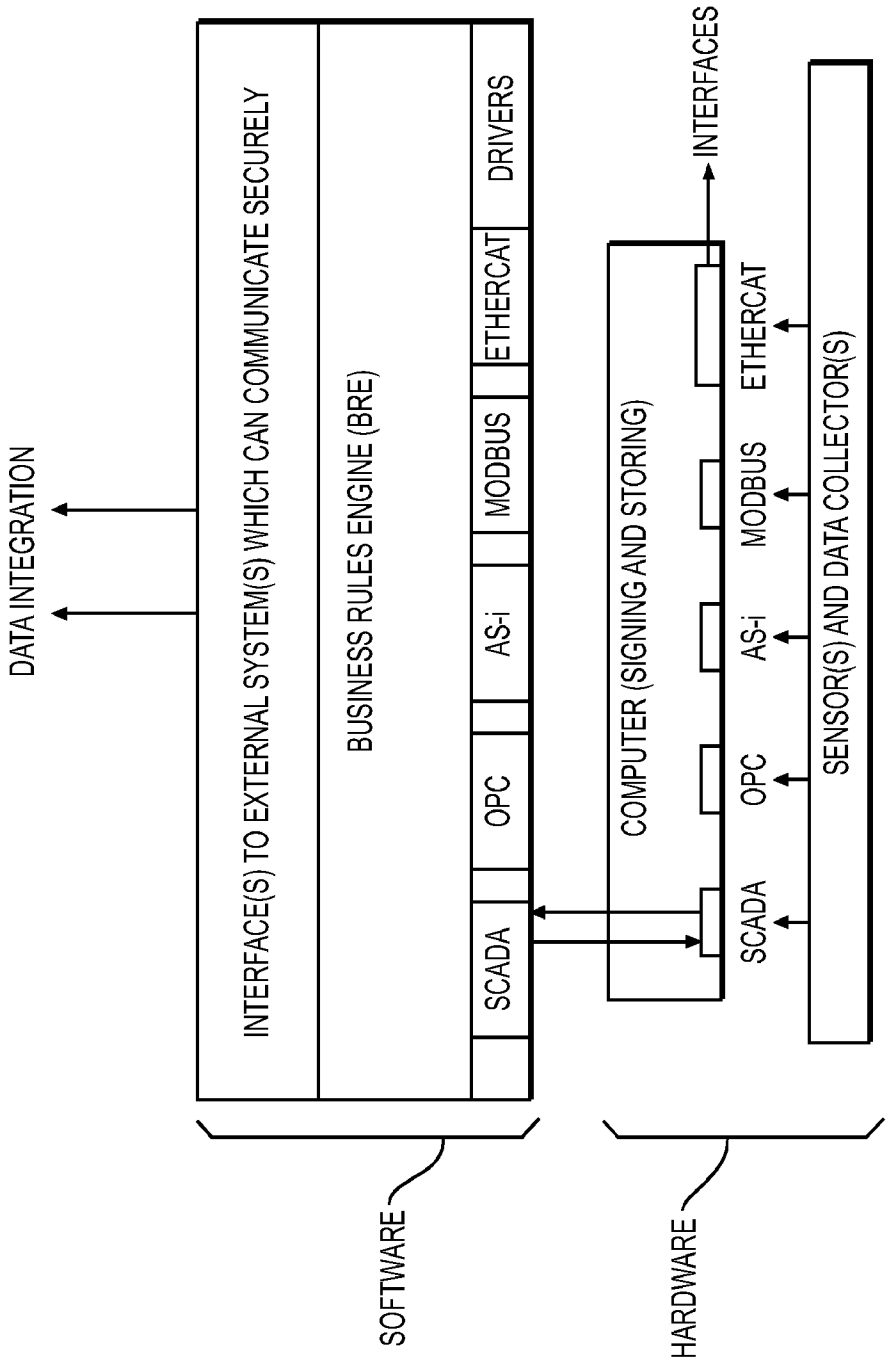

DATA INTEGRATION
INTERFACE(S) TO EXTERNAL SYSTEM(S) WHICH CAN COMMUNICATE SECURELY
BUSINESS RULES ENGINE (BRE)
SCADA
OPC
AS-i
MODBUS
ETHERCAT
DRIVERS
SOFTWARE
COMPUTER (SIGNING AND STORING)
INTERFACES
SCADA
OPC
AS-i
MODBUS
ETHERCAT
SENSOR(S) AND DATA COLLECTOR(S)
HARDWARE

FIG. 9

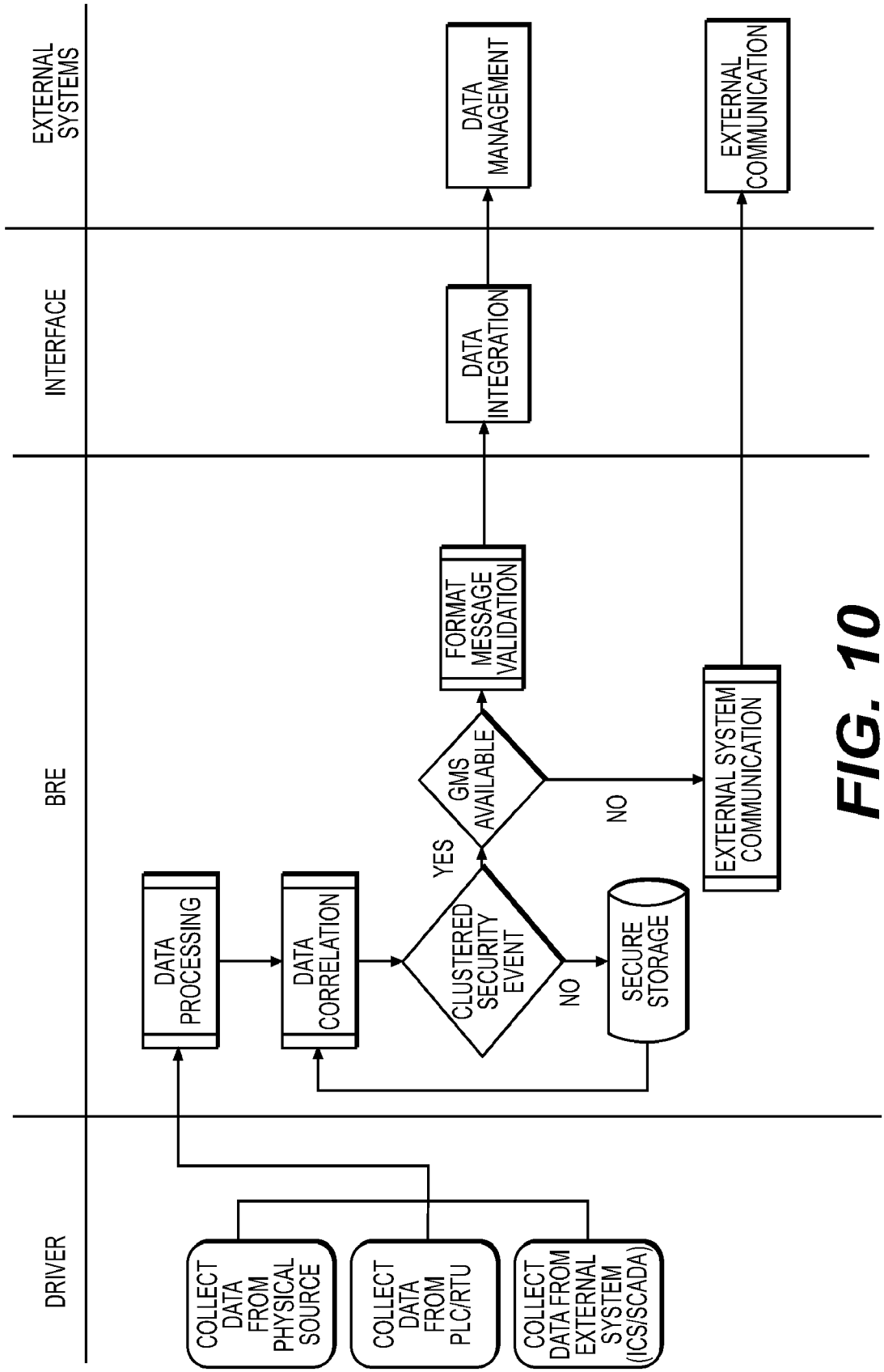

EXTERNAL SYSTEMS
INTERFACE
BRE
DRIVER
DATA MANAGEMENT
EXTERNAL COMMUNICATION
DATA INTEGRATION
FORMAT MESSAGE VALIDATION
GMS AVAILABLE
YES
NO
EXTERNAL SYSTEM COMMUNICATION
DATA PROCESSING
DATA CORRELATION
CLUSTERED SECURITY EVENT
NO
SECURE STORAGE
COLLECT DATA FROM PHYSICAL SOURCE
COLLECT DATA FROM PLC/RTU
COLLECT DATA FROM EXTERNAL SYSTEM (ICS/SCADA)

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/033027

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G01F 15/00 (2014.01)
USPC - 702/55
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) - G01F 15/00; 15/02; 15/04 (2014.01)
USPC -702/33; 702/55; 702/127

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
CPC - G01F 1/00; 15/00; 15/007 (2014.02)

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/0158294 A1 (CLEMENTS) 21 JUNE 2012 (21.06.2012) entire document	1-3,17-19,35-3, 46-49
A	US 4,551,719 (CARLIN et al) 05 NOVEMBER 1985 (05.11.1985) entire document	1-3,17-19,35-38, 46-49

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

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 August 2014	28 AUG 2014
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/033027

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.: 4-16, 20-34, 39-45, 50
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.