

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

(19) World Intellectual Property

Organization

International Bureau

(43) International Publication Date

27 August 2020 (27.08.2020)



(10) International Publication Number

WO 2020/172389 A1

(51) International Patent Classification:

G06F 21/50 (2013.01) H04W 12/00 (2009.01)

G06F 21/88 (2013.01)

(21) International Application Number:

PCT/US2020/019009

(22) International Filing Date:

20 February 2020 (20.02.2020)

Published:

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

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

16/280,687 20 February 2019 (20.02.2019) US

(71) Applicant: SAUDI ARABIAN OIL COMPANY

[SA/SA]; 1 Eastern Avenue, Dhahran, 31311 (SA).

(71) Applicant (for AG only): ARAMCO SERVICES COM-

PANY [US/US]; 1200 Smith Street, Two Allen Building, Houston, Texas 77002 (US).

(72) Inventors: AL-YOUSEF, Hassan S.; WC-1352, Al-Midra

Tower, Dhahran, 31311 (SA). ALKHABBAZ, Fouad M.; Saudi Aramco, P.O. Box 11627, Dhahran, 31311 (SA).

ABU AL SAUD, Zakarya A.; Saudi Aramco, P.O. Box 18807, Dhahran, 31311 (SA). ALMADI, Solomon M.; Saudi Aramco, P.O. Box 10823, Dhahran, 31311 (SA).

(74) Agent: BRUCE, Carl E. et al.; Fish & Richardson P.C.,

P.O. Box 1022, Minneapolis, Minnesota 55440-1022 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every

kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,

(54) Title: EMBEDDED DATA PROTECTION AND FORENSICS FOR PHYSICALLY UNSECURE REMOTE TERMINAL UNIT (RTU)

(57) Abstract: Systems and methods include a method for protecting data for a remote terminal unit (RTU) and providing audit trail information for forensics procedures. Monitoring is performed for conditions detected at an RTU that warrant a data protection operation at the RTU. The monitoring is performed by an instrumented security function (ISF) chip communicating with the RTU in a supervisory control and data acquisition system (SCADA) network. Upon determining that conditions are warranted, the data protection operation is initiated by the ISF chip. The system also provides audit trail information for forensics procedures upon detecting a threat in the vicinity of the RTU. The system invokes the forensics procedure by initiating the localization services (HBL) embedded as part of the RTU's disk apparatus triggered by a change to the disk apparatus such as a power disconnect or by receiving a security signal from the NAC or local occupancy sensors.



WO 2020/172389 A1

EMBEDDED DATA PROTECTION AND FORENSICS FOR PHYSICALLY UNSECURE REMOTE TERMINAL UNIT (RTU)

CLAIM OF PRIORITY

[0001] This application claims priority to U.S. Patent Application No.
5 16/280,687 filed on February 20, 2019, the entire contents of which are hereby
incorporated by reference.

BACKGROUND

[0002] The present disclosure applies to protecting data in supervisory control
and data acquisition system (SCADA) networks and provide audit trail information for
10 forensics procedures. A SCADA includes automation software written specifically to
perform data acquisition requirements for an individual plant. The software can control
commands and data transfer between Master Stations (MS) (including servers and
software responsible for communicating with field equipment), human machine
interfaces (HMIs) workstations, and field devices connected to remote terminal units
15 (RTUs). Field devices can include, for example, pressure transmitters, flow meters, and
temperature sensors. SCADA networks that include RTUs can present challenges
regarding data protection.

SUMMARY

[0003] The present disclosure describes techniques that can be used for
20 providing embedded data protection and forensics for a physically unsecure remote
terminal unit (RTU). In some implementations, methods include a computer-
implemented method for protecting data for a Remote Terminal Unit (RTU) in addition
to providing audit trail information for forensics procedures. Monitoring is performed
for conditions detected at an RTU that warrant a data protection operation and forensics
25 procedures at the RTU. The monitoring is performed by an instrumented security
function (ISF) chip communicating with the RTU in a supervisory control and data
acquisition system (SCADA) network. Upon determining that the conditions detected
at the RTU warrant the data protection operation and the forensics procedures, the data
protection operation and forensics procedures are initiated by the ISF chip.

30 [0004] The present disclosure relates to providing embedded data protection and
forensics capabilities for RTUs in SCADA systems. More particularly, the present

disclosure relates to a system and a method for protecting an RTU's buffering information, configuration data, and associated personnel identification and authentication information. Additionally, a system to facilitate audit trails is also provided for forensics procedures by way of localization services embedded as part of the RTU's disk apparatus. As an example, a chip as described with reference to FIG. 9
5 can be incorporated into an RTU and can provide the embedded data protection and forensics capabilities. Techniques described in the present disclosure can be part of SCADA systems, for example, for upstream oil and gas applications, pipeline applications, and power and utility applications that may not be protected by adequate
10 physical security controls.

[0005] Distributed Control Systems (DCSs) are designed to perform regulatory control algorithms and processes to keep processes within set-points in a specific area, or risk area, of the plant. A DCS can provide supervisory control, including performing event-based monitoring algorithms that perform data-gathering over a large
15 geographical area. Unlike DCSs, SCADAs can provide telemetry-based process control commands initiated from the Central Master Station ("master station"). Commands can be provided either manually by an operator or automatically using an application. Each command can initiate an action or change an analog set point in a remotely-located control station, for example, using an RTU. Commands can be provided over a
20 bidirectional communications link using specific communication protocols. Commands can depend on quality process-related alarm or event data and can follow timely bidirectional confirmation and acknowledgment executing sequences (for example, check before operate (CBO)) between a master and the station.

[0006] Each master station can include multiple servers, distributed software
25 applications, and disaster recovery sites. Master stations can include network switch and connectivity devices that are required to communicate with RTUs and remote sites. Communications can use bidirectional information transfer (in both directions) between master stations and remote terminals within a communication channel. As part of SCADA operations, commands can be sent by operators or by applications in binary or
30 analog formats. The commands can be sent from a human machine interface (HMI) station to field instruments connected to a particular RTU to provide a status reading or to perform a certain action remotely. The command originating from the HMI station can typically be delivered to its target as quickly as possible, such as within seconds or

sub-seconds. If a command cannot be delivered or acted upon, the SCADA system can report that failure to the operator.

[0007] Master stations, HMIs, and remote terminal units (RTUs) can use a communication medium that facilitates signaling between these terminals, such as by using a path between a master station, HMIs, RTUs, and programmable logic controllers (PLCs). The communication medium can be part of an overall communications subsystem that performs the transmitting and receiving of digital information for the entire SCADA. The communication medium can use media such as fiber optics, copper cabling, wireless, and very small aperture terminal (VSAT) communications.

[0008] In some instances, the remote RTU can be configured with a system buffer capable of storing field information for a configurable period of time (for example, seven days) in the course of transmission from one point to another. The buffer can be used to compensate for a difference in the flow of data, or a time of occurrence of events, when transmitting data from one device to another. If a flow of data is compromised, the data may be used maliciously to determine a type of the facility (for example, an oil, gas, or water well). Additionally, the compromised data may be used to generate trends or patterns, which can expose intelligent and sensitive information as to a well's ascending or descending production capacity. Further, the frequency between data transmissions can indicate an "importance" of the facility to an organization.

[0009] Another important type data to protect at an RTU location is the RTU's own configuration file. If compromised, the configuration parameters specified in the configuration file can be used to set up (or spoof) a rogue RTU that can simulate inputs from the field so as to act as a real RTU. The RTU's configuration file may typically be stored in an unprotected part of the RTU's controller board, easily accessible by any hand-held computer.

[0010] Another important type of data to protect at the RTU location is the data pertaining to the physical occupancy and authentication processes. The data can include inputs from motion detection, radio frequency identification (RFID), and personal identification number (PIN) input devices that capture personnel movements and personal identification information within a vicinity of the RTU. A remote data protection function that combines these types of data protection can be imperative for assuring field data integrity and availability.

[0011] The system is also capable of providing audit trail information for

forensics procedures once a threat is detected in the vicinity of the RTU. The system invokes the forensics procedure by initiating the localization services embedded as part of the RTU's disk apparatus upon the detection of any change to the disk apparatus such as a power disconnect or by receiving a security signal from the NAC or local occupancy
5 sensors.

[0012] The previously described implementation is implementable using a computer-implemented method; a non-transitory, computer-readable medium storing computer-readable instructions to perform the computer-implemented method; and a computer-implemented system including a computer memory interoperably coupled
10 with a hardware processor configured to perform the computer-implemented method/the instructions stored on the non-transitory, computer-readable medium.

[0013] The subject matter described in this specification can be implemented in particular implementations, so as to realize one or more of the following advantages. First, techniques can be used to secure SCADA network access to a remote RTU in a
15 physically unprotected location, providing embedded RTU data protection and forensics capability. Second, the techniques can help to assure the security and integrity of the SCADA network, including data stored at the RTU in a physically unprotected location. Third, the techniques can be used to provide audit trails and evidence information for forensic procedures.

[0014] The details of one or more implementations of the subject matter of this specification are set forth in the Detailed Description, the accompanying drawings, and the claims. Other features, aspects, and advantages of the subject matter will become
20 apparent from the Detailed Description, the claims, and the accompanying drawings.

DESCRIPTION OF DRAWINGS

[0015] FIG. 1 is a block diagram showing an example of a replication process, according to some implementations of the present disclosure.

[0016] FIG. 2 is a block diagram showing an example of dynamic backup and restore process information, according to some implementations of the present disclosure.

[0017] FIG. 3 is a block diagram showing an example of an enabling process, according to some implementations of the present disclosure.
30

[0018] FIG. 4 is a block diagram of an example of a network security architecture, according to some implementations of the present disclosure.

[0019] FIG. 5 is a block diagram showing an example of a centralized implementation that includes a central instrumented security function (ISF) and an intelligent disk apparatus, according to some implementations of the present disclosure.

[0020] FIG. 6 is a block diagram showing an example of an implementation using alternating Simple Network Management Protocol (SNMP) strings, according to some implementations of the present disclosure.

[0021] FIG. 7 is a block diagram of an example of a network security architecture using RTU-to-RTU (remote terminal unit) data replication services, according to some implementations of the present disclosure.

[0022] FIG. 8 is a block diagram of an example of a network security architecture including RTU-to-SCADA (supervisory control and data acquisition) network data replication services, according to some implementations of the present disclosure.

[0023] FIG. 9 is a diagram of an example of a custom hard disk apparatus in communication with the RTU motherboard and the central SCADA network, according to some implementations of the present disclosure.

[0024] FIG. 10 is a flow diagram showing an example of a logic flow for an instrumented security function (ISF) chip, according to some implementations of the present disclosure.

[0025] FIG. 11 is a block diagram depicting examples of disk cluster assignments and file allocation table features for facilitating a rapid erase of information in case of an RTU or disk compromise, according to some implementations of the present disclosure.

[0026] FIG. 12 is a flowchart of an example method for initiating data protection operations and forensics procedures, when conditions monitored at the RTU are detected that warrant the data protection operation and the forensics procedures, according to some implementations of the present disclosure.

[0027] FIG. 13 is a block diagram illustrating an example computer system used to provide computational functionalities associated with described algorithms, methods, functions, processes, flows, and procedures as described in the present disclosure, according to some implementations of the present disclosure.

[0028] Like reference numbers and designations in the various drawings indicate like elements.

DETAILED DESCRIPTION

[0029] The following detailed description describes techniques for providing embedded data protection and forensics for a physically unsecure remote terminal unit (RTU). Various modifications, alterations, and permutations of the disclosed implementations can be made and will be readily apparent to those of ordinary skill in the art, and the general principles defined may be applied to other implementations and applications, without departing from scope of the disclosure. In some instances, details unnecessary to obtain an understanding of the described subject matter may be omitted so as to not obscure one or more described implementations with unnecessary detail and in as much as such details are within the skill of one of ordinary skill in the art. The present disclosure is not intended to be limited to the described or illustrated implementations, but to be accorded the widest scope consistent with the described principles and features.

[0030] The techniques described in the present disclosure can be used to provide embedded RTU data protection and forensics capability within a Supervisory Control and Data Acquisition (SCADA) network. For example, a system that provides integrated security as part of an RTU in the SCADA network can include Internet protocol (IP) video servers and recorders, motion detectors, occupancy sensors, radio frequency identification (RFID) and personal identification number (PIN) identification, a network access controller (NAC), and a network management system (NMS). The system can support the receipt and use of security parameters that are input from the field. The motion detection and occupancy sensing instrumentation can be connected to the RTU in addition to the IP video camera with infra-red (IR) night vision capabilities, RFID identification, and PIN identification.

[0031] In some implementations, a system can provide remote RTU data protection and forensics capabilities and automated configuration assignment processes. The system can include a custom hard disk apparatus in communication with a central SCADA network and an RTU motherboard (for example, for power and data). The custom hard disk apparatus can include a memory, a processor, a relay, an uninterruptable power supply (UPS), a homing beacon, and a global positioning system

(GPS) receiver coupled to an instrumented security function (ISF). The ISF can be implemented, for example, as an ISF chip onboard (and executable by) the RTU. The ISF chip can communicate with multiple inputs from within the RTU and from the SCADA network. The ISF chip can also communicate concurrently with at least one data storage within the custom hard disk apparatus and an off-RTU location. For example, the off-RTU location can be on another RTU or in a central location on the SCADA network. The ISF chip can evaluate inputs received from the NAC apparatus. When the NAC apparatus detects suspicious events, the ISF can trigger a self-destruct routine to erase critical data in RTU storage. Additionally, a homing beacon and localization services can be initiated by the ISF upon detection of negative authentication or a power interruption (for example, detected by the UPS). The system invokes the forensics procedure by initiating the localization services (homing beacon) embedded as part of the RTU's disk apparatus upon the detection of any change to the disk apparatus such as a power disconnect or by receiving a security signal from the NAC or local occupancy sensors. The homing beacon and localization parameters (position coordinates) are transmitted wirelessly to a Fly-By unmanned aerial vehicle (UAV), Global System for Mobile (GSM) network, or standard wireless backhaul connection.

Data Protection and Forensics

[0032] To ensure full restoration of the RTU data after an erase procedure, the data at the RTU can be periodically replicated locally onto an encrypted data storage or onto an encrypted data storage in another RTU in the field. The replication and restore procedure can include the RTU node communication configuration such as a transmission control protocol/Internet protocol (TCP/IP) address stored on erasable programmable read-only memory (EPROM), as once this is lost or damaged, the communication capability with the rest of the network is lost.

[0033] In another implementation, a "Restore" process can be used to restore all information back to a wiped disk but not to a wiped EPROM. An RTU with a damaged or wiped EPROM can require either a manual configuration using recommend standard (RS)-232 serial communication connected by laptop or by devising a new automatic method. Though the backup process covers the RTU configuration file which contains the RTU name and address fields, the configuration file in the description resides on the

disk rather than on the EPROM but copies other RTU parameters residing elsewhere, such as the EPROM.

[0034] In another implementation, the replication process can be performed using a full disk encryption feature (for example, Bitlocker). Replication can serve the purpose of preserving the data, for example, for disaster recovery procedures.

[0035] FIG. 1 is a block diagram showing an example of a replication process 100, according to some implementations of the present disclosure. For example, FIG. 1 shows interactions between triggers, the ISF, and a SCADA Master Station in activating Backup and Restore processes. In some implementations, the replication process 100 (including Backup and Restore functions) is based on two-dimensional triggers, including triggers 102 initiating an ISF 104 and triggers 106 initiating a SCADA Master Station (MS) 108. The triggers 102 can include, for example, RFID events 102a, log events 102b, and NAC events 102c. The triggers 106 can include, for example, routine backup cycle events 106a, testing events 106b, and RTU maintenance events 106c.

[0036] The ISF 104 can serve as the ultimate controller for the replication process 100, including being the primary host of a synchronized Dynamic Backup & Restore Process Index (DBRPI) 110. The DBRPI 110 can use (or can include) a simple information array that maps RTU names and addresses to the Backup/Restore job information (for example, identifying scope, cycle and priority). The two-dimensional triggers can serve as inputs 112 to a decision support function 114 that includes a backup and restoration engine 116. The decision support function 114 can produce outputs 118.

[0037] FIG. 2 is a block diagram showing an example of dynamic backup and restore process information 200, according to some implementations of the present disclosure. The restore process information 200 can be implemented by the DBRPI 110, for example. The DBRPI 110 can be a table that includes fixed length fields. The fields can include, for example, an RTU name 202 consisting of ten alphanumeric characters, such as indicated by examples listed in RTU names 204. In addition, the DBRPI 110 can contain the following fields. An RTU physical address 206 (for example a nine-bit field) can have values as indicated by examples listed in RTU physical addresses 208. A scope entry 210 (for example, five decimal digits) can have values as indicated in example scopes 212. An “Auto” entry 214 (for example, one bit long) can be either ON or OFF, as indicated in example auto bits 216. A “Priority” indicator 218 (for example,

five decimal digits) can have values as indicated in example priorities 220. A “Cycle” 222 (for example, two bits) can have values as indicated in example cycles 224.

[0038] In some instances, the ISF receives input from the Network Access Control (NAC) which might indicate a pending security requirement to perform a data replication process. Similarly, a trigger can be initiated from the SCADA Master Station (MS) indicating a system availability requirement in order to perform the data replication service.

[0039] In some implementations, the data replication triggers can be channeled through a soft switch at the operator’s HMI station to enable an operator’s intervention. The soft switch can be beneficial in events where triggers may be forced to engage or disengage (for example, used in troubleshooting).

[0040] In some implementations, the data replication employs three records of information: an RTU node configuration, RTU security information, and archived field instruments acquisition data. Each of the three fields can have its own run cycle and execution priority. In some instances, a SCADA administrator may elect to assign a higher priority to RTU configuration (for example, in remote sites where deploying a new RTU is cumbersome, but replacing a faulty hard drive is easier). In other cases, the RTU security information may be of higher importance (for example, in cases in which RTUs are installed in very unsecure areas).

[0041] In some implementations, the replication process can be conducted onto a locally attached media that is supported within the chassis of the RTU itself and is connected simultaneously to RTU power and a network. In some implementations, the management of the replication process can be centrally managed by the NAC apparatus or by each RTU as part of a distributed management process. In some implementations, the RTU’s data can be periodically replicated onto an array of encrypted data storage allocated on the SCADA network. Examples of architectures that can support different implementations of replication are provided in FIGS. 4, 7 and 8.

[0042] In some implementations, a custom hard disk apparatus can include a custom Rapid Erase File System (REFS) that can be used to quickly erase information. This can be accomplished by having different types of information ranked by priorities that correspond to criticality levels of different types of information. The priorities can then be used to determine an order of erasure. For example, the RTU’s configuration data can be ranked with a top priority, indicating a greatest criticality, causing the

critically ranked data to be erased before lower priority data. An example of a custom hard disk apparatus that can house the REFS and can be used to quickly erase information is provided with reference to FIG. 4.

[0043] In some implementations, as power is cut off from an RTU, the ISF can enter into a race against time and power reserves to complete the mission of erasing data before the data is compromised. In order to provide mechanisms that support the mission, the REFS embodies a custom file system can be used for storing critical information in “adjacent” clusters so that the entire file can be destroyed at the hardware level.

[0044] In some implementations, the custom REFS file system can include intelligence for storing logical block addressing (LBA) of critical files, such as configuration files, encryption keys, authorization and authentication signals from RFID, motions detection, and personal identification number (PIN) apparatuses. For example, the configuration file can be “tagged” by the ISF to be stored in a particular cylinder, head, and track number that corresponds to a particular LBA of files. The REFS can assign a priority (for example, based on file criticality) that can be used to sequence the file deletion process. An example of LBA addressing for critical files within a disk layout is provided in FIG. 11.

[0045] FIG. 3 is a block diagram showing an example of an enabling process 300, according to some implementations of the present disclosure. In some implementations, the ISF, data replication, and forensics processes can be triggered by a manual dip switches arrangement 302 on the RTU. A dip switch apparatus that includes the manual dip switches arrangement 102 can be in communication with the ISF. The dip switch apparatus can contain three bays, with Bay 1 controlling the ISF, Bay 2 controlling data replication, and Bay 3 controlling forensics. For example, an ISF function enabler 304 using top two switches 302a of the manual dip switches arrangement 302 can control on-off settings for Bay 1, as summarized in table 306. A data replication enabler 308 using middle two switches 302b of the manual dip switches arrangement 302 can control on-off settings for Bay 2, as summarized in table 310. A forensics enabler 312 using bottom two switches 302c of the manual dip switches arrangement 302 can control on-off settings for Bay 3, as summarized in table 314. In some implementations, the dipswitch apparatus can be used in testing and simulation

scenarios and in situations where communication with NAC apparatus is not stable or is intermittent.

[0046] In some implementations, the REFS can store the critical information in a particular location, such as within center tracks of the RTU disk. Storage of the critical information in the particular location can help to minimize the time taken for the head movement to erase targeted data, thus preserving the auxiliary battery. The time can be minimized for center tracks because, on average, the disk read/write head has a higher probability of being closer to the center of the disk.

On-Demand RTU and Data Movement Tracking

[0047] In some implementations, the RTU can communicate with a homing beacon and localization (HBL) services apparatus. The HBL can be managed by the ISF chip using multi-parameter inputs from other instruments. The inputs can include, for example, an electrical relay that senses power feed supply continuation, identification of the UPS which invokes the data storage battery to power the disk apparatus, and other signals received from the NAC apparatus. Upon detection of a power supply disconnection coupled with movement of the RTU or data storage, the HBL can initiate a tracking process by broadcasting a homing beacon according to a time interval. The homing beacon can be a three-fielded signal containing, for example, a device identifier (ID), device GPS coordinates, and a timestamp. The fields can be acquired wirelessly, for example, using a fly-by drone or unmanned aerial vehicle (UAV). Before an HBL process is started, a self-destruct signal can be received from the NAC apparatus and processed accordingly.

[0048] In some implementations, a self-destruct process can be targeted for the entire data structure or can be directed to specific data portions that include, for example, RTU configuration data or accumulated authorization and authentication data (for example, associated with PIN, RFID, IP cameras, and occupancy-sensing devices). Self-destruct procedures can use sanitization software that targets data deletion at the block level, including deleting the mapping table and erasing all blocks that have been written to.

[0049] In some implementations, the RTU configuration and other information can be restored from local or remote encrypted storage. Upon normalization of events at the RTU premises, the NAC can initiate a data restoration process, including passing

a decryption key to the ISF chip and sending a restoration completion notification to an HMI workstation.

[0050] In some implementations, a camera or a fingerprint scanner can be embedded as part of the RTU box. The camera and/or fingerprint scanner can be activated upon a detected movement and can capture facial images and fingerprints for biometric identification and forensic investigation. Additionally, the ISF chip can use a program that is activated, for example, when the RTU is connected to a computer hacker's computing device or to the network. The program can then establish a communication with the RTU owner's backbone system and can provide images, fingerprints and event tracking of what is being processed in the RTU.

[0051] FIG. 4 is a block diagram of an example of a network security architecture 400, according to some implementations of the present disclosure. For example, the network security architecture 400 can be used to periodically replicate data at an RTU onto an encrypted data storage system. Features of the network security architecture 400 that may be provided by some conventional systems are contained in dashed lines 402. Features of the network security architecture 400 that are not provided by conventional systems are contained in RTU data replication services that are included in techniques described in the present disclosure.

[0052] A SCADA network 404 connects a remote RTU 406, field instruments 408, a NAC 410, and an RTU remote site 412. The NAC 410 can receive authentication signals 414 from the RTU remote site 412. Positive authentication 416 can be performed, resulting in either enabling network access 418 or disabling network access 420. A network uplink 422 can serve as the RTU's network uplink to a SCADA network. In some implementations, conventional systems can provide the elements 404-422.

[0053] The network security architecture 400 further includes a forensics on-demand tracker 424 (for example, implemented using an unmanned aerial vehicle (UAV)) that can perform tracking using transmissions from a homing beacon 426 coupled with a mobile battery 428 and a GPS transceiver 430. A hard disk 432 can store data, including the RTU's configuration data. An issue self-destruct command 434 can erase information on the hard disk 432. Replication of data can occur using encrypted storage 436 for storing encrypted data. Decryption of the encrypted data can occur using

a passed decryption key 438. Replication can be part of a data replication/restoration process 440.

[0054] In some implementations, the custom disk apparatus can be implemented centrally for the entire SCADA network, eliminating the need to install an individual intelligent disk apparatus for each RTU in the field. This can be particularly prudent in the presence of a reliable infrastructure, such as dark fiber optics or on top of Wave Division Multiplexing or Time Division Multiplexing transmission systems. The central disk apparatus can be composed of the same components as the de-centralized version but can be missing the homing beacon, the GPS receiver, or the wireless transmitter, as those components are installed on the field RTU to provide HBL services.

[0055] In some implementations, the central disk apparatus can provide centralization of two functions: 1) the RTU disk storage area, which is used to store RTU configuration, security information, forensics, and field acquisition data; and 2) the central disk apparatus, which centralizes power utilization curves for individual RTUs and the REFS files system rapid erase capabilities. In this scenario, the central disk apparatus can utilize virtual links on the SCADA remote site connectivity network to communicate with a virtual implementation of the disk apparatus in the field RTU. The virtual links can be used to constantly check for security information from either the NAC or local motion detectors. The virtual links can also be used to constantly check for main power interruptions as recorded by the central disk apparatus. As is the case for actions of the de-centralized disk apparatus, the centralized disk apparatus can trigger Rapid File Erase procedures and engage HBL services once cybersecurity threats are detected. A difference is that, for the centralized disk apparatus, the information destruction occurs on a specific area of the RTU's central disk apparatus.

[0056] FIG. 5 is a block diagram showing an example of a centralized implementation 500 that includes a central ISF 502 and an intelligent disk apparatus 504, according to some implementations of the present disclosure. The intelligent disk apparatus 504 can be implemented, for example, within field RTUs 506 with a virtual disk apparatus. The central ISF 502 can communicate with a SCADA master station 508. Engineering stations 510 can serve as the front end to the SCADA master station 508.

[0057] In some implementations, the centralized disk apparatus can communicate with the multiple field RTUs 506 using virtual routes on top of a TCP/IP

standard communication stack. While Simple Network Management Protocol (SNMP) version 3 or, for example, Modbus/IP can be used for SCADA telemetry communication, the centralized disk apparatus can use a common and standard Poll/Push IP-based management communication protocol such as SNMP. Using SNMP, the centralized disk apparatus can “Push” commands to the virtual disk apparatus to request, for example, uptime status, power supply fluctuations curves, or abnormal activities within the RTU’s vicinity.

[0058] FIG. 6 is a block diagram showing an example of an implementation using alternating SNMP strings, according to some implementations of the present disclosure. In some implementations, using the implementation 600 for example, a centralized disk apparatus 602 can “Poll” (603) configuration, security, and field acquisition data and information from multiple field RTUs 604 on demand, as requested by the ISF function data analysis or SCADA NAC input. To optimize the security configuration of the SNMP stack on the remote RTU, public community strings 606 and private community strings 608 can be dynamically manipulated by the ISF so that a rogue RTU will never be accepted by the central disk apparatus, as one of both community strings will always be out of synchronization. As part of its function, the ISF can employ an SNMP string manipulation subroutine 610 to dynamically alternate both the public community strings 606 and private community strings 608 required for SNMP communication as per a configurable cycle and algorithm. Once the community strings on both the field RTU 604 and on the central disk apparatus 602 match, a broader communication channel can be used to exchange information between the node and the central controller. Otherwise, a recurrent mismatch can indicate foul play or a rogue (for example, fake) device being inserted into the SCADA network. A synch clock 612 can be used to keep the centralized disk apparatus 602 and the field RTUs 604 in synch.

[0059] FIG. 7 is a block diagram of an example of a network security architecture 700 using RTU-to-RTU data replication services, according to some implementations of the present disclosure. For example, the network security architecture 700 can be used to periodically replicate data at an RTU onto an encrypted data storage in another RTU in the field. The network security architecture 700 is similar to the network security architecture 400 except for the addition of a secondary RTU 702. Features of the network security architecture 700 that may be provided by some conventional systems are contained in dashed lines 402. Features of the network

security architecture 700 that are not provided by conventional systems include RTU-to-RTU data replication services. Replication and restoration procedures that are included in the data replication/restoration process 440 include replication to (and recovery from) the secondary RTU 702.

5 [0060] FIG. 8 is a block diagram of an example of a network security architecture 800 including RTU-to-SCADA network data replication services, according to some implementations of the present disclosure. For example, the network security architecture 800 can be used to periodically replicate data at an RTU onto an array of encrypted data storage allocated on the SCADA network. The network security
10 architecture 800 is similar to the network security architecture 400 except for the addition of a SCADA RTU configuration array 802. Features of the network security architecture 800 that may be provided by some conventional systems are contained in dashed lines 402. Features of the network security architecture 800 that are not provided by conventional systems include RTU-to-SCADA network data replication services.
15 Replication and restoration procedures that are included in the data replication/restoration process 440 include replication to (and recovery from) the SCADA RTU configuration array 802. An RTU configuration server 804 (attached to the SCADA network 404) can be used to complete the data replication/restoration process 440.

20 [0061] FIG. 4 is a diagram of an example of a custom hard disk apparatus 400 in communication with the RTU motherboard (for example, for power and data) and the central SCADA network, according to some implementations of the present disclosure. The custom hard disk apparatus 400 includes a memory 402, a processor 404 (for example, a central processing unit (CPU)), a relay 406, a UPS 408, a homing beacon
25 410, and a GPS receiver 412 coupled to an instrumented security function (ISF) chip 414 executable by an onboard chip. The custom hard disk apparatus 400 further includes a power source (for example, batteries 416), a charger 418 for receiving RTU power 420 (to charge the batteries 416), and an internal power feed circuit 422. The custom hard disk apparatus 400 includes an external serial advanced technology attachment (eSATA)
30 port 424 that can be attached to the RTU motherboard. Input 426 from the NAC (received through the SCADA network) can include a positive authentication 428 and a negative authentication 430.

[0062] FIG. 10 is a flow diagram showing an example of a logic flow 1000 for the ISF chip, according to some implementations of the present disclosure. In some implementations, the ISF chip (or software that implements ISF chip functionality) can be part of the RTU or can be added to the NAC apparatus.

5 [0063] At 1002, hard disk drive (HDD) power supply indicators are read. At 1004, normality verification occurs using inputs from occupancy sensors and an RFID 1006. At 1008, cycling continues in the logic flow 1000, where the cycling continues until normality verification indicates a non-normal state. At 1010, when normality verification indicates a non-normal state, normality is then verified with the NAC. If
10 normality is detected by the NAC, then cycling (508) continues in the logic flow 1000.

[0064] If normality verification at 1010 indicates a non-normal state, then security control and management procedures are initiated at 1012. At 1014, a data self-destruct is initiated, for example, to erase RTU data. At 1016, the emergency power supply is engaged, for example, if the ISF chip 914 determines that the primary power
15 supply has been interrupted (or is intermittent). At 1018, HBL services are activated to activate the homing beacon (for example, the homing beacon 126 or the homing beacon 910).

[0065] FIG. 11 is a block diagram depicting examples of a system 1100 including disk cluster assignments 1102 and file allocation table features 1104 for
20 facilitating a rapid erase of information in case of an RTU or disk compromise, according to some implementations of the present disclosure. The disk cluster assignments 1102 can define locations on a disk 1106 for particular files. For example, adjacent clusters 1108 having a starting address 1110 and an ending address 1112 can be reserved for RTU configuration files 1114.

25 [0066] Each cluster can have a size 1116 (for example, 2048 bytes) and can be equivalent to a number of sectors 1118 (for example, four). Each sector is represented by a single region 1120 depicted on the disk 1106.

[0067] The File Allocation Table (FAT) features 1104 include an instrumented security function 1122 (for example, corresponding to the ISF chip 914) for tracking
30 cybersecurity events 1124. The instrumented security function 1122 can trigger components of the file allocation table features 1104, including an RTU operating system (OS) 1126, an integrated disk controller 1128, and a secure RTU file system 1130. Components of the file allocation table features 1104 can be used to erase the

disk 1106. Erasing the disk 1106 can occur sector-by-sector, for example, giving priority to sectors that should be erased first (for example, sectors containing the RTU configuration files 1114). Erasing can occur faster because of the use of adjacent sectors instead of allowing particular files to be stored as a fragmented file 1132.

5 [0068] The system 1100 can include security configuration software that performs various functions including, for example, resolving logic of securing SCADA network port access. For example, in case of a failed RFID identification or upon a motion detection in the vicinity of the RTU, a countdown can be initiated for entry of a security authorization PIN before a command or notification is sent to the SCADA
10 systems. The command can include, for example, a request to initiate video recording or a network management command to shut down the network port upon timeout expiration.

[0069] FIG. 12 is a flowchart of an example method 1200 for initiating data protection operations and forensics procedures, when conditions monitored at the RTU
15 are detected that warrant the data protection operation and the forensics procedures, according to some implementations of the present disclosure. For clarity of presentation, the description that follows generally describes method 1200 in the context of the other figures in this description. However, it will be understood that method 1200 can be performed, for example, by any suitable system, environment, software, and hardware,
20 or a combination of systems, environments, software, and hardware, as appropriate. In some implementations, various steps of method 1200 can be run in parallel, in combination, in loops, or in any order.

[0070] At 1202, monitoring is performed for conditions detected at an RTU that warrant a data protection operation and forensics procedures at the RTU. The
25 monitoring can be performed, for example, by the ISF chip 914 communicating with the remote RTU 406 in the SCADA network 404.

[0071] In some implementations, monitoring for the conditions can include operations of the logic flow 1000. For example, normality of the RTU can be verified by analyzing inputs received from occupancy sensors and radio frequency identification
30 (RFID) instruments of the RTU. Inputs can be verified as they are received from a network access controller (NAC) in the SCADA network. From 1202, method 1200 proceeds to 1204.

[0072] At 1204, upon determining that the conditions detected at the RTU warrant the data protection operation and forensics procedures, the data protection operation and the forensics procedures are initiated by the ISF chip. A data self-destruct of the RTU data can be initiated (for example, by the ISF chip 914). An emergency power supply can be engaged, such as a non-primary, backup power source of the RTU. A homing beacon and localization services can be activated, for example, that can be used by the forensics on-demand tracker 424.

[0073] In some implementations, initiating a data self-destruct of the RTU data by the ISF chip includes using a rapid erase file system (REFS) to quickly erase different types of information in a prioritized order, where each different type of information is ranked by a priority corresponding to criticality level of the different type of information. For example, the ISF chip 914 can initiate a process to erase clusters of the disk 1106 in an order that is based on priorities assigned to different clusters.

[0074] In some implementations, method 1200 can further include storing critical RTU data, including RTU configuration data, in adjacent clusters on a disk to decrease erasing times. For example, the RTU configuration files 1114 can be stored in adjacent clusters near the center of the disk 1106.

[0075] In some implementations, method 1200 further includes operations used to recover replicated RTU data. For example, RTU data of the RTU can be periodically replicated to preserve the RTU data for use in a recovery of the RTU data. At a time after completion the data protection operation and the forensics procedures, a presence of normal conditions at the RTU can be determined. Upon determining the presence of normal conditions at the RTU, the RTU data can be recovered.

[0076] In some implementations, periodically replicating the RTU data can be done in various ways. For example, the RTU data can be replicated to an encrypted storage device in the RTU. In another example, the RTU data can be replicated to an encrypted storage device in a different RTU. In another example, the RTU can be replicated data to an array of encrypted data storage allocated on the SCADA network.

[0077] FIG. 13 is a block diagram of an example computer system 1300 used to provide computational functionalities associated with described algorithms, methods, functions, processes, flows, and procedures described in the present disclosure, according to some implementations of the present disclosure. The illustrated computer 1302 is intended to encompass any computing device such as a server, a desktop

computer, a laptop/notebook computer, a wireless data port, a smart phone, a personal data assistant (PDA), a tablet computing device, or one or more processors within these devices, including physical instances, virtual instances, or both. The computer 1302 can include input devices such as keypads, keyboards, and touch screens that can accept user
5 information. Also, the computer 1302 can include output devices that can convey information associated with the operation of the computer 1302. The information can include digital data, visual data, audio information, or a combination of information. The information can be presented in a graphical user interface (UI) (or GUI).

[0078] The computer 1302 can serve in a role as a client, a network component,
10 a server, a database, a persistency, or components of a computer system for performing the subject matter described in the present disclosure. The illustrated computer 1302 is communicably coupled with a network 1330. In some implementations, one or more components of the computer 1302 can be configured to operate within different environments, including cloud-computing-based environments, local environments,
15 global environments, and combinations of environments.

[0079] At a high level, the computer 1302 is an electronic computing device operable to receive, transmit, process, store, and manage data and information associated with the described subject matter. According to some implementations, the computer 1302 can also include, or be communicably coupled with, an application server, an email
20 server, a web server, a caching server, a streaming data server, or a combination of servers.

[0080] The computer 1302 can receive requests over network 1330 from a client application (for example, executing on another computer 1302). The computer 1302 can respond to the received requests by processing the received requests using software
25 applications. Requests can also be sent to the computer 1302 from internal users (for example, from a command console), external (or third) parties, automated applications, entities, individuals, systems, or computers.

[0081] Each of the components of the computer 1302 can communicate using a system bus 1303. In some implementations, any or all of the components of the
30 computer 1302, including hardware or software components, can interface with each other or the interface 1304 (or a combination of both), over the system bus 1303. Interfaces can use an application programming interface (API) 1312, a service layer 1313, or a combination of the API 1312 and service layer 1313. The API 1312 can

include specifications for routines, data structures, and object classes. The API 1312 can be either computer-language independent or dependent. The API 1312 can refer to a complete interface, a single function, or a set of APIs.

[0082] The service layer 1313 can provide software services to the computer 5 1302 and other components (whether illustrated or not) that are communicably coupled to the computer 1302. The functionality of the computer 1302 can be accessible for all service consumers using this service layer. Software services, such as those provided by the service layer 1313, can provide reusable, defined functionalities through a defined interface. For example, the interface can be software written in JAVA, C++, extensible 10 markup language (XML), or any other suitable computer coding language. While illustrated as an integrated component of the computer 1302, in alternative implementations, the API 1312 or the service layer 1313 can be stand-alone components in relation to other components of the computer 1302 and other components communicably coupled to the computer 1302. Moreover, any or all parts of the API 15 1312 or the service layer 1313 can be implemented as child or sub-modules of another software module, enterprise application, or hardware module without departing from the scope of the present disclosure.

[0083] The computer 1302 includes an interface 1304. Although illustrated as a single interface 1304 in FIG. 13, two or more interfaces 1304 can be used according to 20 particular needs, desires, or particular implementations of the computer 1302 and the described functionality. The interface 1304 can be used by the computer 1302 for communicating with other systems that are connected to the network 1330 (whether illustrated or not) in a distributed environment. Generally, the interface 1304 can include, or be implemented using, logic encoded in software or hardware (or a 25 combination of software and hardware) operable to communicate with the network 1330. More specifically, the interface 1304 can include software supporting one or more communication protocols associated with communications. As such, the network 1330 or the interface's hardware can be operable to communicate physical signals within and outside of the illustrated computer 1302.

[0084] The computer 1302 includes a processor 1305. Although illustrated as a single processor 1305 in FIG. 13, two or more processors 1305 can be used according to particular needs, desires, or particular implementations of the computer 1302 and the 30 described functionality. Generally, the processor 1305 can execute instructions and can

manipulate data to perform the operations of the computer 1302, including operations using algorithms, methods, functions, processes, flows, and procedures as described in the present disclosure.

[0085] The computer 1302 also includes a database 1306 that can hold data for the computer 1302 and other components connected to the network 1330 (whether illustrated or not). For example, database 1306 can be an in-memory, conventional, or a database storing data consistent with the present disclosure. In some implementations, database 1306 can be a combination of two or more different database types (for example, hybrid in-memory and conventional databases) according to particular needs, desires, or particular implementations of the computer 1302 and the described functionality. Although illustrated as a single database 1306 in FIG. 13, two or more databases (of the same, different, or combination of types) can be used according to particular needs, desires, or particular implementations of the computer 1302 and the described functionality. While database 1306 is illustrated as an internal component of the computer 1302, in alternative implementations, database 1306 can be external to the computer 1302.

[0086] The computer 1302 also includes a memory 1307 that can hold data for the computer 1302 or a combination of components connected to the network 1330 (whether illustrated or not). Memory 1307 can store any data consistent with the present disclosure. In some implementations, memory 1307 can be a combination of two or more different types of memory (for example, a combination of semiconductor and magnetic storage) according to particular needs, desires, or particular implementations of the computer 1302 and the described functionality. Although illustrated as a single memory 1307 in FIG. 13, two or more memories 1307 (of the same, different, or combination of types) can be used according to particular needs, desires, or particular implementations of the computer 1302 and the described functionality. While memory 1307 is illustrated as an internal component of the computer 1302, in alternative implementations, memory 1307 can be external to the computer 1302.

[0087] The application 1308 can be an algorithmic software engine providing functionality according to particular needs, desires, or particular implementations of the computer 1302 and the described functionality. For example, application 1308 can serve as one or more components, modules, or applications. Further, although illustrated as a single application 1308, the application 1308 can be implemented as multiple

applications 1308 on the computer 1302. In addition, although illustrated as internal to the computer 1302, in alternative implementations, the application 1308 can be external to the computer 1302.

[0088] The computer 1302 can also include a power supply 1314. The power supply
5 1314 can include a rechargeable or non-rechargeable battery that can be configured to be either user- or non-user-replaceable. In some implementations, the power supply 1314 can include power-conversion and management circuits, including recharging, standby, and power management functionalities. In some implementations, the power-supply 1314 can include a power plug to allow the computer 1302 to be plugged into a
10 wall socket or a power source to, for example, power the computer 1302 or recharge a rechargeable battery.

[0089] There can be any number of computers 1302 associated with, or external to, a computer system containing computer 1302, with each computer 1302 communicating over network 1330. Further, the terms “client,” “user,” and other
15 appropriate terminology can be used interchangeably, as appropriate, without departing from the scope of the present disclosure. Moreover, the present disclosure contemplates that many users can use one computer 1302 and one user can use multiple computers 1302.

[0090] Described implementations of the subject matter can include one or more
20 features, alone or in combination.

[0091] For example, in a first implementation, a computer-implemented method for protecting data for a remote terminal unit (RTU) includes the following. Monitoring is performed for conditions detected at an RTU that warrant a data protection operation and forensics procedures at the RTU. The monitoring is performed by an instrumented
25 security function (ISF) chip communicating with the RTU in a supervisory control and data acquisition system (SCADA) network. Upon determining that the conditions detected at the RTU warrant the data protection operation, the data protection operation and the forensics procedures are initiated by the ISF chip.

[0092] The foregoing and other described implementations can each, optionally,
30 include one or more of the following features:

[0093] A first feature, combinable with any of the following features, the method further includes: periodically replicating RTU data of the RTU to preserve the RTU data for use in a recovery of the RTU data; determining, at a time after completion the data

protection operation and the forensics procedures, a presence of normal conditions at the RTU; and upon determining the presence of normal conditions at the RTU, recovering the RTU data.

[0094] A second feature, combinable with any of the previous or following features, where periodically replicating the RTU data includes one or more of:
5 replicating the RTU data to an encrypted storage device in the RTU; replicating the RTU data to an encrypted storage device in a different RTU; and replicating the RTU data to an array of encrypted data storage allocated on the SCADA network.

[0095] A third feature, combinable with any of the previous or following features, where initiating the data protection operation and the forensics procedures
10 includes: initiating a data self-destruct of the RTU data by the ISF chip; engaging an emergency power supply; and activating a homing beacon and localization services.

[0096] A fourth feature, combinable with any of the previous or following features, where initiating a data self-destruct of the RTU data by the ISF chip includes
15 using a rapid erase file system (REFS) to quickly erase different types of information in a prioritized order, where each different type of information is ranked by a priority corresponding to criticality level of the different type of information.

[0097] A fifth feature, combinable with any of the previous or following features, the method further including storing critical RTU data, including RTU
20 configuration data, in adjacent clusters on a disk to decrease erasing times.

[0098] A sixth feature, combinable with any of the previous or following features, where monitoring for the conditions detected at the RTU warranting the data protection operation and the forensics procedures at the RTU includes: verifying
25 normality of the RTU by analyzing inputs received from occupancy sensors and radio frequency identification (RFID) instruments of the RTU; and verifying inputs received from a network access controller (NAC) in the SCADA network.

[0099] In a second implementation, a non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations including the following. Monitoring is performed for conditions detected at
30 an RTU that warrant a data protection operation and forensics procedures at the RTU. The monitoring is performed by an instrumented security function (ISF) chip communicating with the RTU in a supervisory control and data acquisition system (SCADA) network. Upon determining that the conditions detected at the RTU warrant

the data protection operation and the forensics procedures, the data protection operation and the forensics procedures are initiated by the ISF chip.

[00100] The foregoing and other described implementations can each, optionally, include one or more of the following features:

5 [00101] A first feature, combinable with any of the following features, the operations further including: periodically replicating RTU data of the RTU to preserve the RTU data for use in a recovery of the RTU data; determining, at a time after completion the data protection operation and the forensics procedures, a presence of normal conditions at the RTU; and upon determining the presence of normal conditions
10 at the RTU, recovering the RTU data.

[00102] A second feature, combinable with any of the previous or following features, where periodically replicating the RTU data includes one or more of: replicating the RTU data to an encrypted storage device in the RTU; replicating the RTU data to an encrypted storage device in a different RTU; and replicating the RTU data to
15 an array of encrypted data storage allocated on the SCADA network.

[00103] A third feature, combinable with any of the previous or following features, where initiating the data protection operation and the forensics procedures includes: initiating a data self-destruct of the RTU data by the ISF chip; engaging an emergency power supply; and activating a homing beacon and localization services.

20 [00104] A fourth feature, combinable with any of the previous or following features, where initiating a data self-destruct of the RTU data by the ISF chip includes using a rapid erase file system (REFS) to quickly erase different types of information in a prioritized order, where each different type of information is ranked by a priority corresponding to criticality level of the different type of information.

25 [00105] A fifth feature, combinable with any of the previous or following features, the operations further including storing critical RTU data, including RTU configuration data, in adjacent clusters on a disk to decrease erasing times.

[00106] A sixth feature, combinable with any of the previous or following features, where monitoring for the conditions detected at the RTU warranting the data
30 protection operation and forensics procedures at the RTU includes: verifying normality of the RTU by analyzing inputs received from occupancy sensors and radio frequency identification (RFID) instruments of the RTU; and verifying inputs received from a network access controller (NAC) in the SCADA network.

[00107] In a third implementation, a computer-implemented system, including one or more processors and a non-transitory computer-readable storage medium coupled to the one or more processors and storing programming instructions for execution by the one or more processors, the programming instructions instructing the one or more
5 processors to perform operations including: monitoring, by an instrumented security function (ISF) chip communicating with a remote terminal unit (RTU) in a supervisory control and data acquisition system (SCADA) network, for conditions detected at the RTU warranting a data protection operation and forensics procedures at the RTU; and upon determining that the conditions detected at the RTU warrant the data protection
10 operation and the forensics procedures, initiating, by the ISF chip, the data protection operation and the forensics procedures.

[00108] The foregoing and other described implementations can each, optionally, include one or more of the following features:

[00109] A first feature, combinable with any of the following features, the
15 operations further including: periodically replicating RTU data of the RTU to preserve the RTU data for use in a recovery of the RTU data; determining, at a time after completion the data protection operation and the forensics procedures, a presence of normal conditions at the RTU; and upon determining the presence of normal conditions at the RTU, recovering the RTU data.

[00110] A second feature, combinable with any of the previous or following
20 features, where periodically replicating the RTU data includes one or more of: replicating the RTU data to an encrypted storage device in the RTU; replicating the RTU data to an encrypted storage device in a different RTU; and replicating the RTU data to an array of encrypted data storage allocated on the SCADA network.

[00111] A third feature, combinable with any of the previous or following
25 features, where initiating the data protection operation and the forensics procedures includes: initiating a data self-destruct of the RTU data by the ISF chip; engaging an emergency power supply; and activating a homing beacon and localization services.

[00112] A fourth feature, combinable with any of the previous or following
30 features, where initiating a data self-destruct of the RTU data by the ISF chip includes using a rapid erase file system (REFS) to quickly erase different types of information in a prioritized order, where each different type of information is ranked by a priority corresponding to criticality level of the different type of information.

[00113] A fifth feature, combinable with any of the previous or following features, the operations further including storing critical RTU data, including RTU configuration data, in adjacent clusters on a disk to decrease erasing times.

[00114] Implementations of the subject matter and the functional operations
5 described in this specification can be implemented in digital electronic circuitry, in tangibly embodied computer software or firmware, in computer hardware, including the structures disclosed in this specification and their structural equivalents, or in combinations of one or more of them. Software implementations of the described subject matter can be implemented as one or more computer programs. Each computer
10 program can include one or more modules of computer program instructions encoded on a tangible, non-transitory, computer-readable computer-storage medium for execution by, or to control the operation of, data processing apparatus. Alternatively, or additionally, the program instructions can be encoded in/on an artificially generated propagated signal. The example, the signal can be a machine-generated electrical,
15 optical, or electromagnetic signal that is generated to encode information for transmission to suitable receiver apparatus for execution by a data processing apparatus. The computer-storage medium can be a machine-readable storage device, a machine-readable storage substrate, a random or serial access memory device, or a combination of computer-storage mediums.

[00115] The terms “data processing apparatus,” “computer,” and “electronic
20 computer device” (or equivalent as understood by one of ordinary skill in the art) refer to data processing hardware. For example, a data processing apparatus can encompass all kinds of apparatus, devices, and machines for processing data, including by way of example, a programmable processor, a computer, or multiple processors or computers.
25 The apparatus can also include special purpose logic circuitry including, for example, a central processing unit (CPU), a field programmable gate array (FPGA), or an application-specific integrated circuit (ASIC). In some implementations, the data processing apparatus or special purpose logic circuitry (or a combination of the data processing apparatus or special purpose logic circuitry) can be hardware- or software-
30 based (or a combination of both hardware- and software-based). The apparatus can optionally include code that creates an execution environment for computer programs, for example, code that constitutes processor firmware, a protocol stack, a database management system, an operating system, or a combination of execution environments.

The present disclosure contemplates the use of data processing apparatuses with or without conventional operating systems, for example LINUX, UNIX, WINDOWS, MAC OS, ANDROID, or IOS.

[00116] A computer program, which can also be referred to or described as a
5 program, software, a software application, a module, a software module, a script, or
code, can be written in any form of programming language. Programming languages
can include, for example, compiled languages, interpreted languages, declarative
languages, or procedural languages. Programs can be deployed in any form, including
as stand-alone programs, modules, components, subroutines, or units for use in a
10 computing environment. A computer program can, but need not, correspond to a file in
a file system. A program can be stored in a portion of a file that holds other programs
or data, for example, one or more scripts stored in a markup language document, in a
single file dedicated to the program in question, or in multiple coordinated files storing
one or more modules, sub-programs, or portions of code. A computer program can be
15 deployed for execution on one computer or on multiple computers that are located, for
example, at one site or distributed across multiple sites that are interconnected by a
communication network. While portions of the programs illustrated in the various
figures may be shown as individual modules that implement the various features and
functionality through various objects, methods, or processes, the programs can instead
20 include a number of sub-modules, third-party services, components, and libraries.
Conversely, the features and functionality of various components can be combined into
single components as appropriate. Thresholds used to make computational
determinations can be statically, dynamically, or both statically and dynamically
determined.

25 [00117] The methods, processes, or logic flows described in this specification can
be performed by one or more programmable computers executing one or more computer
programs to perform functions by operating on input data and generating output. The
methods, processes, or logic flows can also be performed by, and apparatus can also be
implemented as, special purpose logic circuitry, for example, a CPU, an FPGA, or an
30 ASIC.

[00118] Computers suitable for the execution of a computer program can be based
on one or more of general and special purpose microprocessors and other kinds of CPUs.
The elements of a computer are a CPU for performing or executing instructions and one

or more memory devices for storing instructions and data. Generally, a CPU can receive instructions and data from (and write data to) a memory. A computer can also include, or be operatively coupled to, one or more mass storage devices for storing data. In some implementations, a computer can receive data from, and transfer data to, the mass storage devices including, for example, magnetic, magneto-optical disks, or optical disks. Moreover, a computer can be embedded in another device, for example, a mobile telephone, a personal digital assistant (PDA), a mobile audio or video player, a game console, a global positioning system (GPS) receiver, or a portable storage device such as a universal serial bus (USB) flash drive.

[00119] Computer-readable media (transitory or non-transitory, as appropriate) suitable for storing computer program instructions and data can include all forms of permanent/non-permanent and volatile/non-volatile memory, media, and memory devices. Computer-readable media can include, for example, semiconductor memory devices such as random access memory (RAM), read-only memory (ROM), phase change memory (PRAM), static random access memory (SRAM), dynamic random access memory (DRAM), erasable programmable read-only memory (EPROM), electrically erasable programmable read-only memory (EEPROM), and flash memory devices. Computer-readable media can also include, for example, magnetic devices such as tape, cartridges, cassettes, and internal/removable disks. Computer-readable media can also include magneto-optical disks and optical memory devices and technologies including, for example, digital video disc (DVD), CD-ROM, DVD+/-R, DVD-RAM, DVD-ROM, HD-DVD, and BLURAY. The memory can store various objects or data, including caches, classes, frameworks, applications, modules, backup data, jobs, web pages, web page templates, data structures, database tables, repositories, and dynamic information. Types of objects and data stored in memory can include parameters, variables, algorithms, instructions, rules, constraints, and references. Additionally, the memory can include logs, policies, security or access data, and reporting files. The processor and the memory can be supplemented by, or incorporated in, special purpose logic circuitry.

[00120] Implementations of the subject matter described in the present disclosure can be implemented on a computer having a display device for providing interaction with a user, including displaying information to (and receiving input from) the user. Types of display devices can include, for example, a cathode ray tube (CRT), a liquid

crystal display (LCD), a light-emitting diode (LED), and a plasma monitor. Display devices can include a keyboard and pointing devices including, for example, a mouse, a trackball, or a trackpad. User input can also be provided to the computer through the use of a touchscreen, such as a tablet computer surface with pressure sensitivity or a multi-touch screen using capacitive or electric sensing. Other kinds of devices can be used to provide for interaction with a user, including to receive user feedback including, for example, sensory feedback including visual feedback, auditory feedback, or tactile feedback. Input from the user can be received in the form of acoustic, speech, or tactile input. In addition, a computer can interact with a user by sending documents to, and receiving documents from, a device that is used by the user. For example, the computer can send web pages to a web browser on a user's client device in response to requests received from the web browser.

[00121] The term "graphical user interface," or "GUI," can be used in the singular or the plural to describe one or more graphical user interfaces and each of the displays of a particular graphical user interface. Therefore, a GUI can represent any graphical user interface, including, but not limited to, a web browser, a touch screen, or a command line interface (CLI) that processes information and efficiently presents the information results to the user. In general, a GUI can include a plurality of user interface (UI) elements, some or all associated with a web browser, such as interactive fields, pull-down lists, and buttons. These and other UI elements can be related to or represent the functions of the web browser.

[00122] Implementations of the subject matter described in this specification can be implemented in a computing system that includes a back-end component, for example, as a data server, or that includes a middleware component, for example, an application server. Moreover, the computing system can include a front-end component, for example, a client computer having one or both of a graphical user interface or a Web browser through which a user can interact with the computer. The components of the system can be interconnected by any form or medium of wireline or wireless digital data communication (or a combination of data communication) in a communication network. Examples of communication networks include a local area network (LAN), a radio access network (RAN), a metropolitan area network (MAN), a wide area network (WAN), Worldwide Interoperability for Microwave Access (WIMAX), a wireless local area network (WLAN) (for example, using 802.11 a/b/g/n or 802.20 or a combination

of protocols), all or a portion of the Internet, or any other communication system or systems at one or more locations (or a combination of communication networks). The network can communicate with, for example, Internet Protocol (IP) packets, frame relay frames, asynchronous transfer mode (ATM) cells, voice, video, data, or a combination of communication types between network addresses.

[00123] The computing system can include clients and servers. A client and server can generally be remote from each other and can typically interact through a communication network. The relationship of client and server can arise by virtue of computer programs running on the respective computers and having a client-server relationship.

[00124] Cluster file systems can be any file system type accessible from multiple servers for read and update. Locking or consistency tracking may not be necessary since the locking of exchange file system can be done at application layer. Furthermore, Unicode data files can be different from non-Unicode data files.

[00125] While this specification contains many specific implementation details, these should not be construed as limitations on the scope of what may be claimed, but rather as descriptions of features that may be specific to particular implementations. Certain features that are described in this specification in the context of separate implementations can also be implemented, in combination, in a single implementation. Conversely, various features that are described in the context of a single implementation can also be implemented in multiple implementations, separately, or in any suitable sub-combination. Moreover, although previously described features may be described as acting in certain combinations and even initially claimed as such, one or more features from a claimed combination can, in some cases, be excised from the combination, and the claimed combination may be directed to a sub-combination or variation of a sub-combination.

[00126] Particular implementations of the subject matter have been described. Other implementations, alterations, and permutations of the described implementations are within the scope of the following claims as will be apparent to those skilled in the art. While operations are depicted in the drawings or claims in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed (some operations may be considered optional), to achieve desirable results. In certain

circumstances, multitasking or parallel processing (or a combination of multitasking and parallel processing) may be advantageous and performed as deemed appropriate.

[00127] Moreover, the separation or integration of various system modules and components in the previously described implementations should not be understood as
5 requiring such separation or integration in all implementations, and it should be understood that the described program components and systems can generally be integrated together in a single software product or packaged into multiple software products.

[00128] Accordingly, the previously described example implementations do not
10 define or constrain the present disclosure. Other changes, substitutions, and alterations are also possible without departing from the spirit and scope of the present disclosure.

[00129] Furthermore, any claimed implementation is considered to be applicable to at least a computer-implemented method; a non-transitory, computer-readable medium storing computer-readable instructions to perform the computer-implemented
15 method; and a computer system including a computer memory interoperably coupled with a hardware processor configured to perform the computer-implemented method or the instructions stored on the non-transitory, computer-readable medium.

CLAIMS

What is claimed is:

1. A computer-implemented method, comprising:
 - monitoring, by an instrumented security function (ISF) chip communicating
 - 5 with a remote terminal unit (RTU) in a supervisory control and data acquisition system (SCADA) network, for conditions detected at the RTU warranting a data protection operation and forensics procedures at the RTU; and
 - upon determining that the conditions detected at the RTU warrant the data protection operation and the forensics procedures, initiating, by the ISF chip, the data
 - 10 protection operation and the forensics procedures.
2. The computer-implemented method of claim 1, further comprising:
 - periodically replicating RTU data of the RTU to preserve the RTU data for use
 - in a recovery of the RTU data;
 - determining, at a time after completion the data protection operation and the
 - 15 forensics procedures, a presence of normal conditions at the RTU; and
 - upon determining the presence of normal conditions at the RTU, recovering the RTU data.
3. The computer-implemented method of claim 2, wherein periodically replicating the RTU data includes one or more of:
 - 20 replicating the RTU data to an encrypted storage device in the RTU;
 - replicating the RTU data to an encrypted storage device in a different RTU;
 - and
 - replicating the RTU data to an array of encrypted data storage allocated on the SCADA network.
- 25 4. The computer-implemented method of claim 1, wherein initiating the data protection operation and the forensics procedures includes:
 - initiating a data self-destruct of the RTU data by the ISF chip;
 - engaging an emergency power supply; and
 - activating a homing beacon and localization services.

5. The computer-implemented method of claim 4, wherein initiating a data self-destruct of the RTU data by the ISF chip includes using a rapid erase file system (REFS) to quickly erase different types of information in a prioritized order, wherein each different type of information is ranked by a priority corresponding to criticality level of the different type of information.
6. The computer-implemented method of claim 5, further comprising storing critical RTU data, including RTU configuration data, in adjacent clusters on a disk to decrease erasing times.
7. The computer-implemented method of claim 1, wherein monitoring for the conditions detected at the RTU warranting the data protection operation and the forensics procedures at the RTU includes:
- verifying normality of the RTU by analyzing inputs received from occupancy sensors and radio frequency identification (RFID) instruments of the RTU; and
 - verifying inputs received from a network access controller (NAC) in the SCADA network.
8. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:
- monitoring, by an instrumented security function (ISF) chip communicating with a remote terminal unit (RTU) in a supervisory control and data acquisition system (SCADA) network, for conditions detected at the RTU warranting a data protection operation and forensics procedures at the RTU; and
 - upon determining that the conditions detected at the RTU warrant the data protection operation and the forensics procedures, initiating, by the ISF chip, the data protection operation and the forensics procedures.
9. The non-transitory, computer-readable medium of claim 8, the operations further comprising:
- periodically replicating RTU data of the RTU to preserve the RTU data for use in a recovery of the RTU data;
 - determining, at a time after completion the data protection operation and the forensics procedures, a presence of normal conditions at the RTU; and

upon determining the presence of normal conditions at the RTU, recovering the RTU data.

10. The non-transitory, computer-readable medium of claim 9, wherein periodically replicating the RTU data includes one or more of:

- 5 replicating the RTU data to an encrypted storage device in the RTU;
- replicating the RTU data to an encrypted storage device in a different RTU;
- and
- replicating the RTU data to an array of encrypted data storage allocated on the SCADA network.

10 11. The non-transitory, computer-readable medium of claim 8, wherein initiating the data protection operation and the forensics procedures includes:

- initiating a data self-destruct of the RTU data by the ISF chip;
- engaging an emergency power supply; and
- activating a homing beacon and localization services.

15 12. The non-transitory, computer-readable medium of claim 11, wherein initiating a data self-destruct of the RTU data by the ISF chip includes using a rapid erase file system (REFS) to quickly erase different types of information in a prioritized order, wherein each different type of information is ranked by a priority corresponding to criticality level of the different type of information.

20 13. The non-transitory, computer-readable medium of claim 12, the operations further comprising storing critical RTU data, including RTU configuration data, in adjacent clusters on a disk to decrease erasing times.

 14. The non-transitory, computer-readable medium of claim 8, wherein monitoring for the conditions detected at the RTU warranting the data protection operation and the
25 forensics procedures at the RTU includes:

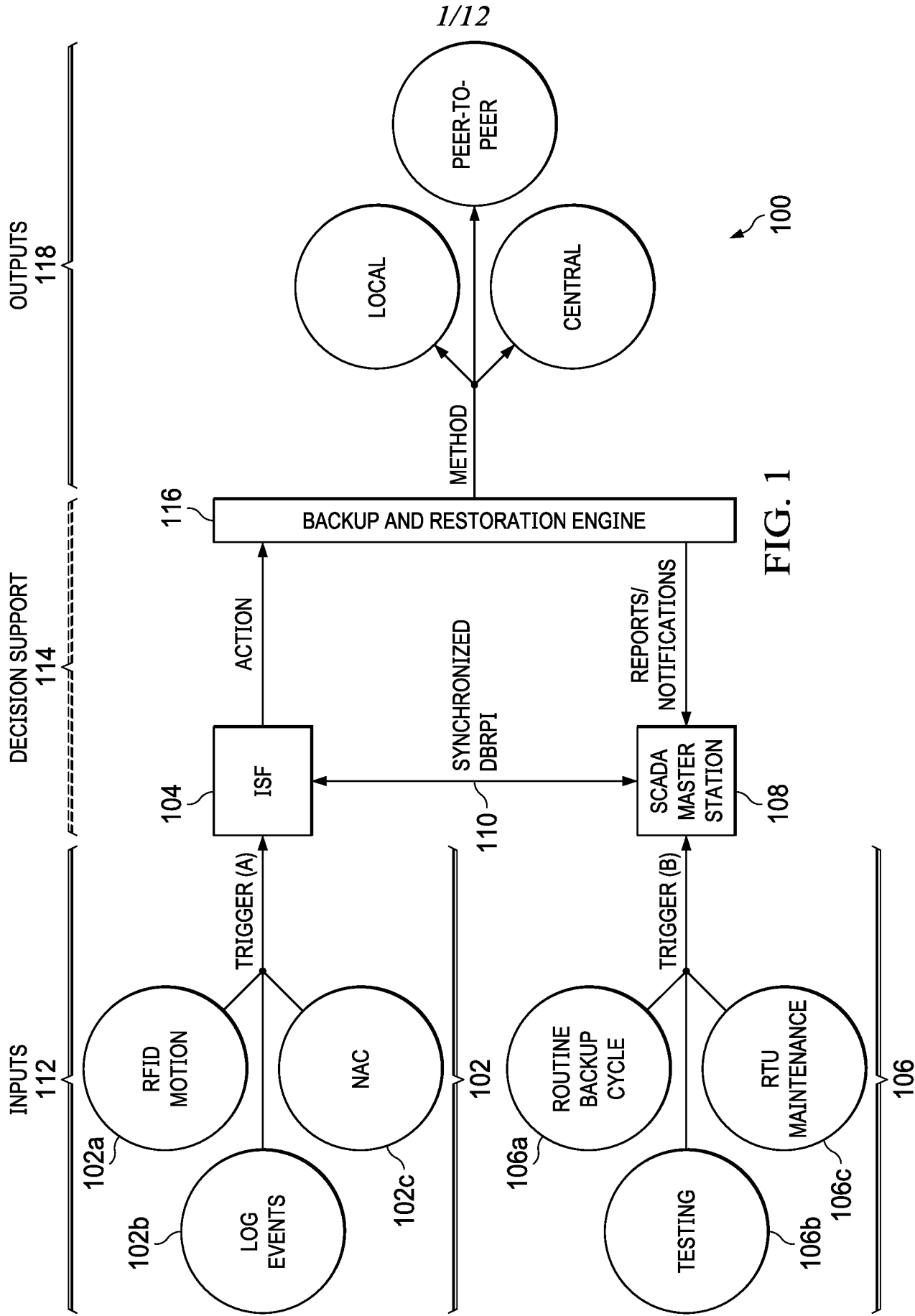
- verifying normality of the RTU by analyzing inputs received from occupancy sensors and radio frequency identification (RFID) instruments of the RTU; and
- verifying inputs received from a network access controller (NAC) in the SCADA network.

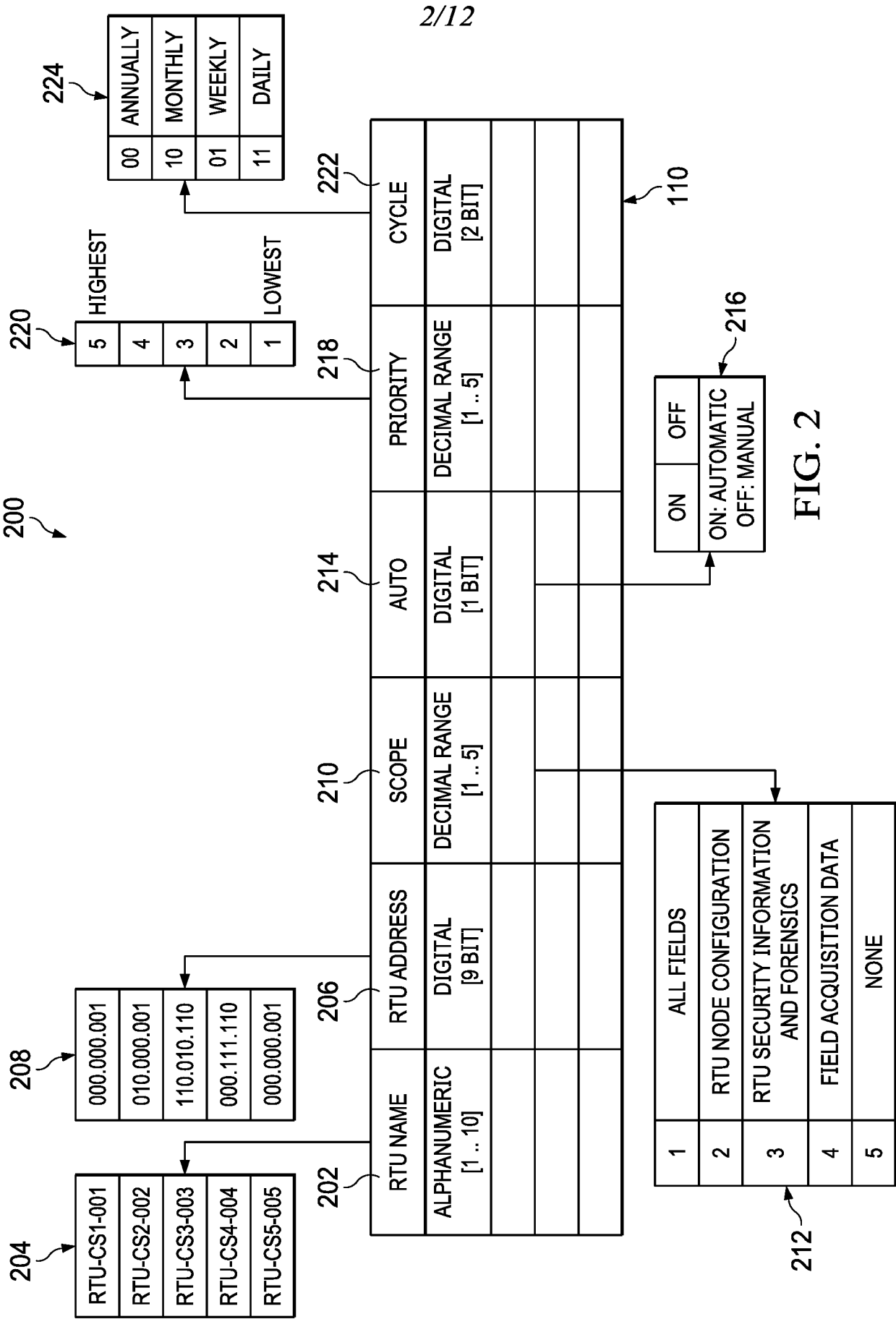
15. A computer-implemented system, comprising:
one or more processors; and
a non-transitory computer-readable storage medium coupled to the one or more
processors and storing programming instructions for execution by the one or more
5 processors, the programming instructions instructing the one or more processors to
perform operations comprising:
monitoring, by an instrumented security function (ISF) chip
communicating with a remote terminal unit (RTU) in a supervisory control and data
acquisition system (SCADA) network, for conditions detected at the RTU warranting a
10 data protection operation and forensics procedures at the RTU; and
upon determining that the conditions detected at the RTU warrant the
data protection operation and the forensics procedures, initiating, by the ISF chip, the
data protection operation and the forensics procedures.
16. The computer-implemented system of claim 15, the operations further comprising:
15 periodically replicating RTU data of the RTU to preserve the RTU data for use
in a recovery of the RTU data;
determining, at a time after completion the data protection operation and the
forensics procedures, a presence of normal conditions at the RTU; and
upon determining the presence of normal conditions at the RTU, recovering the
20 RTU data.
17. The computer-implemented system of claim 16, wherein periodically replicating
the RTU data includes one or more of:
replicating the RTU data to an encrypted storage device in the RTU;
replicating the RTU data to an encrypted storage device in a different RTU;
25 and
replicating the RTU data to an array of encrypted data storage allocated on the
SCADA network.
18. The computer-implemented system of claim 15, wherein initiating the data
protection operation and the forensics procedures includes:
30 initiating a data self-destruct of the RTU data by the ISF chip;
engaging an emergency power supply; and

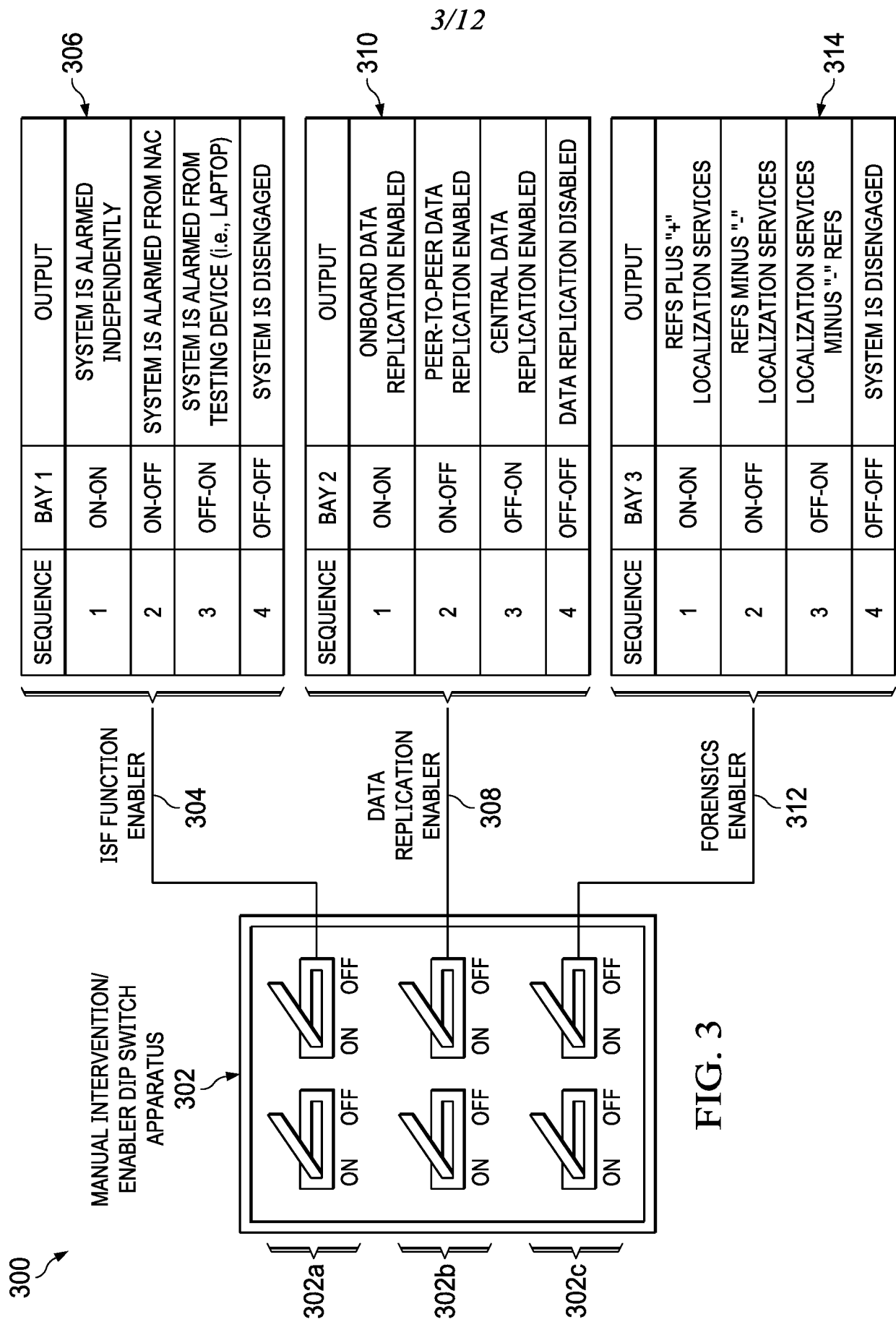
activating a homing beacon and localization services.

19. The computer-implemented system of claim 18, wherein initiating a data self-destruct of the RTU data by the ISF chip includes using a rapid erase file system (REFS) to quickly erase different types of information in a prioritized order, wherein each
5 different type of information is ranked by a priority corresponding to criticality level of the different type of information.

20. The computer-implemented system of claim 19, the operations further comprising storing critical RTU data, including RTU configuration data, in adjacent clusters on a disk to decrease erasing times.







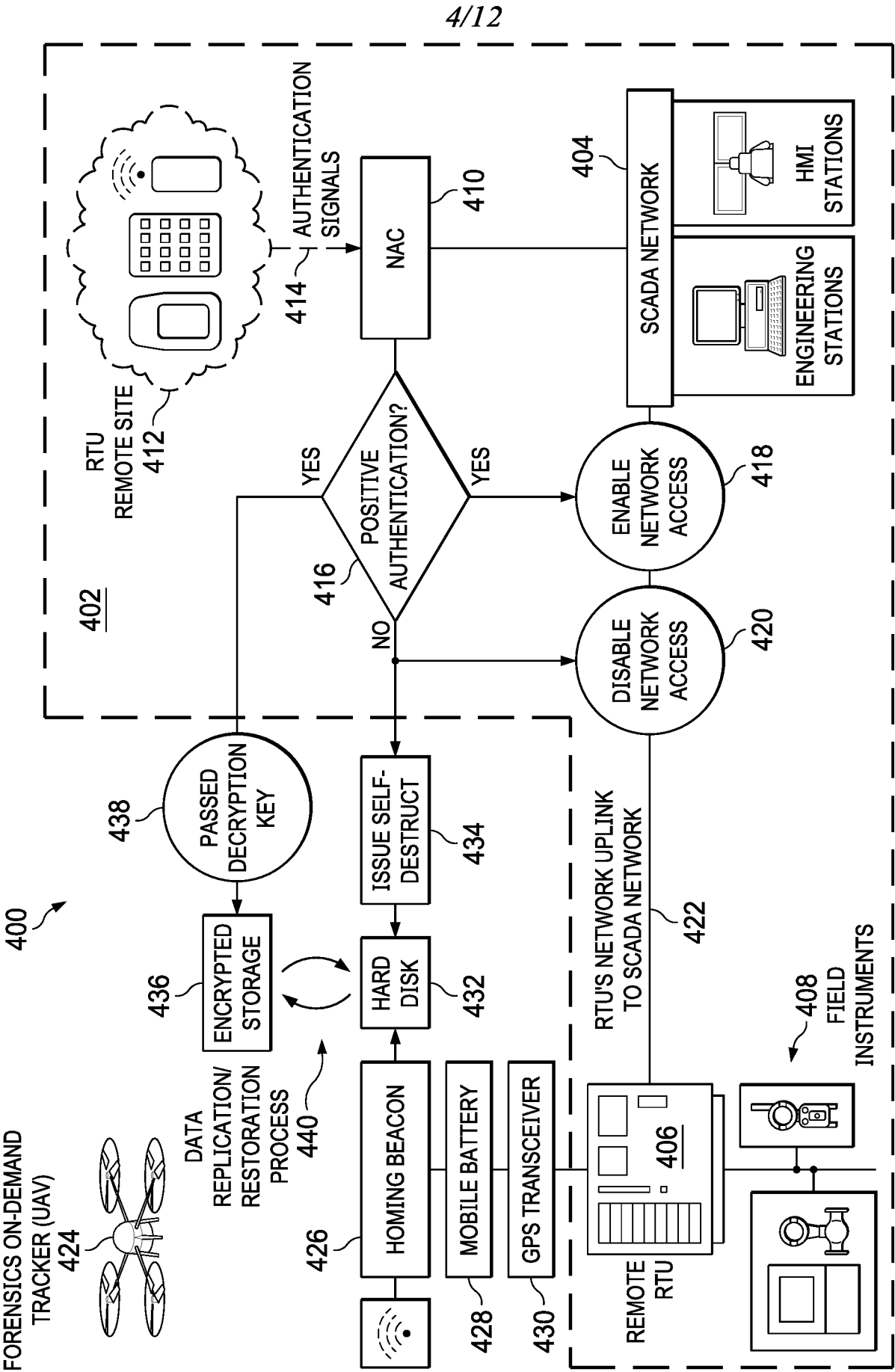


FIG. 4

5/12

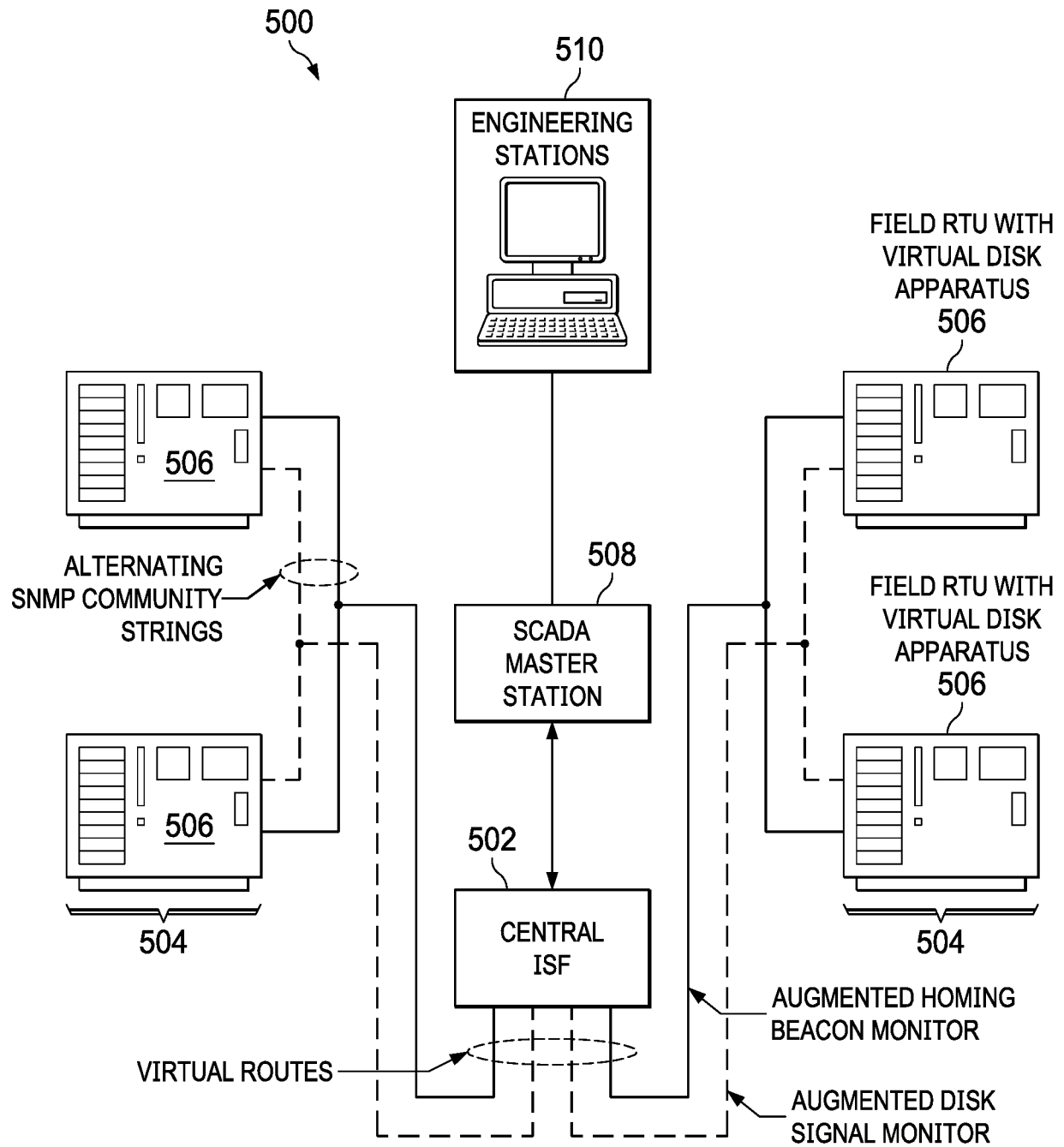


FIG. 5

6/12

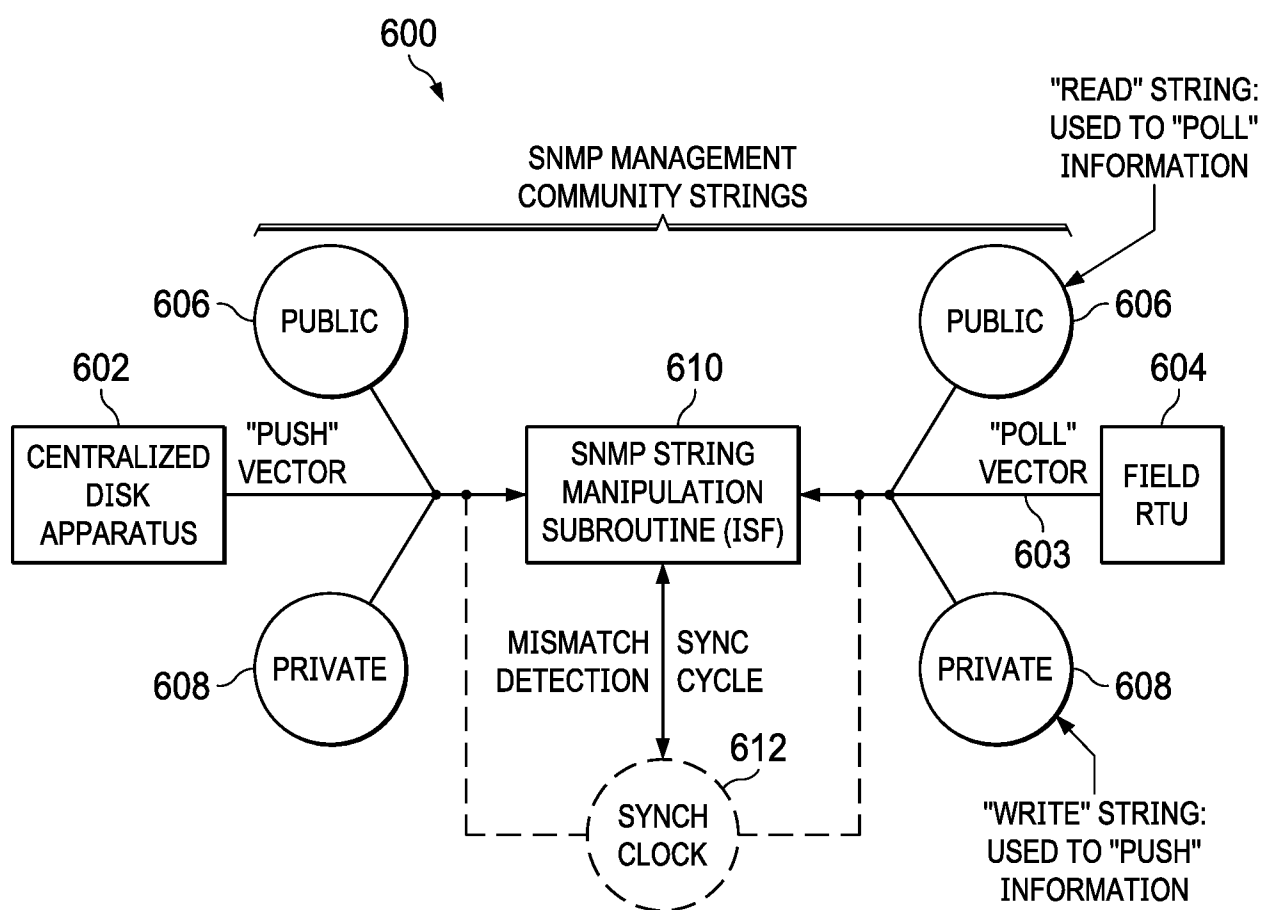


FIG. 6

7/12

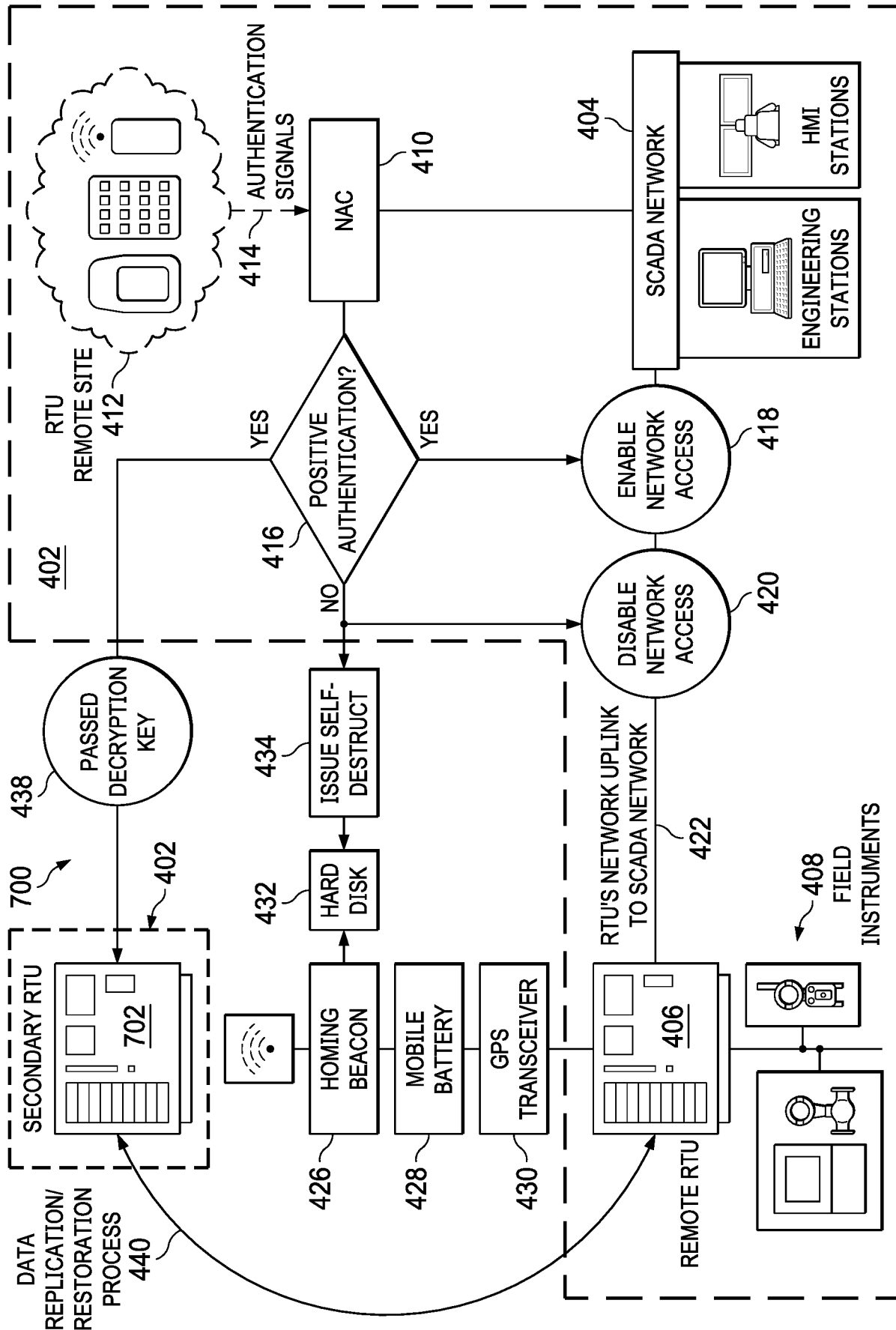


FIG. 7

8/12

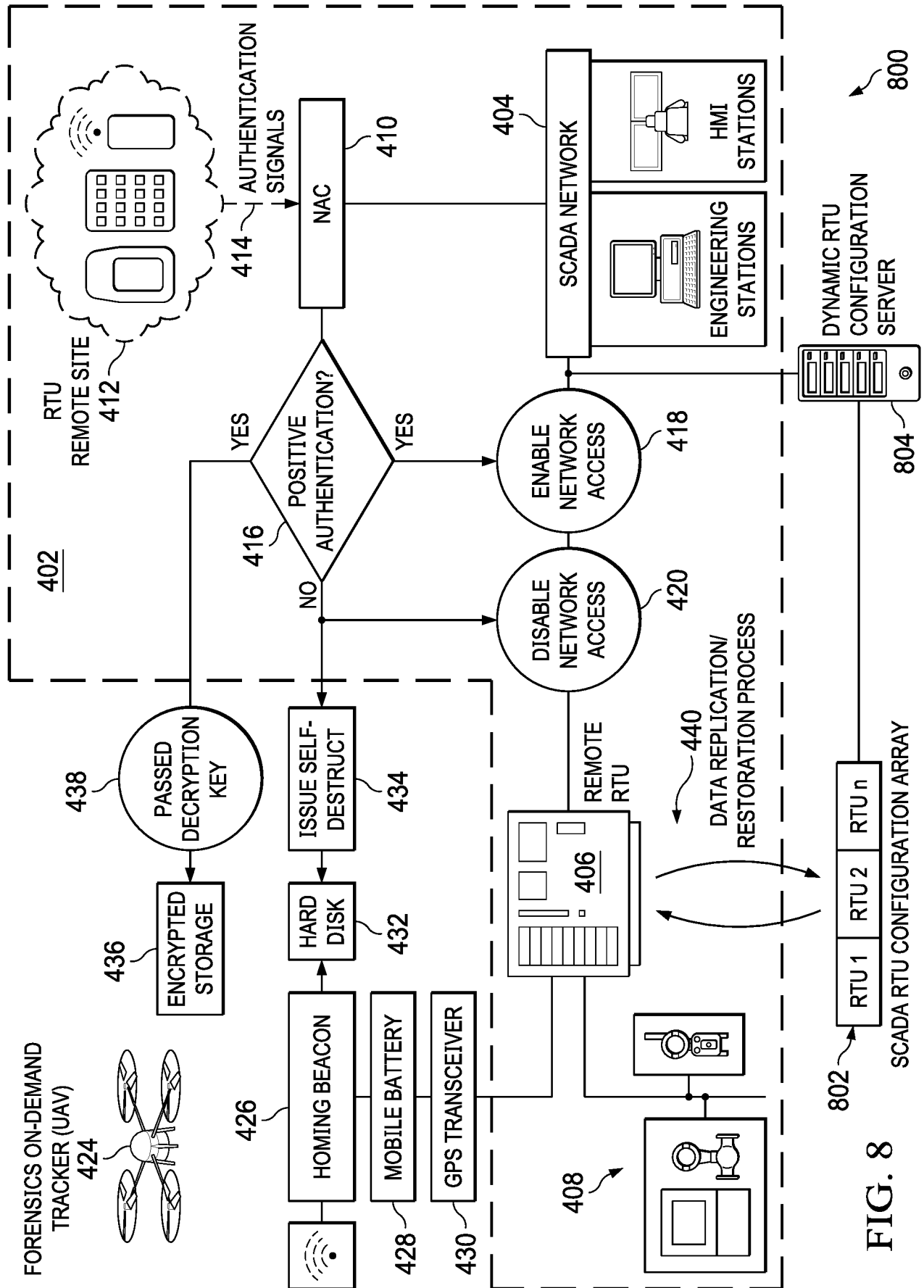
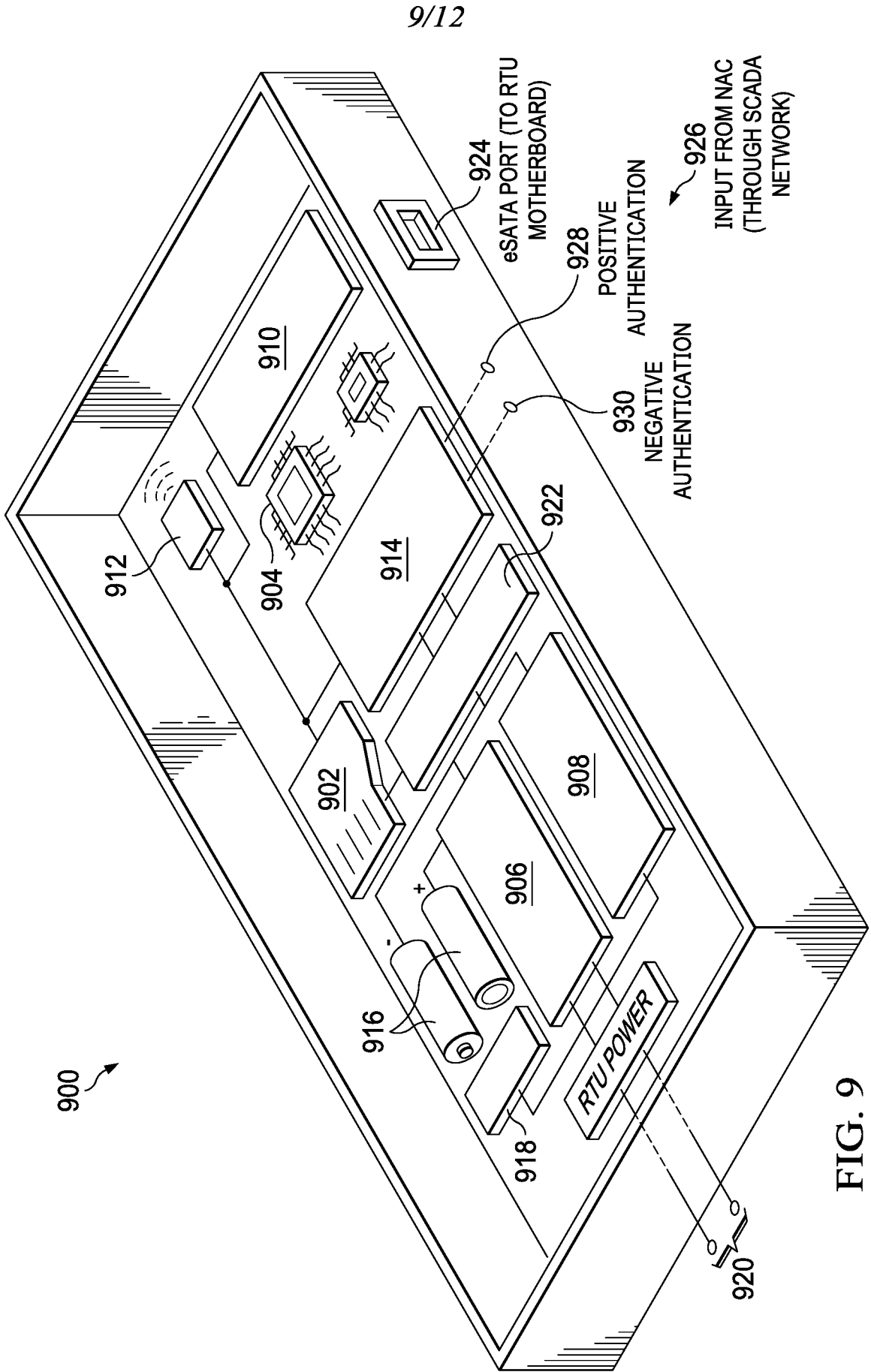


FIG. 8



10/12

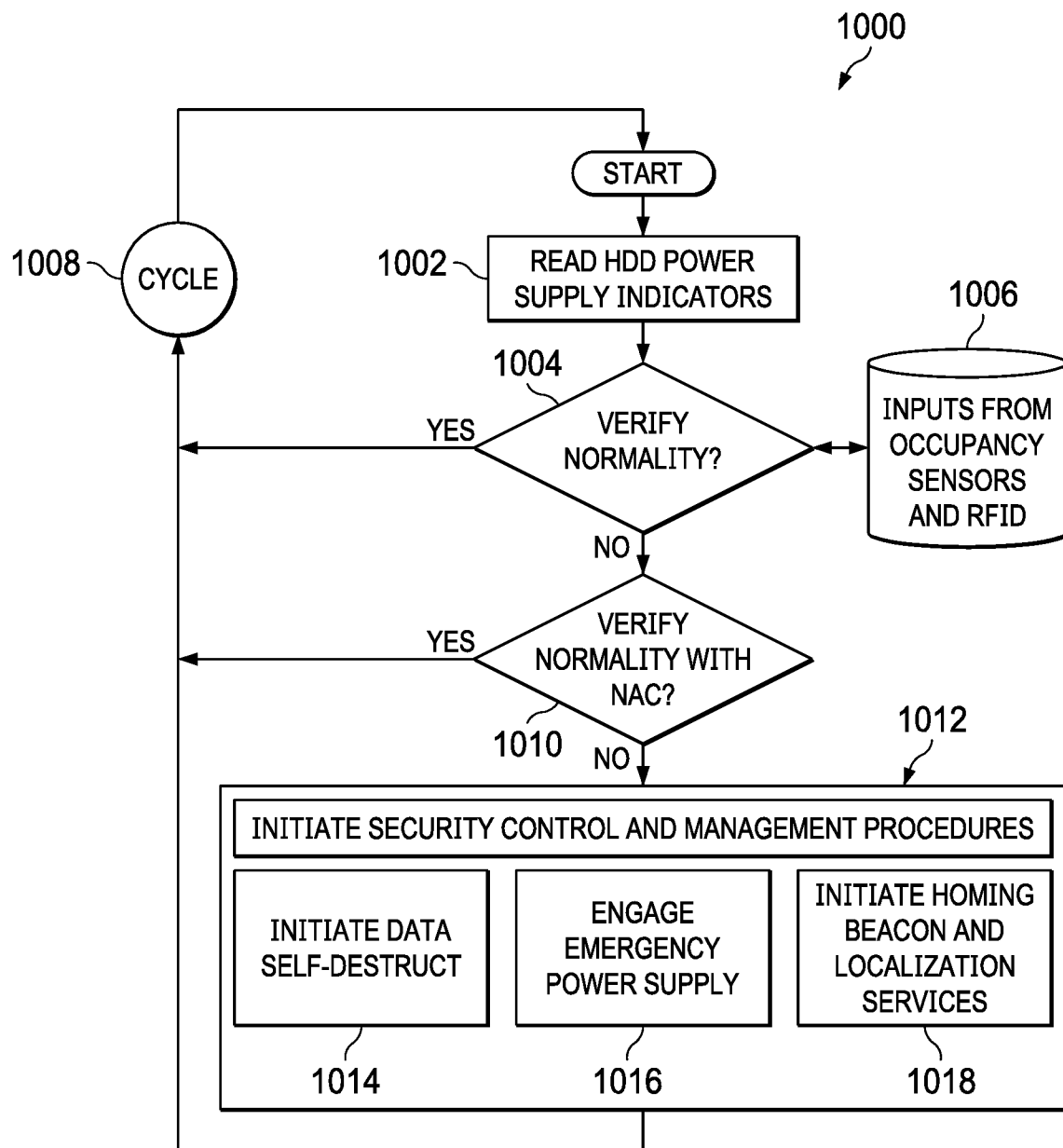
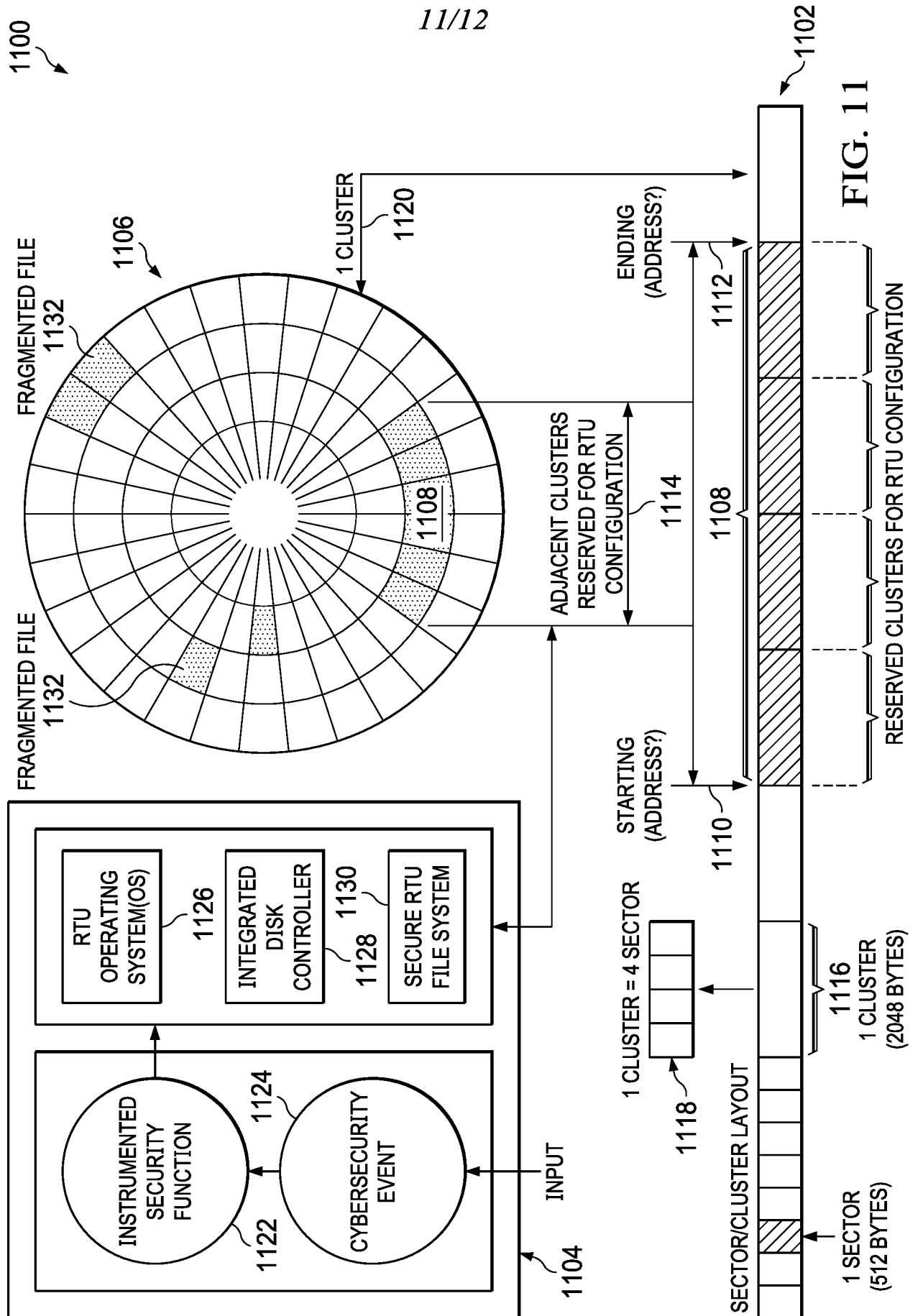


FIG. 10



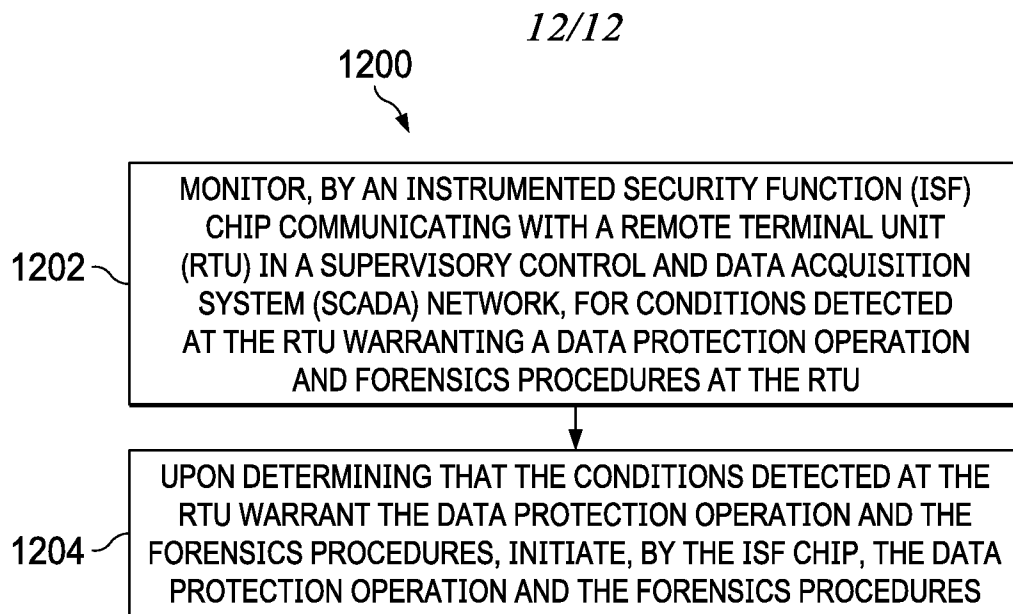


FIG. 12

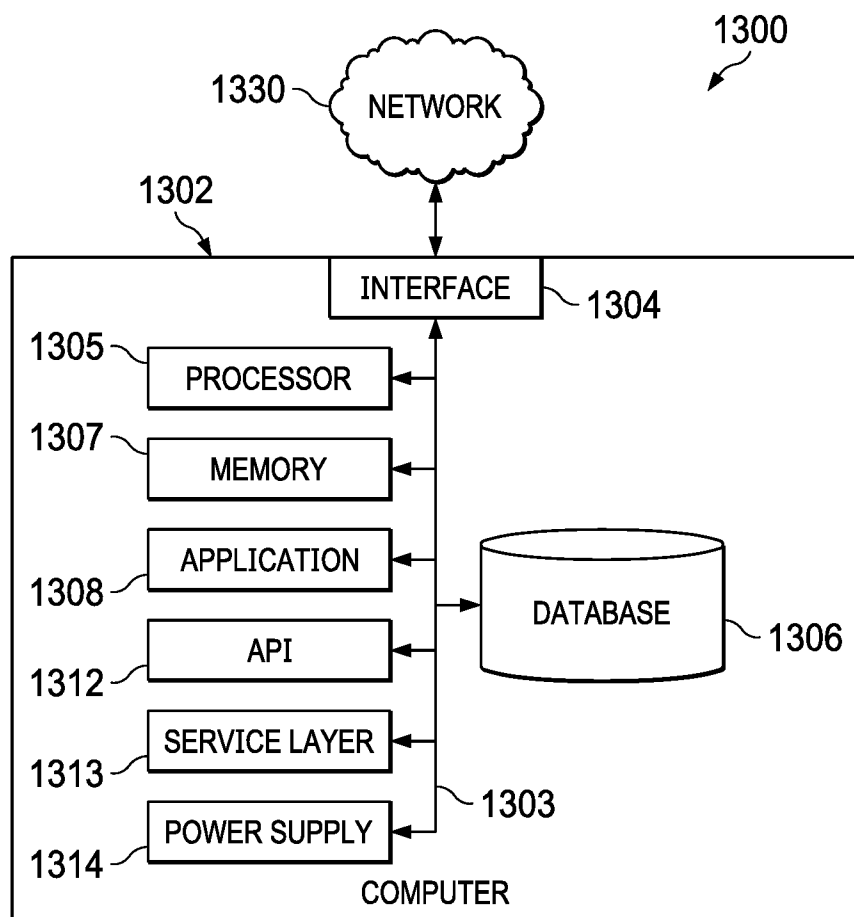


FIG. 13

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2020/019009

A. CLASSIFICATION OF SUBJECT MATTER INV. G06F21/50 G06F21/88 H04W12/00 ADD.		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) G06F H04W		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/060030 A1 (LAMB NICHOLAS L [US]) 8 March 2012 (2012-03-08)	1,7,8, 14,15
Y	paragraphs [0021], [0049] - [0075], [0098], [0138]; claim 18	2-6, 9-13, 16-20
Y	----- WO 2018/207123 A1 (AGARWAL SUBHAM [IN]) 15 November 2018 (2018-11-15) page 11, lines 20-24 page 12, lines 22-32 page 14, lines 4-32 page 16, line 23 - page 17, line 10 page 21, line 17 - page 22, line 4 -----	2,3,9, 10,16,17
Y	US 2014/230057 A1 (BERGER MICHAEL [IL]) 14 August 2014 (2014-08-14) paragraphs [0043] - [0048], [0054] - [0056], [0111] ----- -/-	4,11,18
☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 30 April 2020		Date of mailing of the international search report 08/05/2020
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Herzog, Till-Henning

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2020/019009

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2004/188710 A1 (KOREN RAMI [IL] ET AL) 30 September 2004 (2004-09-30) paragraphs [0053] - [0057] -----	5,6,12, 13,19,20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2020/019009

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012060030	A1	08-03-2012	NONE
WO 2018207123	A1	15-11-2018	NONE
US 2014230057	A1	14-08-2014	EP 2795520 A1 29-10-2014 TW 201344495 A 01-11-2013 US 2014230057 A1 14-08-2014 WO 2013095585 A1 27-06-2013
US 2004188710	A1	30-09-2004	US 2004188710 A1 30-09-2004 US 2005254300 A1 17-11-2005 US 2005256997 A1 17-11-2005 US 2005270843 A1 08-12-2005 US 2009259808 A1 15-10-2009 US 2015153960 A1 04-06-2015