(12) STANDARD PATENT (11) Application No. **AU 2017251920 B2**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Sealing system and method of installing a sealing system

(51) International Patent Classification(s)
G06K 19/073 (2006.01) ***G06K 19/07*** (2006.01)
G06K 7/10 (2006.01) ***G06K 19/077*** (2006.01)

(21) Application No: **2017251920** (22) Date of Filing: **2017.04.13**

(87) WIPO No: **WO17/182398**

(30) Priority Data

(31) Number	(32) Date	(33) Country
16166702.7	**2016.04.22**	**EP**

(43) Publication Date: **2017.10.26**
(44) Accepted Journal Date: **2021.03.25**

(71) Applicant(s)
The European Atomic Energy Community (EURATOM), represented by The European Commission

(72) Inventor(s)
Bergonzi, Claudio;Parnisari, Marco;Littmann, François

(74) Agent / Attorney
Griffith Hack, Level 10 161 Collins St, MELBOURNE, VIC, 3000, AU

(56) Related Art
US 20040239435 A1

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 October 2017 (26.10.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/182398 A1

(51) International Patent Classification:
G06K 19/073 (2006.01) *G06K 19/07* (2006.01)
G06K 19/077 (2006.01) *G06K 7/10* (2006.01)

(21) International Application Number:
PCT/EP2017/059021

(22) International Filing Date:
13 April 2017 (13.04.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16166702.7 22 April 2016 (22.04.2016) EP

(71) Applicant: **THE EUROPEAN ATOMIC ENERGY COMMUNITY (EURATOM), REPRESENTED BY THE EUROPEAN COMMISSION** [BE/BE]; 200, rue de la Loi, 1049 Brussels (BE).

(72) Inventors: **BERGONZI, Claudio**; Via Passo Sentinella 121, 21027 Ispra (IT). **PARNISARI, Marco**; Via Bolzano 5, 21036 Gemonio (IT). **LITTMANN, François**; Contrada Bonè 13, 21034 Cocquio Trevisago (VA) (IT).

(74) Agent: **GEVERS PATENTS**; Intellectual Property House, Holidaystraat 5, 1831 Diegem (BE).

(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, 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,

(54) Title: SEALING SYSTEM AND METHOD OF INSTALLING A SEALING SYSTEM

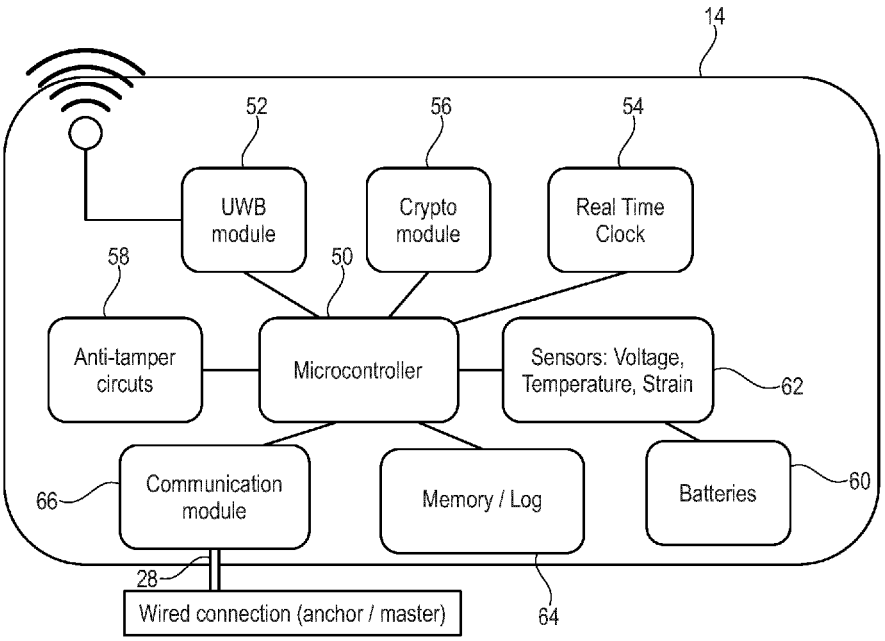


Fig. 2

(57) Abstract: A sealing system for sealing a container lid to a container body e.g. for containing and transporting nuclear waste. The sealing system comprises at least three tags adapted to be mounted to one of the container lid and the container body, each tag having a unique ID and comprising a first RF transceiver configured to transmit, in use, a respective first RF signal. The system comprises at least three anchors adapted to be mounted to the other one of the container lid and the container body, each anchor having a unique ID and comprising a second RF transceiver configured to receive, in use, the first RF signals. A master unit coupled to the tags and anchors is adapted to (i) determine,associated with the ID for each tag, a respective current 3D position, based on the received first RF signals, (ii) store previously determined 3D positions for each tag, and (iii) generate an alert and/or a time stamp and/or a log entry if it determines that separation between the current 3D position of one or more of the tags and a respective previously determined 3D

[Continued on next page]

WO 2017/182398 A1

SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

position is greater than a predetermined distance threshold.

2017251920 15 Feb 2021

SEALING SYSTEM AND METHOD OF INSTALLING A SEALING SYSTEM

Technical field

[0001] The present invention generally relates to sealing systems, in particular for tamper-detection sealing of nuclear containers. With such sealing, a container lid is fixed to a container body and may comprise means for identifying the individual container. The invention further relates to a method of installing a sealing system.

Background Art

[0002] Under some circumstances, the secure sealing of containers is necessary. It is of particular importance if such containers hold dangerous substances, such as fissile materials.

[0003] For example, an inspection agency wishes to verify that a cask (container) containing nuclear spent fuel is transferred between two facilities without being opened. Transport casks are filled at a facility, transferred by truck, rail or boat to another facility and then re-opened.

[0004] The inspector traditionally has access to the casks and lids at three different stages – before they are filled, during transfer and after the cask is opened and emptied.

[0005] It is desirable that casks be filled under surveillance, closed by the operator and sealed by the operator, but no inspector from the agency is required to be present during the filling / closing / sealing operation. The seal applied by the operator must be conceived in a way to (i) avoid intentional/unintentional bad installation that will inhibit/alter the correct function of the seal, (ii) uniquely match cask and lid, (iii) detect an unauthorized opening during transport, (iv) avoid being cloned, and (v) store data and guarantee that the data has not been manipulated.

[0006] Techniques for secure sealing of containers are known, i.e. sealing whereby tampering/opening of the container thereafter is detectable/visible.

2017251920 15 Feb 2021

[0007] Known ways of sealing nuclear containers make use of perforated bolts or other fixtures in combination with wire seals (metal cable or fibre optic loops). All the known systems require the presence of a trusted person (i.e. an inspector) at the time of closing and opening.

[0008] For example, prior solutions involve the use of passive loop seals (like the COBRA seal) or active electronic seals (like EOSS). In each case, a wire or fibre optic is passed through a fixture in the cask and in the lid when the cask is closed. The wire is connected to a seal. In case of the COBRA seal, to open the cask the seal must be broken. In case of the EOSS seal, openings are recorded internally in the seal. A disadvantage is that both previous systems rely on the correct wire installation on the fixtures on the cask. Also, a loose wire may allow the opening of the cask without detection by the seal. Further, the fibre optic wire may be damaged during transport, rendering the seal useless. The COBRA system requires an inspection before the cask is opened (seal broken) because there is no way to determine the time at which the seal was broken.

[0009] Other seals detect displacement by means of contact or magnets, but the methods are not very strong against tampering attempts.

[0010] Even if the existing sealing bolts already seal the containers very securely, there is no known system that fulfils all the requirements, especially the possibility to work unattended without compromising the security of the system.

General Description of the Invention

[0011] The present invention may, in some embodiments, provide a sealing system with improved security features and that is operable whereby a sealing system may be installed by the operator of a storage site without the presence of inspectors, such as those defined in claim 1 or claim 2. The present invention may further, in some embodiments, provide a method of installing a sealing bolt, such as defined in claim 15.

2017251920 15 Feb 2021

[0012] According to one aspect of the invention there is provided a sealing system for sealing a container lid to a container body, said sealing system comprising: at least three tags adapted to be mounted to one of said container lid or said container body, each tag having a unique ID and comprising a first RF transceiver configured to transmit, in use, a respective first RF signal; at least three anchors adapted to be mounted to the other one of said container lid or said container body, each anchor having a unique ID and comprising a second RF transceiver configured to receive, in use, the first RF signals; and a master unit, coupled for communication with the at least three anchors; wherein the master unit is adapted to (i) determine, associated with the ID for each tag, a respective current 3D position, based on the received first RF signals, (ii) store previously determined 3D positions for each tag, and (iii) generate an alert and/or a timestamp and/or a log entry if it determines that separation between the current 3D position of one or more of the tags and a respective previously determined 3D position is greater than a predetermined distance threshold.

[0013] In some embodiments, the master unit may have one of the at least three anchors integrated therein.

[0014] In some embodiments, once the sealing system is placed on the casks and lid by an inspector, the system may be transparent to the operator that will fill and close the casks. The operator may thus not have to perform any operation to install or activate the sealing system, so no mistake (intentional or unintentional) can be made.

[0015] In practical terms, this sealing system may in some embodiments be more secure: it may require less work by the operator, who will not have any extra activity, and may require fewer inspections from the inspectors of the agency, who may also inspect the sealing system at the most convenient time.

[0016] Each of the anchors may be configured for transmitting, periodically or on command from the master unit, a second RF signal, the second RF signal comprising a timing signal.

2017251920 15 Feb 2021

[0017] Each first RF signal may comprise a signal generated at a respective tag in response to the second RF signal and/or including an indication of the time of arrival at the tag of the second RF signal.

[0018] The master unit may be configured for performing temporal averaging of the first RF signal and/or data indicative of the 3D position.

[0019] The master unit may be configured for determining a time point at which the separation between the anchors and the tags has minimised, or stabilised.

[0020] The anchors may be fixedly attached on the container at known locations, for example equally spaced on the circumferential periphery of the container, and the master unit is configured to determine, for each tag, a respective current 3D position based on the known locations.

[0021] The master unit may be configured to determine, for each tag, a respective current 3D position using a triangulation algorithm.

[0022] In some embodiments, each tag and/or each anchor may include a real-time clock, and the first RF signal and/or the second RF signal may incorporate a timestamp derived from a respective real-time clock.

[0023] In some embodiments, each of said anchors may be configured to transmit a combined signal to the master unit, the combined signal comprising a package for each of said at least three tags, each package including the tag ID and time of arrival data. Such transmission may e.g. be performed via a bus.

[0024] In some embodiments, each tag and/or each anchor and/or the master unit may comprise a non-volatile memory (NVM) for storing said 3D positions, in association with respective tag IDs.

[0025] In some embodiments, each tag may include a first cryptographic module configured for generating and storing a first cryptographic key and/or first digital signature, and each tag may be configured for signing said first RF signal using said first cryptographic key or first digital signature prior to transmission to an anchor.

2017251920 15 Feb 2021

[0026] In some embodiments, each anchor tag may include an optional second cryptographic module configured for generating and storing a second cryptographic key and/or second digital signature, and each anchor is configured for (i) signing said second RF signal using said second cryptographic key or second digital signature prior to transmission to a tag; and/or (ii) signing said combined signal using said second cryptographic key or second digital signature prior to transmission to the master unit. The second cryptographic key and/or second digital signature may be generated by the first cryptographic module.

[0027] The digitally signed data may be stored locally or sent remotely by the master, without any risk of data alteration. An intermediate verification of the seal may not be required, since all the events related to the lid closure or opening may be stored and may be retrieved from a signed log in the NVM.

[0028] In some embodiments, each tag and/or each anchor may include a tamper detection sensor configured for generating, in the event of detection thereby of tampering with a housing of a tag or an anchor, tamper detection data indicative of said tampering with the housing.

[0029] In some embodiments, each tag and/or each anchor may include one or more batteries, coupled thereto, a voltage detection sensor configured for generating, in the event of detection thereby of exceptional voltage levels outside a first predetermined range, voltage exception data indicative of tampering with the battery or batteries.

[0030] In some embodiments, each tag and/or each anchor may include a temperature sensor configured for generating, in the event of detection thereby of exceptional temperature levels outside a second predetermined range, temperature exception data indicative of tampering with a tag or an anchor.

[0031] In some embodiments, each tag or anchor may be attached to the container lid or container body, by a rigid tension belt, for example made of steel, plastic or composite, each tag and/or each anchor includes a strain sensor, for example a strain gauge, adapted for sensing strain in the belt, the strain sensor being configured for generating, in the event of detection thereby

2017251920 15 Feb 2021

of exceptional strain levels outside a third predetermined range, strain exception data indicative of tampering with a tag or an anchor.

[0032] The master unit may include a long-range communications module, for example a cellular communications module, and may be configured, in response to the generation of the alert, to (a) generate a cask opened alert, optionally append thereto any data indicative of tampering with the housing, data indicative of tampering with the battery or batteries, temperature exception data and/or strain exception data, and (b) transmit the cask opened alert to a remote control location using the long-range communications module.

[0033] The master unit may be configured, in response to a status request received from a remote control location using the long-range communications module, for transmitting a sealing system status report, the sealing system status report including the timestamp and details of any cask opened alert, and optionally any data indicative of tampering with the housing, data indicative of tampering with the battery or batteries, temperature exception data and/or strain exception data; wherein the sealing system status report is transmitted to the remote control location using the long-range communications module.

[0034] According to another aspect of the invention there is provided a method of installing a sealing system, comprising: providing a sealing system according to any of claims 1 to 14 of the appended claims; mounting the tags and anchors to the container lid and the container body respectively; and initiating the sealing system.

[0035] Further advantages of the invention, at least in some embodiments, may include:

a. Unattended operation. Once the sealing system is applied to the container by an inspector, that status of the container (open/closed) is monitored. All the loading, closing, opening and unloading operations are done by the operator and do not require the presence of an inspector.

b. Simple system for sealing the container.

2017251920 15 Feb 2021

c. High security and with real time information.

d. Minimal exposure of inspectors to radiation.

e. Better time organization afforded, as the inspector is not forced to be physically present at the closure of each individual container, but can concentrate its activities in a short time frame on a batch of containers.

Brief Description of the Drawings

[0036] Further details and advantages of the present invention will be apparent from the following detailed description of several non-limiting embodiments with reference to the attached drawings, wherein:

Fig.1 is a disassembled view of a cask (container), having a sealing system according to a preferred embodiment of the invention mounted thereon;

Fig.2 is a schematic block diagram of a tag or anchor used in the sealing system of Fig.1;

Fig.3 is a schematic block diagram of a master unit used in embodiments of the invention; and

Fig.4 is a flow chart of software/firmware processes carried out in the elements in Fig. 1 according to an embodiment of the invention.

Description of Preferred Embodiments

[0037] The need for a sealing system able to be installed by the operator without the presence of an inspector is of utmost importance and urgency. At least in embodiments, the present invention seeks to provide a sealing system to be applied to nuclear dry storage casks that fulfils one or more of the following requirements:

a. It shall operate automatically, unattended.

b. It shall be used on the lid and body of nuclear containers, without any modification to the container body or lid and without interfering with normal loading/unloading procedures.

2017251920 15 Feb 2021

c. It shall uniquely identify container body and container lid together as a single item (avoiding cloning).

d. It shall be easily installed and removed.

e. It shall detect any opening / closing of the container by removing the lid.

f. It shall detect any attempt to remove the sealing device from the container lid or body.

g. It shall be able to log and digitally sign opening/closing and tampering events.

h. It shall be remotely interrogated for remote/real time control.

i. It shall be self-powered (no need of external power supply) for transport operations.

j. It can be installed by the operator alone and be verified later on, during an inspection, by an inspector who has to trust that the seal has not been tampered in the meantime, meaning that the content of the cask is the same as when it was initially sealed.

k. It can include an anti-tampering enclosure containing the seal and an electronic monitoring device enabling the package to be shipped by the inspectors to the operator, while trusting that it has not been modified before installation.

l. It can allow verification of the identity and integrity of the seal through inspection.

m. It can carry an identity which can be univocally coupled with the container; and

n. It is able to withstand harsh operating conditions.

[0038] In the description and drawings, like numerals are used to designate like elements. Unless indicated otherwise, any individual design feature, component or step may be used in combination with any other design features, components or steps disclosed herein.

2017251920 15 Feb 2021

[0039] Fig.1 illustrates a disassembled view of a cask (container) 10, having a sealing system according to a preferred embodiment of the invention mounted thereon.

[0040] In this embodiment, the sealing system includes three electronic devices of a first type (A1 to A3; herein referred to as “anchors” 14, 16, 18) that are attached to the outer periphery of a container body 12 at its open end 20. The container body 12 is of the type, for example, to be filled with nuclear waste materials or other hazardous waste products. The three anchors 14, 16, 18 are linked and in communication via a wired connection, namely bus 22. In this embodiment, a master unit 24 is linked via a further wired connection 28 to one of the anchors, in this case anchor 14.

[0041] However, in another, preferred, embodiment (not shown), the functionalities and/or componentry of master unit 26 are incorporated into one of the anchors 14, 16, 18, for example anchor 14. This integration provides optimization and simplifies manufacture/setup.

[0042] The anchors 14, 16, 18 are mounted on the container body 12 at known locations, e.g. equally spaced apart around the circumferential periphery of container body 12. Thus, in the case of three anchors 14, 16, 18, these are angularly spaced at 120 degree intervals. It will be appreciated, however, that four or more anchors 14, 16, 18 may be used around the periphery of container body 12, so that in the case of four anchors, these are angularly spaced at 90 degree intervals, and so on.

[0043] In a preferred embodiment, the three anchors 14, 16, 18 are fixed to the container body 12 by a rigid tension belt (not shown), to prevent unauthorized removal.

[0044] The sealing system according to this embodiment of the invention also includes, mounted on lid 13 of the container 10, three electronic devices of a second type (T1, T2, T3; herein referred to as “tags” 30, 32, 34).

[0045] In a preferred embodiment, the three tags 30, 32, 34 are fixed to the container lid 13 by a rigid tension belt (not shown). In the case that three tags 30, 32, 34 are present, these are angularly spaced at c. 120 degree intervals. It

2017251920 15 Feb 2021

will be appreciated, however, that four or more tags 30, 32, 34 may be used around the periphery of container lid 13, so that in the case of four anchors, these are angularly spaced at c. 90 degree intervals, and so on.

[0046] Generally, the use of more tags and anchors can increase the precision.

[0047] In use, the sealing system comprising the anchors 14, 16, 18 and the tags 30, 32, 34, as well as master unit 26, is fixed to the container 10 prior to filling the container body 12. The filling and sealing of the container does not require the presence of an inspector.

[0048] In accordance with embodiments of the invention, the anchors 14, 16, 18 and the tags 30, 32, 34 communicate with each other using Ultra Wide Band (UWB) radio frequency (RF) signals in order to determine device separation distances and/or positions in 3 dimensions (3D), as discussed in detail below. While, in this embodiment, UWB RF transceivers are used, it will be appreciated that non-UWB RF techniques may be employed.

[0049] Figure 2 shows a schematic block diagram anchor 14 used in the sealing system of Fig.1. (The tags 30, 32, 34 are similar devices to anchors 14, 16, 18 and share the same architecture, but are programmed differently, e.g. in firmware. For the sake of brevity, only the architecture of anchor 14 is discussed here; the tags 30, 32, 34 and anchors 16, 18 are constructed similarly. As used herein, “device” may refer to each of tags 30, 32, 34, to each of anchors 14, 16, 18, or to any or all of these.)

[0050] The core of the device is a low power microcontroller 50, to manage all the information of the different subsystems of the device and to coordinate all the communications with other devices, including the master unit 26. The RF (e.g. UWB) ranging – to determine the relative 3D position of at least each of the tags 30, 32, 34 – is accomplished through a dedicated UWB module 52 that transmits and receives data packages (including time of flight (ToF) data) and timestamps, the latter being provided by real-time clock (RTC) 54. Real-time clock 54 is preferably a precise real time clock that keeps track of time for precise time-stamping of data (packages) / RF messages.

2017251920 15 Feb 2021

[0051] The anchor 14 also contains a cryptographic module 56 (crypto-chip) that can generate and store cryptographic keys to digitally sign the data (packages) before being transmitted. That is, each tag and anchor is equipped with a cryptographic module 56 with a unique ID and its own unique private key, to avoid cloning. Keys are generated and stored in the crypto chip inside the device, for maximum protection. All the communications between the devices are digitally signed with an asymmetric algorithm for authentication.

[0052] An anti-tamper sensor 58 detects if the anchor 14 is removed from its position on the container. The sensor 58 may be in the form of tamper detection switches on the case/housing (not shown) of the devices, and a protective circuit mesh (not shown) to avoid drilling into the case/housing.

[0053] The anchor 14 is powered by one or more batteries 60 (preferably a dual battery system), and is provided with a set of sensors 62 to monitor voltage and temperature to ensure the correct functioning and detect tamper attacks. The temperature sensor is used to detect extreme temperatures that may alter the functioning of the seal. Through the use of the temperature sensor, processor 50 is able to determine whether the current temperature is within a predetermined operational range, and/or generate an alert/exception (message) when the sensed temperature is outside that predetermined operational range.

[0054] The on-board voltage monitoring sensor (circuit) ensures the correct power supply to the device. The voltage monitoring sensor is used to detect exceptional voltages output by battery 60 that may alter the functioning of the seal. Through the use of the voltage monitoring sensor, processor 50 is able to determine whether the current voltage output is within a predetermined operational range, and/or generate an alert/exception (message) when the sensed voltage output is outside that predetermined operational range.

[0055] The device also has a strain sensor (e.g. a strain gauge or similar sensor) to check or monitor the tension of the fixing belt (not shown) used to fixedly attach the anchors 14, 16, 18 to the container body and/or to attach the tags 30, 32, 34 to the container lid 13. The strain sensor is used to detect exceptional levels of strain in the fixing belt (not shown) that may be indicative

2017251920 15 Feb 2021

of an attempt to remove the belt of devices (i.e. tampering). Through the use of the strain gauge sensor, processor 50 is able to determine whether the current level of strain is within a predetermined operational range, and/or generate an alert/exception (message) when the sensed level of strain is outside that predetermined operational range.

[0056] The anchor 14 keeps a log of all detected events, and/or all sensor data, in an internal non-volatile memory (NVM) 64. Data stored in NVM 64 is preferably time-stamped using a precise timestamp from RTC 54.

[0057] Finally, the anchor 14 communicates with the master unit (26; Fig. 1) through a wired communication link 28 (such as a serial or parallel link) using communication module 66.

[0058] Figure 3 is a schematic block diagram of a master unit 26 used in embodiments of the invention. This is identical to the anchor 14 of Fig. 2, except as described in the following. The master unit 26 acts as a control unit for the sealing system.

[0059] In the master unit 26 of Fig. 3, a communication module 66', identical to the communication module 66 of anchor 14 and operating on the same protocol, e.g. serial or parallel, is included, for communication with the anchor 14 via wired communication link 28. In addition, the master unit 26 includes a long-range communications module 70, for communication to and from a remote central control station (not shown), e.g. belonging to a nuclear safety agency. The long-range communications module 70 may be a cellular communications module 70, e.g. GSM, 3G, 4G, 5G/LTE or the like.

[0060] In use, anchors 14, 16, 18 initiate the communication with the tags 30, 32, 34, i.e. each anchor 14, 16, 18 has a communication exchange with each of the tags 30, 32, 34. Once the container lid 13 with three tags is positioned close to a container body 12 with three anchors 14, 16, 18, the container body 12 and lid 13 are effectively paired, and any relative movement of the lid 13 with respect to the container body 12 will be detected, including lifting and or rotation.

2017251920 15 Feb 2021

[0061] Anchors 14, 16, 18 and tags 30, 32, 34 exchange data packages containing timing information. These packages are digitally signed, using cryptographic module 56 to avoid counterfeits. The master unit 26 collects all these data packages and calculates the time of flight of signals between anchors 14, 16, 18 and tags 30, 32, 34, and subsequently, through a triangulation algorithm, their relative (3D) positions. Sensors inside anchors 14, 16, 18 and tags 30, 32, 34 can detect if the device is removed from its position on the container 12. As discussed in more detail below, any attempt to lift the lid 13 is detected by the system and logged.

[0062] As discussed in more detail hereinafter, through the exchange of messages and consequent ranging/positioning, the devices (anchors 14, 16, 18 and tags 30, 32, 34) are “aware” of their respective position in 3D space and behave like a unique seal, i.e. unique to this container body 12 and lid 13 pairing. This “network” of 3D localized seal devices allows a precise detection of movement (of the devices, and therefore of lid 13, relative to container body 12), e.g. to an accuracy of about 5 to 15 cm.

[0063] In operation, each of the three anchors 14, 16, 18 interrogates the three tags 30, 32, 34. Each anchor 14, 16, 18 can determine at which distance the tags 30, 32, 34 are positioned, using time of flight information. The three anchors 14, 16, 18 are placed around the container body 12 in a plane parallel to the surface of the container lid 13, preferably at 120 degrees angular separation round the circumference of the container body 12. Anchors 14, 16, 18 and tags 30, 32, 34 exchange messages to determine the time of flight. These messages are digitally signed, to prevent any other fake tag from impersonating a legitimate one. All the anchors 14, 16, 18 provide the distance information to the master unit 26 over the wired communication channel 28. The master unit 26 collects all the authenticated information and, through a triangulation algorithm, determines the 3D position of each tag 30, 32, 34.

[0064] As the position of the three anchors 14, 16, 18 on the container body 12 is fixed and known, the position of the tags 30, 32, 34 can be determined by the master unit 26 therefrom. Three anchors 14, 16, 18 and three tags 30, 32,

2017251920 15 Feb 2021

34 is the minimum number to ensure a good 3D positioning. Four anchors 14, 16, 18 and four tags 30, 32, 34 may increase the precision of the 3D positioning, but at added cost/complexity.

[0065] Once the lid 13 is placed over the container body 12, the master unit logs the proximity of the three tags 30, 32, 34 connected to the lid 13. Any change to the position of each tag (or change greater than a threshold distance [threshold 1], e.g. lying in the range of 0.1 to 15 cm, preferably 0.1 to 5 cm, more preferably 0.1 to 1 cm) is considered as an opening of the lid. An algorithm processes the position/distance changes relative to the detection threshold(s) and may average the position/distance overtime to avoid false alarms.

[0066] Figure 4 is a flow chart of software/firmware processes carried out in the elements in Fig. 1 according to an embodiment of the invention. That is, there are illustrated the steps or processes implemented at each tag 14, 16, 18, at each anchor 30, 32, 34, and at the master unit 26, in carrying out monitoring, detection of tampering with or opening of the cask (container) 10, and alerting. (For brevity, the process is described in relation to a single tag 30 and a single anchor 14; the process for the other tags and anchors is similar.)

[0067] Referring to the left hand column (tag) in Fig. 4, each tag 30, 32, 34 has its own unique identifier (ID), and using cryptographic module 56, tag 30 operates to generate a signature from the stored cryptographic key and tag ID (step s402). The tag 30 then listens for messages received via RF (step s404). At step s406, if no message is received, tag 30 continues to listen for messages received. If, at step s406, it is found that an RF message has been received, a check is made (step s408) as to whether it is recognisable as an initiation message from an anchor 14. At step s408, if no initiation message has been received, tag 30 continues to listen for messages received (s404).

[0068] Referring briefly to the central column in Fig. 4, each anchor 14, 16, 18 has its own unique identifier (ID), and using cryptographic module 56, anchor 14 operates to generate a signature from the stored cryptographic key and tag ID (step s430). Either periodically according to a preset periodicity using the

2017251920 15 Feb 2021

real-time clock, or on command from the master unit 26, anchor 14 broadcasts (step s432) an initiation message to tags 30, 32, 34 in the vicinity, using UWB RF, the initiation message being designed to prepare tags 30, 32, 34 for 2-way communication and a 3D position determination operation.

[0069] As seen in the left hand column in Fig. 4, if, at step s408, it is found that initiation message has been received, tag 30 initiates (step s410) all sensors 58, 62 and communications modules 52, 66. The tag 30 then listens for a timing message via UWB RF. If, at step s412, it is found that no timing message has been received, tag 30 continues to listen for messages received (s404).

[0070] Following transmission of the initiation message by the anchor 14, and as seen in the central column in Fig. 4, e.g. a predetermined period thereafter, the anchor 14 broadcasts (s434) a timing message.

[0071] Returning to the left hand column in Fig. 4, if, at step s412, it is found that a timing message has been received from anchor 14, tag 30 determines (step s414) the time of arrival (ToA) of the timing signal using real-time clock 54 and timestamps the ToA based on the reading of the real-time clock 54. The ToA can subsequently be used to determine time of flight (ToF) from anchor 14 to tag 30.

[0072] Next, at step s416, a data package containing the ID of tag 30 and the ToA are digitally signed using the generated signature for the tag 30. The signed data package is then broadcast by the tag 30 at step s418.

[0073] A check is then made (step s420) in case a Terminate command has been received from the master unit 26 (e.g. via an anchor 14), indicating the RF transmissions or processing is to terminate; and if so, the process at tag 30 ends. If no Terminate command has been received, processing returns to step s404.

[0074] At the anchor 14 (see central column in Fig. 4), after transmission of the timing message by the anchor 14, a delay timer is initiated (step s436), the delay being designed to permit reception of responses from tags 30, 32, 34 to the timing signal.

2017251920 15 Feb 2021

[0075] A check is made (step s438) as to whether the delay has elapsed; and, if so, processing returns to step s432, where anchor 14 (re)broadcasts an initiation message to tags 30, 32, 34 in the vicinity.

[0076] If the delay has not elapsed, a determination is made (step s440) as to whether data packages (responses to the timing signal) for all tags 30, 32, 34 have been received by the anchor 14. If not, processing returns to step s438.

[0077] If it is determined (step s440) that data packages for all tags 30, 32, 34 have been received, the signed data packages are decrypted (s442) to derive ToA and ID for Tag 30. In this case (3 tags), the 3 data packages (Tag IDs + ToAs) are compiled into combination package at step s444.

[0078] Then, at step s446, the combination package is signed using the signature of anchor 14. Next, the combination package is sent (step s448) to the master unit 26 as a signed data package.

[0079] A check is then made (step s450) in case a Terminate command has been received from the master unit 26, indicating the RF transmissions or processing is to terminate; and if so, the process at anchor 14 ends. If no Terminate command has been received, processing returns to step s432.

[0080] Referring to the right hand column in Fig. 4, following the communication (step s448) of the combination package to master unit 26, as signed data package, and the determination (step s460) that the combination package has been received, the signed combination package is decrypted (step s462).

[0081] Next, based on the decrypted packages for each tag 30, 32, 34, the ToA and ID for each tag is derived (step s464); the ToF for each tag is derivable from the ToAs, as will be known to persons skilled in the art. For example, the timing message may comprise a precise timestamp indicating time of sending. The tag 30 applies a precise timestamp to the received timing message, indicating ToA. The tag 30 may calculate ToF = timestamp(arrival) - timestamp(sending), and include this in the data package broadcast to the anchor 14. More preferably, the tag 30 broadcast the ToA (timestamp), together with either the precise timestamp indicating time of sending, from the timing

2017251920 15 Feb 2021

message, or an identifier of the timing message, from which the precise timestamp indicating time of sending can be obtained at the anchor 14 or master unit 26, thus enabling determination at the anchor 14 or master unit 26 of ToF (timing message) = timestamp(arrival) - timestamp(sending).

[0082] Then, for each tag, its current 3D position is determined (step s466) from known locations of anchors 14, 16, 18 and the derived ToAs and IDs, using triangulation algorithm.

[0083] Once the current 3D position is determined, then, for each tag, its current 3D position is compared (step s468) with the previously determined 3D position for that tag (stored in NVM 64; Fig. 2). A check is then made (step s470) as to whether the magnitude of the separation of current and previously determined 3D positions is greater than a first threshold (threshold1).

[0084] If the magnitude of the separation is not greater than the first threshold, the determined current 3D position for each tag is stored (step s472) in NVM 64.

[0085] If, on the other hand, the magnitude of the separation is greater than the first threshold, indicating that substantial movement of the lid 13 relative to the container 12 (Fig. 1) corresponding to an act of tampering or (attempted) opening has occurred, the master unit generates (step s474) a “Cask opened” alert (message), including timestamp of opening; the alert is logged in NVM 64.

[0086] As seen at step s476, optionally a check is made for any tag/device tampering, temperature, voltage or strain sensor exception data, i.e. from sensors 58, 62, respectively, and optionally this data is appended (step s478) to “Cask opened” alert (message).

[0087] The three anchors 14 are fixed on the container body 12 using a rigid tension belt (not shown) under tension. Each anchor 14, 16, 18 can monitor the tension of the belt. In case of an attempt to remove the system from the cask 10, the tension from the belt is released, and the master unit 26 detects the tampering, generating the strain gauge exception data. A similar detection system is in place on the belt (not shown) that fixes the three tags 30, 32, 34 to

2017251920 15 Feb 2021

the lid 13. Similar appending action is performed in the event of tag/device tampering, temperature, or voltage level exception data.

[0088] Then, at step s480, the "Cask opened" alert (message) is sent to remote central control (not shown) via a cellular network, e.g. GSM, 3G, 4G etc., using communications module 70 (Fig. 3) of master unit 26.

[0089] The master unit 26 is configured to be interrogated by an inspector with a suitable reader (not shown), e.g. via wired (serial/parallel) device port, or by short-range wireless communication, such as Bluetooth®. Alternatively or additionally, master unit 26 is provided with a remote communication module 70 that uses existing telecom infrastructure (i.e. GSM, GPRS, 3G or other system), allowing a remote interrogation of master unit 26, e.g. to obtain status data, logs and/or tampering reports/alerts. Such data may be securely communicated to a remote location/station in digitally signed form using the unique cryptographic key and the cryptographic module 56 of master unit 26.

[0090] The duty of the inspector (e.g. from a nuclear inspection agency) is to check that the initial installation of the fixing belt (not shown) of anchors 14, 16, 18 and tags 30, 32, 34 is correct. This meets the requirement that sealing system 10 shall be installed by a trusted person (an inspector) on the container some time before the container is loaded. This is a simple operation and can be done on a batch of containers at the most convenient time in a non-restricted area where exposure to radiation is minimal or absent. This is the only operation that requires the presence of an inspector. That is, all other operations may be unattended (by the inspector).

[0091] The sealing system 10, once in place, is autonomous. Once a lid 13 is placed close to a container body 12, the sealing system 10 detects the lid 13 and pairs it to the container body 12. Everything is automatic and wireless, and no wiring or any mechanical operation is needed. This means that the container is loaded and closed by the nuclear power plant operator without the presence of an inspector.

[0092] Moreover, the sealing system 10 can be remotely interrogated to check its status and access the internal log. Once the container is opened and

2017251920 15 Feb 2021

emptied, the sealing system 10 can be removed from the container and sent back to the inspectors to be reused.

[0093] While embodiments have been described by reference to embodiments having various components in their respective implementations, it will be appreciated that other embodiments make use of other combinations and permutations of these and other components.

[0094] Furthermore, some of the embodiments are described herein as a method or combination of elements of a method that can be implemented by a processor of a computer system or by other means of carrying out the function. Thus, a processor with the necessary instructions for carrying out such a method or element of a method forms a means for carrying out the method or element of a method. Furthermore, an element described herein of an apparatus embodiment is an example of a means for carrying out the function performed by the element for the purpose of carrying out the invention.

[0095] In the description provided herein, numerous specific details are set forth. However, it is understood that embodiments of the invention may be practiced without these specific details. In other instances, well-known methods, structures and techniques have not been shown in detail in order not to obscure an understanding of this description.

[0096] Thus, while there has been described what are believed to be the preferred embodiments of the invention, those skilled in the art will recognize that other and further modifications may be made thereto without departing from the scope of the invention, and it is intended to claim all such changes and modifications as falling within the scope of the invention. For example, any formulas given above are merely representative of procedures that may be used. Functionality may be added or deleted from the block diagrams and operations may be interchanged among functional blocks. Steps may be added or deleted to methods described within the scope of the present invention.

[0097] In the claims which follow and in the preceding description of the invention, except where the context requires otherwise due to express language or necessary implication, the word “comprise” or variations such as “comprises”

2017251920 15 Feb 2021

or “comprising” is used in an inclusive sense, i.e. to specify the presence of the stated features but not to preclude the presence or addition of further features in various embodiments of the invention.

[0098] It is to be understood that, if any prior art publication is referred to herein, such reference does not constitute an admission that the publication forms a part of the common general knowledge in the art, in Australia or any other country.

2017251920 15 Feb 2021

Legend:

10	sealing system	50	processor
12	container body	52	UWB RF module
13	container lid	54	real-time clock
14	anchor	56	cryptographic module
16	anchor	58	anti-tamper sensor
18	anchor	60	battery
20	open end	62	voltage, temperature and strain sensors
22	bus		
26	master unit	64	NVM
28	wire link	66	wired communications module
30	tag		
32	tag	70	cellular communications module
34	tag		

2017251920 15 Feb 2021

Claims

1. Sealing system for nuclear containers, sealing a container lid of a nuclear container to a container body of said nuclear container, said sealing system comprising:

   at least three tags adapted to be mounted to one of said container lid or said container body, each tag having a unique ID and comprising a first RF transceiver configured to transmit, in use, a respective first RF signal;

   at least three anchors adapted to be mounted to the other one of said container lid or said container body, each anchor having a unique ID and comprising a second RF transceiver configured to receive, in use, the first RF signals; and

   a master unit, coupled for communication with the at least three anchors;

   wherein the master unit is adapted to

   (i) determine, associated with the ID for each tag, a respective current 3D position, based on the received first RF signals,

   (ii) store previously determined 3D positions for each tag, and

   (iii) generate an alert and/or a timestamp and/or a log entry if it determines that separation between the current 3D position of one or more of the tags and a respective previously determined 3D position is greater than a predetermined distance threshold.

2. Sealing system according to claim 1, wherein said master unit has one of said at least three anchors integrated therein.

3. Sealing system according to claim 1 or 2, wherein each of the anchors is configured for transmitting, periodically or on command from the master unit, a second RF signal, the second RF signal comprising a timing signal.

4. Sealing system according to claim 1, 2 or 3, wherein each first RF signal comprises a signal generated at a respective tag in response to the second

2017251920 15 Feb 2021

RF signal and/or including an indication of the time of arrival at the tag of the second RF signal.

5. Sealing system according to any of the preceding claims, wherein the master unit is configured for performing temporal averaging of the first RF signal and/or data indicative of the 3D position.

6. Sealing system according to any of the preceding claims, wherein the master unit is configured for determining a time point at which the separation between the anchors and the tags has minimised, or stabilised.

7. Sealing system according to any of the preceding claims, wherein the anchors are fixedly attached on the container body or container lid at known locations, for example equally spaced on the circumferential periphery of the container body or container lid, and the master unit is configured to determine, for each tag, a respective current 3D position based on the known locations.

8. Sealing system according to any of the preceding claims, wherein the master unit is configured to determine, for each tag, a respective current 3D position using a triangulation algorithm.

9. Sealing system according to any of the preceding claims, wherein each tag and/or each anchor includes a real-time clock, and the first RF signal and/or the second RF signal incorporates a timestamp derived from a respective real-time clock.

10. Sealing system according to any of the preceding claims, wherein each of said anchors is configured to transmit a combined signal to the master unit via a bus, the combined signal comprising a package for each of said at least three tags, each package including the tag ID and time of arrival data.

2017251920 15 Feb 2021

11. Sealing system according to any of the preceding claims, wherein each tag and/or each anchor and/or the master unit comprises a non-volatile memory for storing said 3D positions, in association with respective tag IDs.

12. Sealing system according to any of the preceding claims wherein

(i) each tag includes a first cryptographic module configured for generating and storing a first cryptographic key and/or first digital signature, and each tag is configured for signing said first RF signal using said first cryptographic key or first digital signature prior to transmission to an anchor; and/or

(ii) each anchor includes an optional second cryptographic module configured for generating and storing a second cryptographic key and/or second digital signature, and each anchor is configured for:

a. signing said second RF signal using said second cryptographic key or second digital signature prior to transmission to a tag; and/or

b. signing said combined signal using said second cryptographic key or second digital signature prior to transmission to the master unit.

13. Sealing system according to any of the preceding claims, wherein

(i) each tag and/or each anchor includes a tamper detection sensor configured for generating, in the event of detection thereby of tampering with a housing of a tag or an anchor, tamper detection data indicative of said tampering with the housing; and/or

(ii) each tag and/or each anchor includes one or more batteries, coupled thereto, a voltage detection sensor configured for generating, in the event of detection thereby of exceptional voltage levels outside a first predetermined range, voltage exception data indicative of tampering with the battery or batteries; and/or

(iii) each tag and/or each anchor includes a temperature sensor configured for generating, in the event of detection thereby of exceptional temperature levels outside a second predetermined

2017251920 15 Feb 2021

range, temperature exception data indicative of tampering with a tag or an anchor; and/or

(iv) each tag and/or each anchor is attached to the container lid or the container body, by a rigid tension belt, for example a steel belt, each tag and/or each anchor includes a strain sensor, for example a strain gauge, adapted for sensing strain in the belt, the strain sensor being configured for generating, in the event of detection thereby of exceptional strain levels outside a third predetermined range, strain exception data indicative of tampering with a tag or an anchor.

14. Sealing system according to any of the preceding claims, wherein the master unit includes a long-range communications module, for example a cellular communications module, and is configured

(i) in response to the generation of the alert, to

a. generate a cask opened alert, optionally append thereto any data indicative of tampering with the housing, data indicative of tampering with the battery or batteries, temperature exception data and/or strain exception data, and

b. transmit the cask opened alert to a remote control location using the long-range communications module, and/or

(ii)in response to a status request received from a remote control location using the long-range communications module, to transmit a sealing system status report, the sealing system status report including the timestamp and details of any cask opened alert, and optionally any data indicative of tampering with the housing, data indicative of tampering with the battery or batteries, temperature exception data and/or strain exception data; wherein the sealing system status report is transmitted to the remote control location using the long-range communications module.

15. A method of installing a sealing system, comprising:

providing a sealing system according to any of claims 1 to 14;

2017251920 15 Feb 2021

mounting the at least three tags to the container lid;

mounting the at least three anchors, or the at least two anchors and the master unit, to the container body; and

initiating the sealing system.

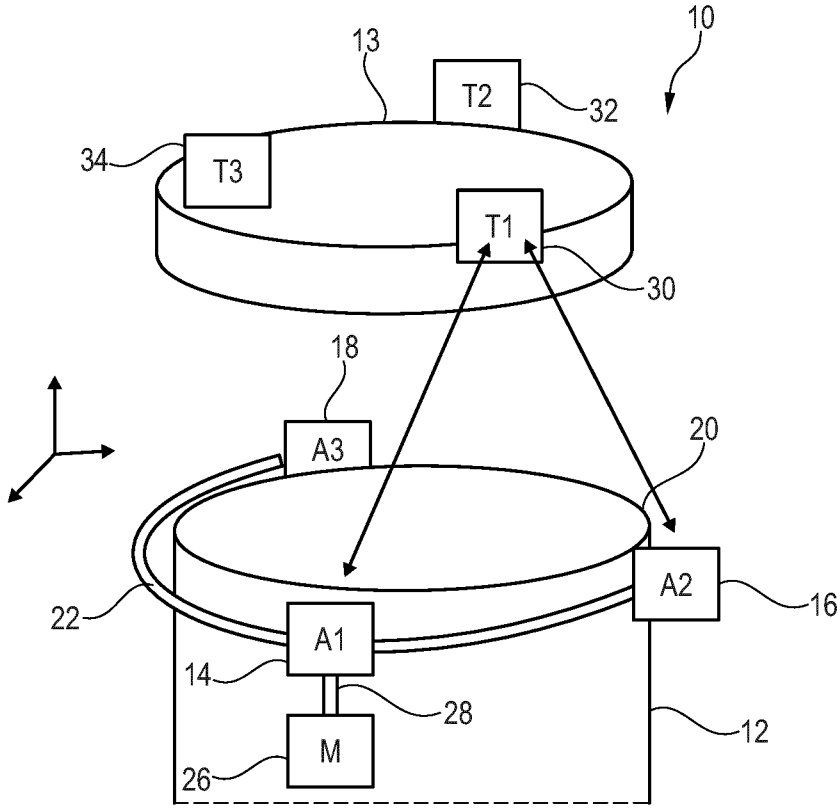

10
13
T2
32
34
T3
T1
30
18
A3
20
A2
16
22
A1
14
28
12
M
26

Fig. 1

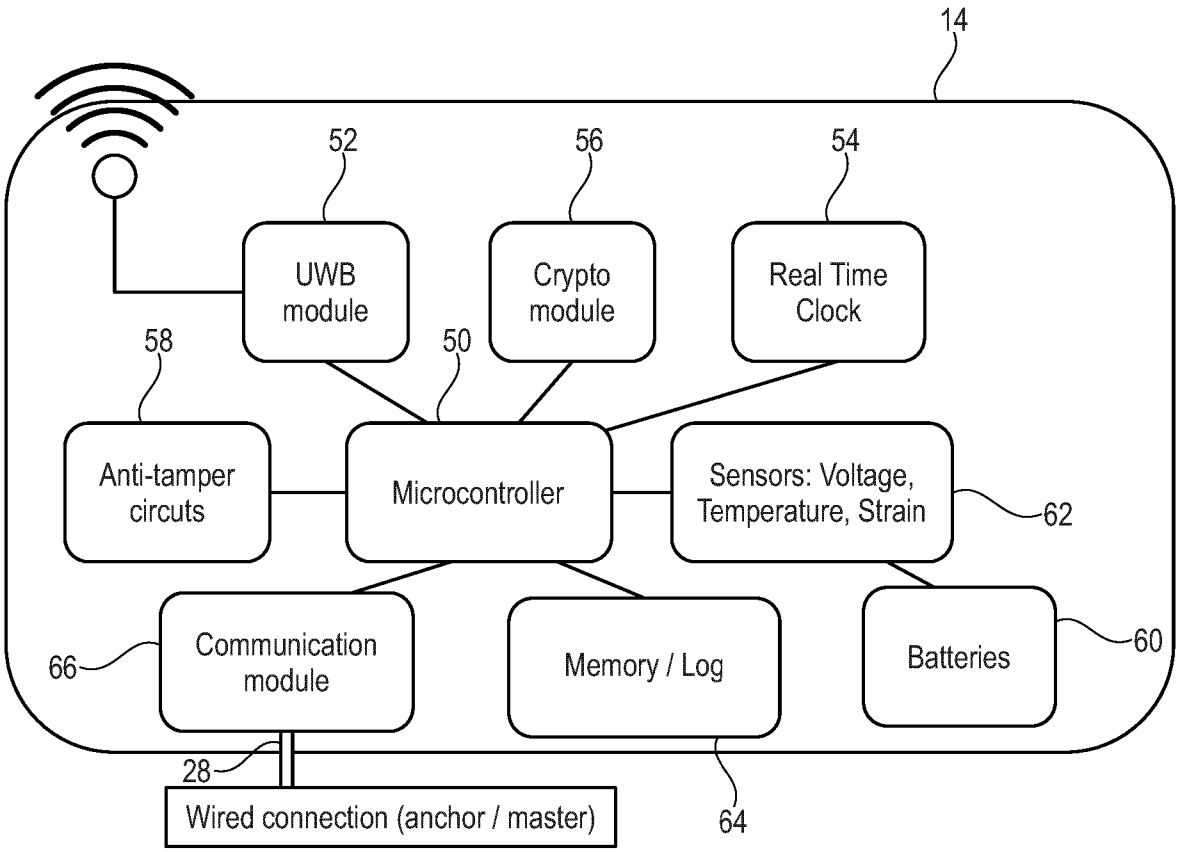

14
52
56
54
UWB module
Crypto module
Real Time Clock
58
50
Anti-tamper circuts
Microcontroller
Sensors: Voltage, Temperature, Strain
62
66
Communication module
Memory / Log
Batteries
60
28
Wired connection (anchor / master)
64

Fig. 2

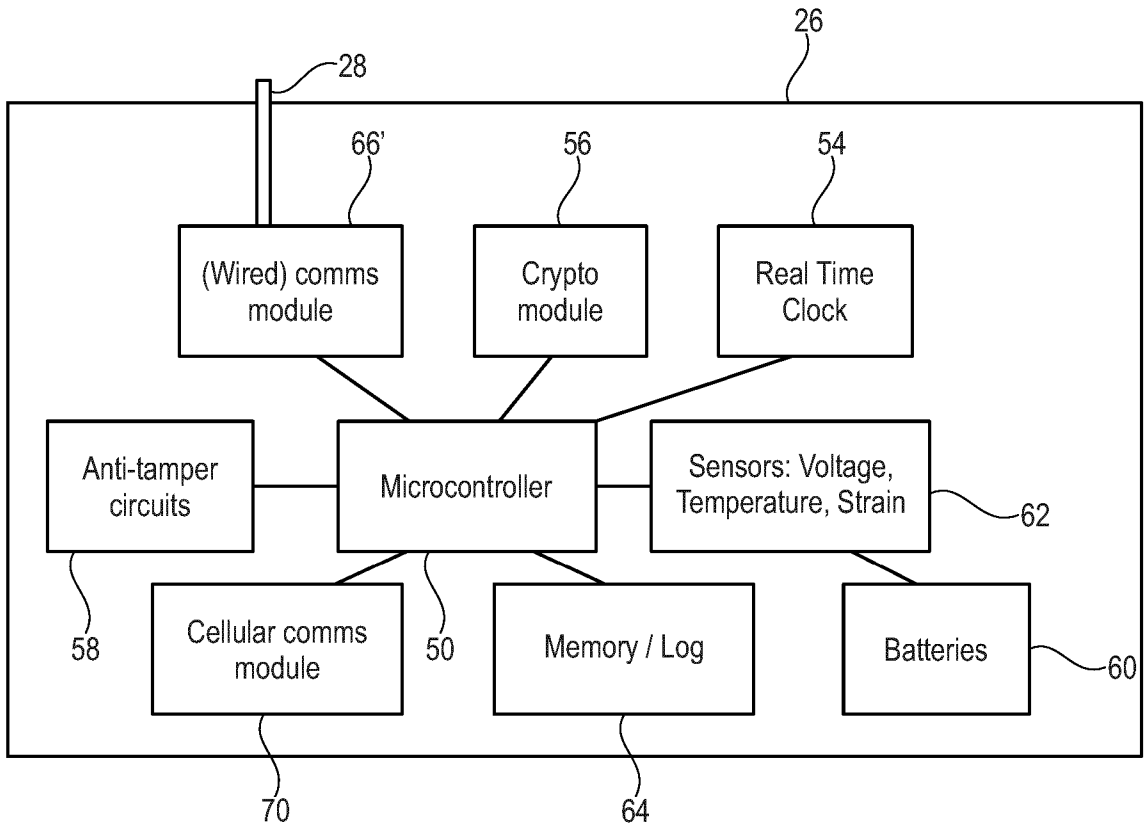

26
28
66'
56
54
(Wired) comms module
Crypto module
Real Time Clock
Anti-tamper circuits
Microcontroller
Sensors: Voltage, Temperature, Strain
62
58
Cellular comms module
50
Memory / Log
Batteries
60
70
64

Fig. 3

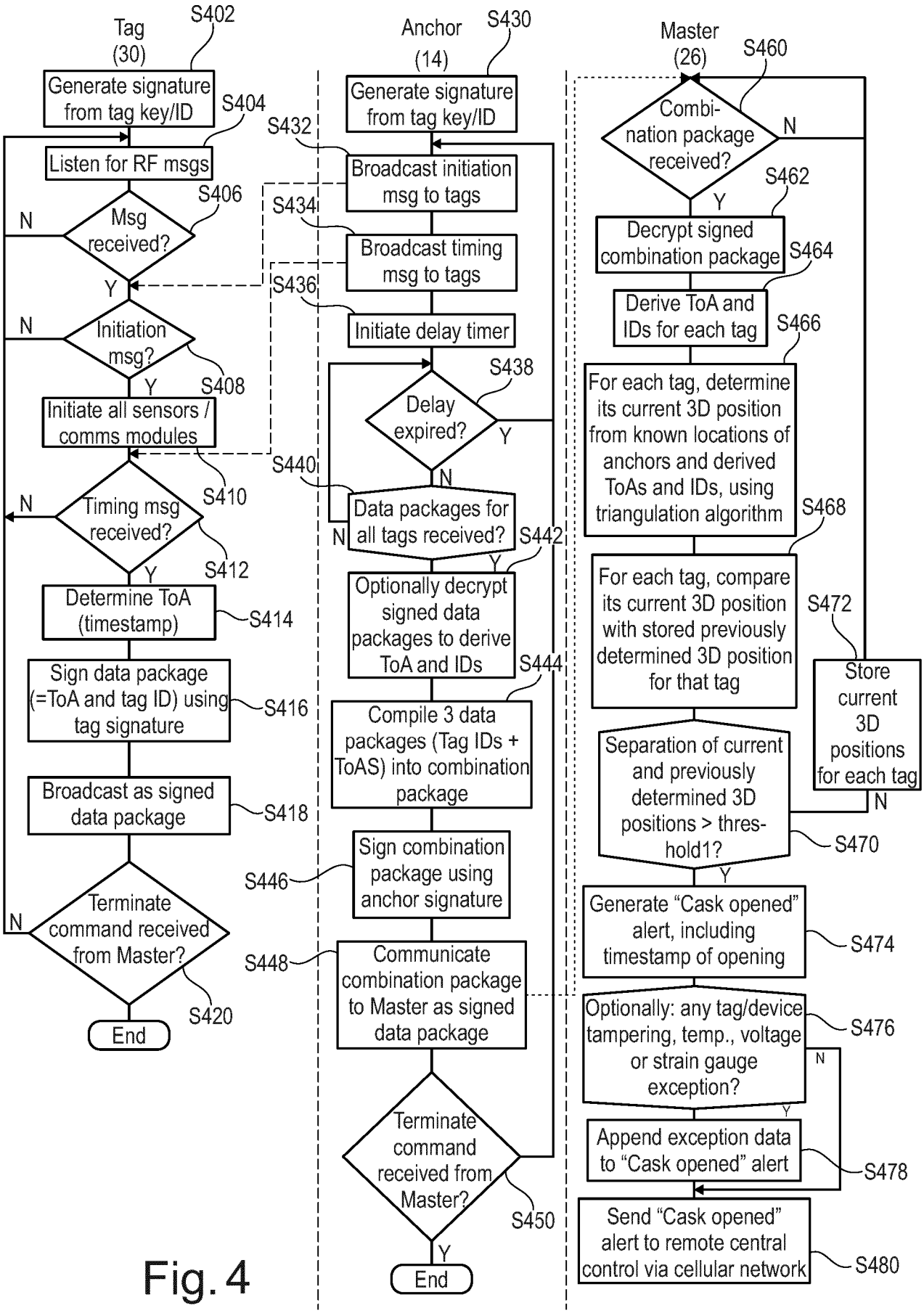

Tag (30)
S402
Generate signature from tag key/ID
S404
Listen for RF msgs
S406
Msg received?
N
Y
S408
Initiation msg?
N
Y
Initiate all sensors / comms modules
S410
Timing msg received?
N
Y
S412
Determine ToA (timestamp)
S414
Sign data package (=ToA and tag ID) using tag signature
S416
Broadcast as signed data package
S418
Terminate command received from Master?
N
S420
End
Anchor (14)
S430
Generate signature from tag key/ID
S432
Broadcast initiation msg to tags
S434
Broadcast timing msg to tags
S436
Initiate delay timer
S438
Delay expired?
Y
N
S440
Data packages for all tags received?
N
S442
Y
Optionally decrypt signed data packages to derive ToA and IDs
S444
Compile 3 data packages (Tag IDs + ToAS) into combination package
S446
Sign combination package using anchor signature
S448
Communicate combination package to Master as signed data package
Terminate command received from Master?
S450
Y
End
Master (26)
S460
Combi-nation package received?
N
Y
S462
Decrypt signed combination package
S464
Derive ToA and IDs for each tag
S466
For each tag, determine its current 3D position from known locations of anchors and derived ToAs and IDs, using triangulation algorithm
S468
For each tag, compare its current 3D position with stored previously determined 3D position for that tag
S472
Store current 3D positions for each tag
N
Separation of current and previously determined 3D positions > thres-hold1?
S470
Y
Generate “Cask opened” alert, including timestamp of opening
S474
Optionally: any tag/device tampering, temp., voltage or strain gauge exception?
S476
N
Y
Append exception data to “Cask opened” alert
S478
Send “Cask opened” alert to remote central control via cellular network
S480

Fig. 4