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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 May 2014 (15.05.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/071465 A1

(51) International Patent Classification:
G06F 19/00 (2011.01)

(21) International Application Number:
PCT/AU2013/001303

(22) International Filing Date:
12 November 2013 (12.11.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2012904989 12 November 2012 (12.11.2012) AU
2013204965 12 April 2013 (12.04.2013) AU

(71) Applicant: **C2 SYSTEMS LIMITED** [CN/CN]; c/o Marks & Clerk Hong Kong, Level 9, Cyberport 1, 100 Cyberport Road, Pok Fu Lam, Hong Kong (CN).

(72) Inventor; and
(71) Applicant : **STORR, James Robert** [AU/AU]; c/o Wrays Pty Ltd, Ground Floor, 56 Ord Street, West Perth, Western Australia 6005 (AU).

(74) Agent: **WRAYS PTY LTD**; Ground Floor, 56 Ord Street, West Perth, Western Australia 6005 (AU).

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

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

Published:

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

(54) **Title**: A SYSTEM, METHOD, COMPUTER PROGRAM AND DATA SIGNAL FOR THE REGISTRATION, MONITORING AND CONTROL OF MACHINES AND DEVICES

(57) **Abstract**: The present invention provides a method for controlling a robotic device, comprising the steps of, receiving at a computing device at least one command arranged to effect an operation on the robotic device, reviewing the command to determine whether the command is suitable for execution, wherein the command is provided to the device only if the command is suitable for execution.

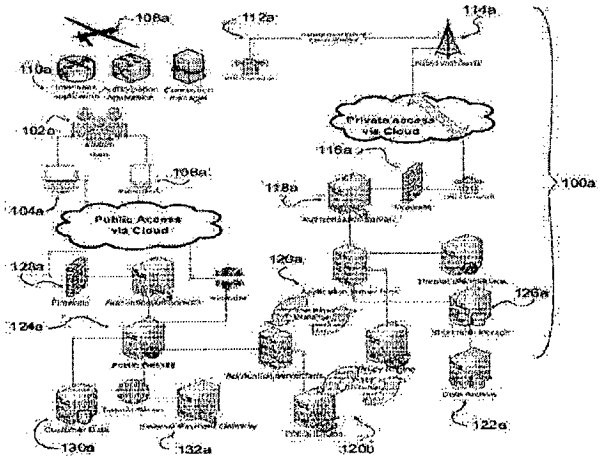


Figure 2

WO 2014/071465 A1

A SYSTEM, METHOD, COMPUTER PROGRAM AND DATA SIGNAL FOR THE REGISTRATION, MONITORING AND CONTROL OF MACHINES AND DEVICES

Technical Field

[0001] The present invention relates to a system, method, computer program and data signal for the registration, monitoring and control of machines and devices. Embodiments of the invention find specific, but not exclusive, use in the registration, monitoring and control of robotic devices, autonomous vehicles, "smart" devices, and other programmable and computer controlled devices.

Background Art

[0002] The following discussion of the background art is intended to facilitate an understanding of the present invention only. The discussion is not an acknowledgement or admission that any of the material referred to is or was part of the common general knowledge as at the priority date of the application.

[0003] Science fiction predicted the eventual development of robotic devices and "smart" devices which are arranged to autonomously perform one or more functions. In the past, due to limitations in computing power and the ability to create reliable, cost-effective electronics, robotic devices have largely been used in very specialized applications (such as in manufacturing applications) or as "show-pieces" (e.g. the development of ASIMO, a humanoid robot developed by Honda Corporation).

[0004] However, the explosion in and frenzied development of telecommunications and computing technology (such as the development of cell phone technology, the Internet, wireless Internet, the release of Global Positioning System technology for consumer use and minituarised computing technology) now provides a platform for the development and creation of consumer robots.

[0005] For example, robot vacuum cleaners, small remote controlled robotic devices (e.g. helicopters and multicopters) and the more recent development of autonomous 'self-driving' vehicles are examples of practical and increasingly accessible robots and smart devices available to average consumers.

[0006] It is against this background that embodiments of the present invention have been developed.

Summary of Invention

[0007] In a first aspect, the present invention provides system for controlling at least one robotic device, comprising a computing device capable of communication with at least one robotic device and arranged to receive at least one command from a command module, the command being arranged to contain at least one instruction which is arranged to effect an operation on the robotic device and identification information to identify the at least one robotic device, wherein the computing device includes a processor and a database, the processor being arranged to receive the command and review the command against information in the database to determine whether the command is suitable for execution by the at least one robotic device, wherein the command is provided to the robotic device if the command is suitable for execution.

[0008] In one embodiment, the processor determines whether the command is associated with at least one authorisation code.

[0009] In one embodiment, the at least one authorisation code is received independently of the at least one command.

[0010] In one embodiment, the processor determines whether the command is one of a predetermined set of commands by accessing a set of predetermined commands stored in the database.

[0011] In one embodiment, wherein at least one of the at least one command, the authorisation code and the identification code is encrypted.

[0012] In one embodiment, the processor decrypts the at least one of the at least one command, the authorisation code and the identification code prior to reviewing the command to determine whether the command is suitable for execution.

[0013] In one embodiment, at least one of the at least one command, the authorisation code and the identification code includes a checksum, wherein the checksum is utilised to determine the correctness of the at least one command, the authorisation code and the identification code.

[0014] A system in accordance with any one of the preceding claims, wherein the robotic device is a programmable device.

[0015] In one embodiment, the robotic device includes at least one processor arranged to receive and execute the at least one command.

[0016] In one embodiment, the robotic device is capable of performing at least one physical function.

[0017] In a second aspect, the present invention provides a system for controlling a robotic device, comprising a computing device capable of receiving at least instruction, a processor capable of generating a command based on the at least one instruction, wherein the command is one of communicated via the computing device to initiate a response based on the at least one generated command.

[0018] In one embodiment, the processor requests further information to further assess the instruction, prior to initiating a response.

[0019] In a third aspect, the present invention provides a method for controlling a robotic device, comprising the steps of, receiving at a computing device at least one command arranged to effect an operation on the robotic device, reviewing the command to determine whether the command is suitable for execution, wherein the command is provided to the device only if the command is suitable for execution.

[0020] In one embodiment, the step of reviewing the command includes the step of determining whether the command is associated with at least one authorisation code.

[0021] In one embodiment, the at least one authorisation code is received independently of the at least one command.

[0022] In one embodiment, the step of reviewing the command includes the further step of determining whether the command is one of a predetermined set of commands.

[0023] In one embodiment, the invention provides the further step of the computing device receiving at least one identification code arranged to identify the robotic device.

[0024] In one embodiment, the invention provides the further step of receiving the identification code with the at least one command.

[0025] In one embodiment, at least one of the at least one command, the authorisation code and the identification code is encrypted.

[0026] In one embodiment, the invention provides the further step of decrypting the at least one of the at least one command, the authorisation code and the identification code prior to reviewing the command to determine whether the command is suitable for execution.

[0027] In one embodiment, at least one of the at least one command, the authorisation code and the identification code includes a checksum, wherein the checksum is utilised to determine the correctness of the at least one command, the authorisation code and the identification code.

[0028] In a fourth aspect, the present invention provides a system for controlling a robotic device, comprising a computing device in communication with the robotic device and arranged to receive at least one command which is arranged to effect an operation on the robotic device, wherein the computing device reviews the command to determine whether the command is suitable for execution, and the command is provided to the device only if the command is suitable for execution.

[0029] In a fifth aspect, the present invention provides a computer program including at least one command, which, when executed on a computing system, is arranged to perform the method steps in accordance with the third aspect of the invention.

[0030] A computer readable medium incorporating a computer program in accordance with the fifth aspect of the invention.

[0031] In a sixth aspect, the present invention provides a data signal encoding at least one command and being arranged to be receivable by at least one computing device, wherein, when the encoded command is executed on the computing system, the computing system performs the method steps in accordance with the third aspect of the invention.

Brief Description of the Drawings

[0032] Further features of the present invention are more fully described in the following description of several non-limiting embodiments thereof. This description is included solely for the purposes of exemplifying the present invention. It should not be understood as a restriction on the broad summary, disclosure or description of the invention as set out above. The description will be made with reference to the accompanying drawings in which:

Figure 1 is an example computing system which is capable of operating a device, system, method and/or computer program in accordance with an embodiment of the present invention;

Figures 2 and 2a are example systems in accordance with an embodiment of the invention;

Figure 3 is an example of a server module, including software/hardware modules and databases, arranged to implement an embodiment of the present invention;

Figure 4 is a flowchart depicting a computer implemented registration process in accordance with an embodiment of the invention;

Figure 5 is a flowchart depicting a computer implemented clearance process in accordance with an embodiment of the invention;

Figures 5a to 5d are computer implemented processes in accordance with an embodiment of the invention;

Figure 6 is a flowchart depicting a computer implemented profile creation process in accordance with an embodiment of the invention;

Figure 7 is a flowchart depicting a computer implemented profile update process in accordance with an embodiment of the invention;

Figures 7a to 7c are diagrams illustrating a computer implemented process in accordance with an embodiment of the invention;

Figure 8 is a diagram depicting a computer implemented system indicating process flows with regard to excluding, ghosting and shrouding processes in accordance with an embodiment of the invention;

Figure 9 is a stylised diagram depicting a series of computer implemented process flows with regard to excluding, ghosting and shrouding processes in accordance with an embodiment of the invention;

Figures 9a to 9c are diagrams illustrating a computer implemented process in accordance with an embodiment of the invention;

Figure 10 is flowchart depicting a computer implemented process for creating an exclusion, shrouding or ghosting zone in accordance with an embodiment of the invention;

Figure 11 is flowchart depicting a computer implemented privacy constraints process in accordance with an embodiment of the invention;

Figures 11a to 11k are diagrams illustrating a computer implemented process in accordance with an embodiment of the present invention;

Figure 12 is flowchart depicting a computer implemented sense/scan process in accordance with an embodiment of the invention;

Figure 13 is flowchart depicting a computer implemented seizure process in accordance with an embodiment of the invention;

Figures 14 and 15 are stylised diagrams depicting a computer implemented identification process in accordance with an embodiment of the invention; and

Figure 16 is a diagram illustrating another example of a computer implemented identification process in accordance with an embodiment of the invention.

Description of Embodiments

General Overview

[0033] The present invention relates generally to a system, method, computer program and data signal for the registration, monitoring and control of machines and devices. In particular,

embodiments of the invention relate to the registration, monitoring and control of robotic devices, autonomous vehicles, "smart" devices, and other programmable and computer controlled devices.

[0034] In more detail, one aspect of the embodiments described herein provides a method for controlling a robotic device. The method comprises the steps of, receiving at a computing device at least one command arranged to effect an operation on the robotic device. When the command is received, it is reviewed to determine whether the command is suitable for execution and is directed to the correct robotic device. The command is only provided to the device if the command is suitable for execution and directed to the correct robotic device.

[0035] In other words, one broad aspect of the embodiments described herein provides a system for controlling and monitoring the commands issued to autonomous or "smart" devices. Such a system is particularly useful for situations where the autonomous or smart devices are to be operated in a public space, where inappropriate operation of such devices may pose safety, security and financial risks to other members of the public.

[0036] One embodiment of the method is codified in a computing system, such as the computing system shown at Figure 1.

[0037] In Figure 1 there is shown a schematic diagram of a computing system, which in this embodiment is a server 100 suitable for use with an embodiment of the present invention. The server 100 may be used to execute application and/or system services such as a system and method for facilitating the controlling, monitoring and issuing of commands in accordance with an embodiment of the present invention.

[0038] With reference to Figure 1, the server 100 may comprise suitable components necessary to receive, store and execute appropriate computer instructions. The components may include a processor 102, read only memory (ROM) 104, random access memory (RAM) 106, an input/output devices such as disc drives 108, remote or connected input devices 110 (such as a mobile computing device, a smartphone or a 'desktop' personal computer), and one or more communications link(s) 114.

[0039] The server 100 includes instructions that may be installed in ROM 104, RAM 106 or disc drives 112 and may be executed by the processor 102. There may be provided a plurality of communication links 114 which may variously connect to one or more computing devices 110 such as servers, personal computers, terminals, wireless or handheld computing devices, or mobile communication devices such as a mobile (cell) telephone. At least one of a plurality of communications link 114 may be connected to an external computing network through a telecommunications network.

[0040] In one particular embodiment the device may include a database 116 which may reside on the storage device 112. It will be understood that the database may reside on any suitable storage device, which may encompass solid state drives, hard disc drives, optical drives or magnetic tape drives. The database 116 may reside on a single physical storage device or may be spread across multiple storage devices.

[0041] The server 100 includes a suitable operating system 118 which may also reside on a storage device or in the ROM of the server 100. The operating system is arranged to interact with the database and with one or more computer programs to cause the server to carry out the

steps, functions and/or procedures in accordance with the embodiments of the invention described herein.

[0042] Broadly, the invention relates to a computing method and system arranged to interact with one or more remote devices via a communications network. The remote devices may take the form of computing devices as described above, but may also take the form of robotic devices, as will be described in more detail later.

[0043] The system, in one embodiment, utilises a server including a database arranged to contain biometric or other identifying information regarding one or more entities. The database is arranged to receive the information via the communications network from the one or more remote devices and to subsequently communicate information to one or more remote robotic devices.

[0044] Figure 2a illustrates a Service Orientation Architecture suitable for use with an embodiment of the invention.

[0045] Other aspects of the broad inventive concept relate to a corresponding method, computer program, computer readable media and data signal. The method facilitates the transfer of commands regarding the desired instructions to be sent to an autonomous or "smart" device (also referred to as a "robot" device) between one or more remote devices and a centralized database. The centralized database receives a request to provide the command to the one or more remote devices, and forwards the information via a communications network to the one or more remote robotic devices.

Initial Interaction with the System

[0046] For a user to interact with the system in one embodiment, it is necessary for the user to identify themselves and register with the system. This is achieved through a resgistration process that is analogous to many other consumer product registration processes, such as the registering of a vehicle.

[0047] Preferably, a user may be required to prove or verify their identity by undertaking an identification check.

[0048] In one embodiment, prospective users ('prospective registrants') are required to set up a "profile account" or obtain an "eLicence". For the purpose of the broader invention described herein, a "profile account" or "ELicence" are any type of digital and/or electronic identifying means utilised to verify the identity of a user. In a co-pending application filed by Digital (ID)entity Limited, a Hong Kong company, novel and inventive embodiments of eLicence and Profile Accounts are described in more detail and are incorporated herein by reference.

[0049] The user uses their eLicence or Profile Account (along with other identifying information, such as a password) to connect or log-in a device (such as device 110) to a registry Server such as server cluster 100a (Figure 2) or registry server 300 (Figure 3) via a communications network. This connection and the entering of the code allow the prospective user to interact with the server cluster 100a.

[0050] Once the user is registered with the system, the user then registers their robotic device. As with a vehicle or boating license, the user, preferably, only has one license, but is able to register a plurality of robotic devices, as the user may have more than one robotic device.

Command and Control System

[0051] Each robotic device includes an internal secure computing device which is arranged to validate, authenticate and execute commands which are generated either from by the robotic device itself or by external parties.

[0052] That is, each robotic device includes an internal "logic" where, before an action is taken (whether physical or otherwise), the robotic device firstly receives an "Intention". The Intention must then be Validated against some internal logic or rules (i.e. a policy). Once the Intention is Validated, the Intention can then be Communicated to the relevant section of the robotic device and consequently Approved.

[0053] The Command and Control (CC) structure is now described in more detail with reference to Figure 2. In Figure 1a, any reference to a server, computing system, computer or other computing device refers to a server with capabilities analogous to the server 100 of Figure 2.

[0054] Referring now to Figure 2 there is shown a series of interconnected servers (a server cluster) generally denoted by 100a. A user 102a can interact with the server cluster 100a via their client device 104a or their mobile client device 106a.

[0055] When a robotic device 108a receives or generates a request (intention), the request originates from an "intention" application 110a. The intention application passes the intention request from the intentions application 110a to a validation controller (not shown). The validation controller ensures the robotic device and software have not been tampered with. The validation controller also ensures that all the physical components of the robotic device are in working order and approved for use within policy guidelines.

[0056] The request is then encrypted and transferred over a secure protocol (Virtual Private Network (VPN) connection 112a) to the server cluster 100a. All data packets are encrypted before transmission using key pair authentication or any other suitable encryption methodology, as may be required.

[0057] Once connected the robotic device establishes a secure Virtual Private Network (VPN) tunnel over a public communications mesh such as a mobile telecommunications network 114a, which may utilise a 3G (3rd Generation GSM standard) and/or 4G (4th Generation GSM standard) cellular network standard.

[0058] All communication to the server cluster 100a is via a secure firewall service 116a that limits VPN endpoints and ports that are available within the VPN. An appropriate standard, such as Secure Socket Layer (SSL) is utilised for the tunnel.

[0059] Once packets sent by the intention application (via the communications manager application) are encrypted and the VPN communication is secured and passes through the firewall, the robotic device authenticates to establish a connection with the CC system (i.e. the server cluster 100a). In the embodiment described herein, an authentication server 118a is utilised to authenticate the robotic device, through the exchange of certificates, although it will be understood that other authentication methods or systems may be utilised.

[0060] The CC system 100a further includes an application platform 120a that manages communication, requests, manifest distribution and ultimately the control of the robotic device.

In the context of the embodiment described herein, no action can be executed by the robotic device without first passing through the application platform 120a.

[0061] The application platform 120a interfaces with a policy engine 120b as the capabilities and allowed actions of each registered robotic device are stored as policies within the system 100a. The policy engine 120b allows each robotic device to be controlled uniquely as required by law, device capabilities and end user requirements. Policies are transmitted to the robotic device via the server cluster 100a as a base set of guidelines that cannot be breached. The workings of the application platform and the policy engine are described in more detail below.

[0062] The CC system is also responsible for recording an audit trail of all actions taken and all data received from the end device. This includes data such as the make and model of the robotic device, the capabilities of the device, flight manifests (where the robotic device is capable of flight), previous approvals for flight or movement, GPS movement and position data, including associated times and dates, instrument metrics, etc. Such information is stored in the Data Archive 122a, so that it may be accessed if necessary for auditing purposes.

[0063] A website 124a is provided as an interface to administer the application logic and all associated data/metadata. This includes information such as updating device policies, capabilities manifests, and other services, including, special services such as "ghosting" and "shrouding" (which are described in more detail below).

[0064] A fast, high Input/Output (IO) data retention service 126a caches incoming data feeds from the robotic device. Once cached the data is subsequently moved to the Data Archive 122a where it can be data mined as required for auditing purposes.

[0065] Returning to end users 102a, a web interface provides access from both a client device 104a and a mobile client device 106a. Through these interfaces the end user is able to securely instruct a robotic device to take actions, receive feedback on the status of the device and track results. All communication into the client device 104a and mobile client device 106a are secured via standard secure web protocols and firewall access 128a.

[0066] Once a connection is established the consumer may authenticate against the platform using password or biometric exchange to prove their identity, as previously described (i.e. using a "Profile Account" or "eLicence"). Depending on policies set by the end user and the platform the authentication can be more or less strict as required.

[0067] All end user (customer) data is secured and protected within a series of databases generally denoted by computing system 130a. In one embodiment, users may be required to pay for use of some services provided by the server cluster 100a. In such an embodiment, end users can carry out purchases or cash transactions via a standard, secure payment gateway 132a. This service is in the form of a shopping cart style interface with account management.

[0068] The end user interacts with the web application to execute robotic device commands and receive feedback. This application provides a series of interfaces and logic for robotic device administration.

[0069] At no time does the end user have direct access to a robotic device. While an end user would provide a series of policies about their robotic device and what they wish the device to do in certain instance these policies are not applied directly, but are vetted by the policy engine.

[0070] That is, all policies are exchanged and validated with the policy engine 120b to ensure that server cluster 100a has ultimate control of the device. As such, the server cluster 100a utilizes a "Command and Control" type structure to control the movement and action of robotic devices, to prevent unauthorised or illegal use.

Internal Robotic Device Validation

[0071] Each robotic device is capable of performing a predefined set of actions (physical or otherwise) and each action in the set of actions are associated with one or more instructions. Taken together, these allowable actions and associated instructions form the "policy" for the robotic device.

[0072] For example, a robotic drone (pilotless flying device) may be capable of flying in any direction, but may be limited to flying only in certain predefined air space, due to privacy, security or safety reasons.

[0073] One set of instructions necessary for the robotic device to be allowed to perform a command would be to undertake a diagnostic test each time the robotic device is activated.

[0074] The system would include a range of 'tests', beginning with regular (e.g. fixed date) tests. However, as problems can occur between regular checks (e.g. consumers may unintentionally or unknowingly damage their robots), it will be understood that diagnostic tests may also occur at random time intervals.

[0075] In addition to performing tests, test data can be gathered and in one embodiment, test data is communicated to the server cluster 100a as shown in Figure 2.

[0076] An example of the types of data collected during tests is described below:

[0077] The system's approved diagnostic tests are undertaken (completed) by an object or component written for the express purpose of performing one or more of the following operations:

1. identifying the robot, not limited to, for example:
    - 1.1. make, model, type;
    - 1.2. history, e.g. relevant dates/times, test results;
    - 1.3. registered owner(s)/user(s);
    - 1.4. possession of valid user security and protection mechanisms, e.g. biometric user locks;
    - 1.5. whether the device is currently registered, and will remain registered during the course of its (pending) assignment and/or function;
    - 1.6. hardware, software and capabilities, not limited to: functional specifications, valid 'default failure', 'seizure', 'rendezvous' and 'privacy' (e.g. software) protocols;
    - 1.7. that the device is approved to be used or operated as per the user's requested assignment or 'restricted' function, and that the assignment or function application (i.e. robot 'app ') itself is approved, including passing any Digital Rights

2. identifying the user or controller of the robot—particularly, that the robot is associated with and receiving assignment or function instructions from a user that possesses a valid account and up-to-date profiles and may further confirm if, and require that, the user or controller is also listed as an approved party to use or control this specific robot (not limited to, biometric authentication);

3. analysing and confirming if the robot's hardware and software are intact and remain untampered (e.g. not 'rooted', 'jailbroken' or hacked);

4. locating and identifying problems with or within the hardware, software, capabilities or any combination thereof in the robot's system, or the network of systems the robot may intend or be required to operate in or with;

5. carrying out performance or function tests to verify upheld originally approved operational proficiency, for example:

    5.1. it has or will have the capabilities and functional capacity (not limited to available fuel or energy charge, payload weight constraints/capacity) to acceptably complete its assignment or restricted function;

    5.2. its current performance would satisfy operational requirements required or anticipated for and during the requested assignment or function;

6. confirming that the robot does not have any outstanding maintenance, service, inspection or other orders;

7. establishing if the robot possesses or is carrying any unapproved or illicit payloads—in one instance, by analysing movement agility, e.g. if outside of normal baseline values/parameters this may account for unapproved payload weights; in another instance, by analysing data acquired from sensors or scanners on, in or within range of the robot that may detect unapproved payloads, e.g. these devices may be biosensors, molecular-level scanners, sensitive electronic chemical noses, etc.

[0078] Once the system receives confirmation that all registration, diagnostic and/or health tests have been successfully completed, the system issues relevant clearance codes to allow the robotic device to perform the function.

Command and Control Structure in More Detail

[0079] Figure 3 is a block diagram illustrating various components of a registry server which is equivalent to the structure shown generally at numeral 100a in Figure 2. The server 300 shown in Figure 3 illustrates an alternative view of the embodiment described with reference to Figure 2, in that Figure 3 is divided into functional modules rather than physical hardware. That is, Figure 3 does not delineate the application server farm 120a and the policy engine 120b and some aspects of the public access infrastructure shown in Figure 2, such as servers 130a and 132a, as separate components, but rather illustrates how such components functionally interact.

[0080] In other words, Figure 2 is an illustration of one embodiment of a server infrastructure in accordance with the broader inventive concept. Figure 3 is a high level "module" illustration

of one embodiment of an infrastructure in accordance with the broader inventive concept. Figures 2 and 3 provide different perspectives of the same inventive concept and are not to be taken to be directed to different inventions, but rather to different views of the same broad inventive concept.

[0081] The Server 300 includes various modules and databases which provide functionality that enables robotic devices to be monitored, controlled and managed in order to uphold, for example, safety, security and privacy considerations. A short summary of each module is provided below:

301 Administration Module

[0082] An Administration Module 301 is provided to transmit system administrative function commands to one or more robotic device. The commands can include commands that would be common to a number of robotic devices, including powering on and off, setting access control, software updates, performance monitoring, statistic gathering and/or other administrative functions not directly related to diagnostic tests, clearance codes and/or policing 'rogue' robots.

302 Communications Module

[0083] The system further provides a Communications Module 302 which enables communication between the robotic devices and the Registry's Server 300, and/or other registry servers (not shown).

[0084] Further, in another use of the Communications Module 302, clearance codes (that may be generated, outputted or stored in a Clearance Code Database 331) may be transmitted to users' robots, devices or vehicles.

[0085] Additionally, the Communications Module 302 may also facilitate communications with the Server 300 by other entities (or the same entity) to facilitate operations, activities or tasks such as:

- Maintenance, which may be in conjunction with an Orders Module 310, which accesses a Registered Robot Database 323 to determine any outstanding orders required to be addressed;
- Software upgrades, which are allocated to and stored in a Manufacturer and Robot Database 324 before being distributed to registered robots, devices or vehicles that are listed in the Registered Robot Database 323 - distribution is effected by a Task/Activities/Programs Module 312;
- Profile uploads retrieved from a User/Owner/Client Account Database 321, a subsequently stored in a Profiles Database 332;
- Robot registration application uploads, which are provided by a Tasks/Activities/Programs Module 312, in collaboration with a Robot Database 324 and a Registered Robot Database 323;
- User, application uploads, from a User/Owner/Client Account Database 321;
- Surveillance data uploads from users' robots or devices, from the User/Owner/Client Account Database and a Robot 'Apps'/Function Database

325 to confirm, for example, if a user or owner is authorised to be conducting surveillance operations;

- Identifying the user or controller of the robot or device; and/or
- Receiving user privacy constraints, via an Exclusion/Privacy Protocol Module 307.

303 Transaction Module

[0086] A Transaction Module 303 is employed to process financial transactions to pay for services provided by a Server 300 or associated, related third party.

[0087] In one embodiment, a Transaction Module 303 is responsible for issuing or processing product and/or service subscription accounts for users, owners or clients, which may be listed in a User/Owner/Client Account Database 321. Such subscriptions may be for the initiation or execution of exclusion zones or privacy constraints (not limited to, shrouding or ghosting).

[0088] Moreover, the Transaction Module 303 may be responsible for issuing or processing fines, infringements or penalties in relation to, for example, not limited to, inappropriate, unauthorised, unregistered, illicit, illegal or unruly use, control, management or ownership of a robot, device or vehicle. Such fines, infringements or penalties may be communicated to the relevant party or parties using a Tasks/Activities/Programs Module 312, a Seizure Protocol Module 309, and/or a Communications Module 302.

304 Controller

[0089] In some embodiments, the modules and databases listed operate autonomously. However, in the embodiment described herein, a central controller 304 is utilised to provide a "supervisory" function. The central controller may operate autonomously or may be controlled by a user, to "override" the autonomous functioning of any individual module. For example, if a breach of compromise of the system is detected, a user may use the controller to override any given clearance code or other permission given to a particular robotic device.

305 Proposed & Active Assignments/Functions & Travel Plans & Tracks Module

[0090] A Proposed & Active Assignments/Functions & Travel Plans & Tracks Module 305 is responsible for a variety of processes or tasks, including receiving, analysing, storing and outputting, as necessary, an end user's proposed robotic device commands.

[0091] The Proposed & Active Assignments/Functions & Travel Plans & Tracks Module 305 utilises data or information stored in a User/Owner/Client Account Database 321 or an Ineligible Database 322 to confirm that a proposed assignment or function is permissible, i.e. can be authorized

[0092] The Proposed & Active Assignments/Functions & Travel Plans & Tracks Module 305 also utilises data or information stored in a Registered Robot Database 323 to determine, whether a particular class, model or type of robotic device possesses the hardware, software or capabilities (including functional or operational) to undertake and successfully complete a proposed assignment, operation or function.

[0093] The Proposed & Active Assignments/Functions & Travel Plans & Tracks Module 305 also confirms that proposed or active assignments, operations or functions are permissible or

authorised according to information in the Robot 'Apps'/Functions Database 325 and/or information in the Operational Spaces Database 326, which contains approved, 'restricted' or disallowed assignments, operations or functions.

[0094] The Proposed & Active Assignments/Functions & Travel Plans & Tracks Module 305 may consult with, check and/or confirm information and data contained or stored in one or more of a Server's 300 databases or modules for the purpose or running any necessary test such as those that may be conducted by a Diagnostic Tests Database 327.

306 Clearance Code Module

[0095] A Clearance Code Module 306 allows the generation of suitable authorisation codes, for the purposes of allowing or approving a user robot, device or vehicle to undertake or successfully complete an assignment, operation or function.

[0096] In some instances, the Clearance Code Module 306 may cause a robot, device or vehicle to perform another type of assignment, operation or function that may not have been proposed or initiated by a user.

[0097] Where there is a requirement to perform a diagnostics test prior to conducting a task, the Clearance Code Module may be instructed by a Tasks/Activities/Programs Module 312 following the successful passing of the diagnostic test.

307 Exclusion/Privacy Protocol Module

[0098] An Exclusion/Privacy Protocol Module 307 may be a Server 300 component that is responsible for processing all privacy-related matters such as, but not limited to, exclusion zones, shrouding and ghosting, which may otherwise be known as privacy constraints.

[0099] In one embodiment, the Exclusion/Privacy Protocol Module 307 includes a web-based interface which allows users to access or interact with available server tools or features leading to the creation, setting up, amendment, removal and/or payment of a privacy constraint and/or a subscription or an associated user account. Such an account may be listed in or stored by a User/Owner/Client Account Database 321. An Exclusion/Privacy Protocol Module 307 may communicate with a User/Owner/Client Account Database 321 when necessary to allow, for example, a user to create, set up, amend or remove an account which may only exist for the purposes of enacting privacy constraints that may be conveyed to other's robots, devices or vehicles for execution or implementation. A Communications Module 302 may facilitate the connection between a user's (remotely located) device that is used to connect to a Server's 300 Exclusion/Privacy Protocol Module 307. Communications Module 302 may also facilitate the distribution of privacy constraints to other Servers and/or user robots, devices or vehicles.

[00100] The Exclusion/Privacy Protocol Module 307 may also impose changes to a Robot 'Apps'/Functions Database 325, for example, by altering or amending aspects of robot apps or functions, not limited to disallowing robots to travel into or within a particular space when execution a particular assignment, operation or function.

[00101] In this context, an Operational Spaces Database 326 may be altered to reflect changes to travel spaces.

[00102] In another instance, an Exclusion/Privacy Protocol Module 307 may communicate with a Diagnostic Tests Database 327, not limited to the following, for the purposes of altering,

amending, analysing, reviewing and/or confirming that a Diagnostic Tests Database 327 would appropriately and accurately instruct or command a robot, device or vehicle to perform all necessary tests before, during or after an assignment, operation or function with respect to any existing, or newly imposed changes to, privacy constraints listing in or stored on an Exclusion/Privacy Protocol Module 307.

[00103] For example, a user may form or create a new privacy constraint that may pose a particular challenge or be a different set of parameters not previously dealt with by a robot, device or vehicle. Accordingly, amendments and/or additions are made to relevant or applicable diagnostic tests on a Diagnostic Tests Database 327 which would cause all relevant or applicable robots, devices or vehicles to undertake or successfully complete an updated diagnostic test when next required.

[00104] The Exclusion/Privacy Protocol Module 307 may communicate with a Payload Database 328 for the purpose of forming a new or altering or amending an existing list of authorised payloads that is carried in, on or by a robot, device or vehicle. Certain privacy constraints may dictate which robots, devices or vehicles can carry or transport particular payloads. Authorised payloads may be dictated also by any restrictions placed upon, a user, which is listed in the User/Owner/Client Account Database 321.

[00105] The Exclusion/Privacy Protocol Module 307 may also communicate with a Surveillance Database 330 for the purpose of altering or amending authorised and unauthorised surveillance areas. Further to a Surveillance Database 330, an Operational Spaces Database 326 may be utilised for the same purpose.

[00106] The Exclusion/Privacy Protocol Module 307 also communicates with a Profiles Database 332 for the purpose of implementing any privacy constraints that may involve Profiles. For example, a user may upload to a Server 300 using their robot, device or vehicle, with the assistance of a Communications Module 302, a new or updated Profile to a Profile Database 332, with any updates to a Master Profile that relate to a privacy constraint communicated with an Exclusion/Privacy Protocol Module 307 which is then distributed out to any relevant or applicable robots, devices or vehicles.

308 Rendezvous (Sensor/Scanner) Protocol Module

[00107] A Rendezvous (Sensor/Scanner) Protocol Module 308 is a Server 300 component responsible for processing all rendezvous protocols (not limited to the example of a 'Sense/Scan' operation). These protocols may relate to the relocations of robots, devices or vehicles to specified locations. Rendezvous protocols may be formed, set up, amended or removed from one or more Server 300 databases or modules, not limited to a Rendezvous (Sensor/Scanner) Protocol Module 308 by either the registry party, users, governing bodies or other stakeholders or third parties.

[00108] Using the 'sense/scan' rendezvous protocol as an example scenario, such a protocol utilises a software application that executes on dedicated or shared hardware or other peripherals, which cause robots, devices and vehicles to perform, in one example, a predefined operation. Further, a Rendezvous (E.g. Sensor/Scanner) Protocol Module 308 may communicate with one or more databases such as a user/Owner/Client Account Database 321 or a Registered Robot Database 323 to determine which users, owners or clients require their robots, devices or vehicles to be tested or examine by example sensors or scanners.

[00109] The Rendezvous (E.g. Sensor/Scanner) Protocol Module 308 may also communicate with a Proposed & Active Assignments/Functions & Travel Plans & Tracks Module 305 in order to plan, program, calculate, anticipate or expect which, when or where robots, devices or vehicles may be 'called upon' (appropriately) for the purposes of a rendezvous protocol. For example, a robot may be in the vicinity of a sense/scan station and, thus, an opportune moment to activate or initiative the relevant rendezvous protocol.

[00110] In another example, using a practice of concealing (final) rendezvous locations or positions as an example scenario, the Rendezvous (Sensor/Scanner) Protocol Module 308 when activating a robot, device or vehicle for sensing or scanning may communicate with a robot, device or vehicle using a Communications Module 302 in order to regulate its surveillance or tracking capabilities, particularly, with respect to data that may be viewed or stored by an unauthorised party.

[00111] An Operational Spaces Database 326 or a Surveillance Database 330 may provide (the most up-to-date) privacy constraints that may need to be obeyed to protect the confidentiality, for example, of a sensor/scanner station's location or position. An Operational Spaces Database 326 may also have a station's location or position updated from time to time.

[00112] Certain clearance codes are generated by a Clearance Code Module 306 or retrieved from, or confirmed against a Clearance Code Database 331. Clearance codes sent may be the data signal which causes robots, devices or vehicles to initiate or execute a particular assignment, operation or function either for the purposes of this instance or another.

[00113] In another example, the Rendezvous (Sensor/Scanner) Protocol Module 308 may lead to a positive detection result of a robot, device or vehicle which may then cause another protocol, for example, a 'seizure protocol' run by a Seizure Protocol Module 309 to be initiated. A seizure protocol overrides any prior commands or instructions conveyed to a robot, device or vehicle by any party to, for example, instruct that a robot, device or vehicle instead execute new commands or instructions that may be issued by the Registry or a governing body.

[00114] The seizure protocol commands program a robot, device or vehicle to undertake or successfully complete a particular assignment, operation or function. For example, the assignment may be to a designated space (e.g. Police impound) that may be listed in an Operational Spaces Database 326. Further, different types or models of robots, devices or vehicles (that may be specified in a Registered Robot Database 323) may have different designated space.

309 Seizure Protocol Module

This module commands a user's robot, device or vehicle be relocated to a registry designated space. This space may be stored in an Operational Spaces Database 326. In various embodiments, a command may be communicated or uploaded to a robot, device or vehicle (using a Communications Module 302). The specific data signal communicated (e.g. an output file) that may trigger an installed software application on a robot, device or vehicle and that application will perform most of the computations. In other embodiments, a Server 300 runs the applicable software application (as a host) and the remotely located robots, devices and vehicles (clients) are simply a vessel which receives the commands from the Server 300.

310 Orders (Maintenance/Service/Inspection) Module

[00115] Module 310 commands that a user's or owner's robot be relocated to a designated space. This space may be listed in an Operational Spaces Database 326. The Module 310 may also incorporate all necessary information, data, tasks, activities or requirements related to maintenance, service, inspection or other matters. This Module 310 may also be a principal module for use by a robot, device or vehicle testing facility; therefore, not only used to instigate relocation of a robot, device or vehicle but able to be used after the robot has arrived at the relocation destination by dictating, undertaking or actioning (e.g. outstanding) orders.

[00116] In another aspect, this Module 310 may communicate with (perhaps, by using the Communications Module 302, for example) an Approved & Historical Assignments/Functions & Travel Plans & Tracks Database 329 to inform the Server 300 of a robot's, device's or vehicle's location or position relative to a designated space as described in the above paragraph. The server and any relevant user, owner or client may be kept updated on any order matters.

312 Tasks/Activities/Programs Module

[00117] This module may be utilised for numerous applications. For example, a module may be responsible for operating, managing, monitoring and controlling (herein—this invention—these may be referred to as 'running' or 'run(s)', depending on the context) one or more of the Server's 300 databases or other modules.

[00118] Some non-exhaustive examples are provided as follows:

- *Diagnostic Tests Database 327:* The 312 Module interfaces with Database 327 for the purpose of (remotely) running robot diagnostic tests, using data contained in the Database 327 as necessary. These tests may be in relation to the requirement that users or owners of robots be proficient or approved before being issues clearance code(s) in order to perform an assignment or function. In another non-limiting instance, tests may be concerned with, preferably, authorised parties that are performing maintenance, service, inspection or other orders on users' or owners' robots.
- *Robot 'Apps'/Functions Database 325:* The 312 Module may interface with Database 325 for the purpose of examining robot applications ('apps') for suitability or approval-for-use by users' or owners' robots, and/or acceptance on the robot app marketplace, which may be publicly or privately accessible. Further, the 312 Module may interact with the Database 325 for the purpose of public or private examinations or evaluations, i.e. the system may allow for open-source or closed-source assessments, comments and/or feedback in the process of determining an app's or function's suitability or approval.
- *Profiles Database 332:* The 312 Module may interface with Database 332 for the purpose of running the users', owner's or clients' Profile inputs and outputs. In one example, new or updated Profile data may be sent to the server and the 312 Module may be responsible for allocating to existing, respective, Master Profiles, or creating a new Master Profile accounts.

[00119] In another example, the 312 Module is also responsible for interacting with the Profiles Database 332 for the purpose of determining the percentage accuracy of a Master Profile.

[00120] In other words, the Module 312 may cause changes in the percentage accuracy assigned to a particular Master Profile. This change may then be distributed to an applicable or associated user, which would signal to the user the requirement to update the subject Profile. Distribution or communication with a remote device (e.g. robot) by the server may instigated by the Communications Module 302.

[00121] If Profiles also apply or are, for example, registered for privacy protection, e.g. Profile Exclusion Zone, Profile Shrouding or Profile Ghosting, then those applicable Profiles from the Profiles Database 332 may interface with Operational Spaces Database 326 (in the case of excluding spaces) and these privacy constraints are implemented in conjunction with the Exclusion/Privacy Protocol Module 307. Further, in performing the above mentioned programs, for example, the Module 312 and Profiles Database 332 may interact with the User/Owner/Client Account Database 321 where necessary. For example, Profiles in the Profiles Database 332 may be linked or associated with specific accounts in the User/Owner/Client Account Database 321.

[00122] In one embodiment, a Tasks/Activities/Programs Module 312 facilitates the policing of 'rogue robots' or unregistered, unlicensed, illegal, non-participating, etc. robots, devices and vehicles. In one aspect, using data and information from sensors, scanners or other surveillance capturing devices (installed on a user's robots, devices or vehicles) and transmitted to a Server 300 (using a Communication Module 302) and received by or stored in a Surveillance Database 330, a Tasks/Activities/Programs Module 312 may run a software program that monitors, for example, surveillance information or data that consists or comprises of identifying factors of a 'rogue robot' that is present or operating in a space that does not correlate with any active assignments, operations or functions listed in or stored on a Proposed & Active Assignments/Functions & Travel Plans & Tracks Module 305, which interfaces with an Operational Spaces Database 326.

[00123] In other words, a Surveillance Database 330 receive data; the data may be a captured video image of a robot, for example; where and when the image was captured may be recorded against or with the image file; a Tasks/Activities/Programs Module 312 and is then cross-indexed with data contained in a Proposed & Active Assignments/Functions & Travel Plans & Tracks Module 305, a Surveillance Database 330, a Registered Robot Database 323, a Manufacturer And Robot Database 324, a Robot 'Apps'/Functions Database 325, an Operational Spaces Database 326 and a Profiles Database 332.

[00124] In more detail:

- a Tasks/Activities/Programs Module 312 may operate to perform most, if not all of the functions described herein, not limited to cross-index data and information listed in or stored on the below list of databases and modules;
- a Proposed & Active Assignments/Functions & Travel Plans & Tracks Module 305 may allow identification of currently active assignments, operations and functions, and where and when they are occurring;
- a Surveillance Database 330 may receive and contain raw or unprocessed robot reference data to be searched, not limited to a digital picture of yet to be identified robot;

- a Registered Robot Database 323 may provide information as to the registration status of any robot that is identified after processing among surveillance data;
- a Manufacturer And Robot Database 324 may provide data or graphical representation information on particular types or models of robots to assist with comparing and contrasting said representations with surveillance data;
- a Robot 'Apps'/Functions Database 325 may allow another form of checking and confirming if a registered robot recently executed or is currently executing a software application that would cause a registered robot to be present at a particular place at a particular time;
- an Operational Spaces Database 326 may be utilised to bolster data or information about a particular space to surveillance data; and
- a Profiles Database 332 may list or storage various relevant robot Profiles to assist this aspect of the invention determine (in)tangible elements, subjects or objects captured in the surveillance data.

321 User/Owner/Client Account Database

[00125] A User/Owner/Client Account Database 321 includes a data structure of all users that participate with the system described herein. The User/Owner/Client Account Database 321 contains data concerning, but not limited to:

- the identity of a user, owner or client, and linked to or associated with some or all information or data listed in or stored on a Profiles Database 332 such as a profile picture or other media file;
- if a user, owner or client is linked to or associated with any registered robots, devices or vehicles, with some or all data listed in a Registered Robot Database 323;
- historical events (dates or times) linked to or associated with a user, owner or client, for example, some or all information relevant or applicable to a user, owner or client in this regard may be listed in or stored on an Approved & Historical Assignments/Functions & Travel Plans & Tracks Database 329;
- whether a user, owner or client currently possesses or formally possessed valid security and/or protection mechanisms or 'password keys', not limited to biometric locks or Profile data used to access or log-on to their robot, device or vehicle, or their Registry account for the purposes of paying a service fee or charge, dealing with privacy constraint matters (creation, amending, etc.), and so on, and relevant or applicable data or information concerning Profiles may be obtained from or referenced with data or information listed in or stored on a Profiles database 332;
- whether a user, owner or client has previously been or currently is associated with a robot, device or vehicle that had been, was or still is 'rooted', 'jailbroken' or hacked, or if there have been issues with or notable reports with respect to a robot's, device's or vehicle's hardware, software or capabilities, and such

information or data may be listed in or stored on a Registered Robot Database 323;

- whether a user, owner or client has any outstanding orders (that may relate to maintenance, service or inspection requests) for a robot, device or vehicle that they are linked to or associated with, and such information or data about orders may be listed on or stored in a Registered Robot Database 323, a Orders (E.g. Maintenance/Service/Inspection) Module 310, and/or a Diagnostic Test Database 327;
- whether a user, owner or client has any special waivers, permissions, authorisation or exemptions listed in or stored against their identity on their account file, not limited to, a waiver to have their robot, device or vehicle operate a surveillance application to allow a parent to supervise their child walking or catching the bus to/from school, or to allow their robot, device or vehicle to carry a particular payload or undertake a certain 'restricted' function, which information or data may be listed in or stored on a Payload Database 328.

322 Ineligible Database

[00126] The Ineligible Database 322 comprises a list of ineligible users, owners or clients. Ineligibility may be for a variety of applications, activities or requests, for example, particular users, owner or clients may not be mature enough (e.g. under a statutory age limit) to possess or have the authority to instruct, command or convey assignments, operations or functions to a particular type or model of robot, device or vehicle. In one embodiment, the Ineligible Database 322 is operated by a Tasks/Activities/Programs Module 312, and receives collaborative information or data from a Manufacturer And Robot Database 324 which specifies the hardware, software and capabilities (i.e. specifications) of a particular type or model of robot, device or vehicle.

[00127] Robots, devices or vehicles that are deemed ineligible may be listed in an Ineligible Database 322 and the corresponding ineligibility rating or status linked to or associated with a user's account which may be listed in the User/Owner/Client Account Database 321.

323 Registered Robot Database

[00128] The Registered Robot Database 323 includes information on robots, devices or vehicles that have been registered by their users, owners or clients. Robots, devices or vehicles that may be or become ineligible for registration may instead be listed in or stored on an Ineligible Database 322.

324 Manufacturer and Robot Database

[00129] A Manufacturer and Robot Database 324 includes data or information regarding manufacturers of robots, devices and vehicles. In more detail, the Manufacturer and Robot Database 324 lists all robots, devices and vehicles recognised by the Server 300 system.

[00130] Further, the Manufacturing and Robot Database 324 includes data with regard to 'Type Approval' methods, typically associated with compliance identifications/ certifications. For example, part of a compliance process may establish a performance baseline for a particular robot type, which would need to be above the required standards for compliance approval.

[00131] Further, data in relation to compliance matters may be stored on a Manufacturing and Robot Database 324. When diagnostic tests are being undertaken, e.g. by a Tasks/Activities/Programs Module 312 in collaboration with a Diagnostic Tests Database 327, the Manufacturing And Robot Database 324 may be referenced for any required data or information.

325 Robot 'Apps'/Functions Database

[00132] A Robot 'Apps'/Functions Database 325 includes data regarding approved or unapproved robot, device or vehicle software applications.

[00133] In more detail, a Server 300 utilises the Robot 'Apps'/Functions Database 325 for the purpose of listing or storing all available 'apps' for download and/or purchase by users, owners or clients, perhaps, for their respective robot, device or vehicle. Those parties may access or log-in to their registry account, navigate a web-based interface in order to search for, select and purchase, then download a desired app.

[00134] The 'app marketplace' may interface with any one or more of the aforementioned modules and/or databases. For example:

- a Communications Module 302 arranged to facilitate data transmission in order to: access an account, complete any transaction activities, download any relevant files from the Server 300 and/or another robot, device or vehicle;
- a Tasks/Activities/Programs Module 312 to operate the 'app marketplace' web-based or API interface;
- a Transaction Module 303 facilitates e-, f- , s- and/or m-Commerce activities;
- a User/Owner/Client Account Database 321 is responsible for assigning restrictions, regulations, listing/storing and/or advising of any applicable or relevant information about, in respect of, or to particular apps;
- an Ineligible Database 322 controls which parties are not eligible to download particular apps;
- a Registered Robot Database 323 which includes of a list of apps that a robot, device or vehicle already possesses, that may be eligible or compatible with particular apps;
- a Manufacturer And Robot Database 324 specifies apps that are suitable for use or compatible with particular apps, or provide guidelines or parameters to specific to different types of robots, devices or vehicles;
- a Robot 'Apps'/Functions Database 325 includes a list of approved or unapproved apps for all types of robots, devices or vehicles available in the 'app marketplace';
- an Operational Spaces Database 326 discloses all spaces that are authorised to work with or are approved-for-use by an app, which is accessible via a web-based interactive map that illustrates the specific areas;

- a Diagnostic Tests Database 327 determines which tests should or must be run before particular apps are executed on robots, devices or vehicles, during and/or after the execution of those apps;
- a Payload Database 328 determines which, if any, payloads may be utilised with a particular app;
- an Approved & Historical Assignments/Functions & Travel Plans & Tracks Database 329 provides statistical data or information concerning the number of occasions a particular app has been utilised;
- a Surveillance Database 330 informs which apps in the 'app marketplace' have restrictions placed upon them in respect of surveillance activities performed by a robot, device or vehicle;
- a Profile Database 332 determines which Profiles are required to be exchanged or transmitted to a Server 300 and/or another robot, device or vehicle.

326 Operational Spaces Database

[00135] An Operational Spaces Database 326 is provided which includes an entire inventory of environments, places, areas or spaces approved for particular robots, devices or vehicles. The Tasks/Activities/Programs Module 312 interfaces with this database to transmit information to the robots, devices or vehicles.

[00136] In more detail, the Operational Spaces Database 326 regulates particular assignments, operations or functions of robots, devices or vehicles. For example, a particular airspace may be permanently excluded-for-use by all or particular robots, devices or vehicles for safety, security or privacy considerations.

327 Diagnostic Tests Database

[00137] The Diagnostic Tests Database 327 includes a plurality of tests for execution on robots, devices and vehicles. In one embodiment, a robot, device or vehicles utilises the Server 300 Diagnostic Tests Database 327 when required to perform a test, and/or the Server 300 may reference its Diagnostic Tests Database 327 to confirm that a robot, device or vehicle possesses the correct tests on its own database(s) and/or module(s).

[00138] The Server's 300 Tasks/Activities/Programs Module 312 and/or Communications Module 302 is utilised to, respectively:

(i) run or perform the test on or for a robot, device or vehicle, remotely; and

(ii) facilitate any necessary transmissions to/from the host (e.g. registry Server 300) and clients (e.g. users', owners' or clients' robots, devices or vehicles) for these purposes.

329 Approved & Historical Assignments/Functions & Travel Plans & Tracks Database

[00139] An Approved & Historical Assignments/Functions & Travel Plans & Tracks Database 329 contains registry, governing body or other third party approved robot, device or vehicle assignments, operations or functions, which includes permissible operational spaces travel for robots, devices and vehicles.

[00140] The Proposed & Active Assignments/Functions & Travel Plans & Tracks Module 305 communicate or references information or data contained in the Approved & Historical Assignments/Functions & Travel Plans & Tracks Database 329 before approving or amending any proposed or active assignments, operations or functions.

[00141] A Clearance Code Module 306 is utilised to generate any relevant or appropriate clearance codes after a Proposed & Active Assignments/Functions & Travel Plans & Tracks Module 305 has deemed an assignment, operation or function is acceptable or approved following collaboration with an Approved & Historical Assignments/Functions & Travel Plans & Tracks Database 329.

330 Surveillance Database

[00142] In addition to aspects already described herein, a Surveillance Database 330 may be utilised to collect particular surveillance data or information from a plurality of robots, devices or vehicles.

[00143] A user may run a particular software application (that may be listed in or stored on a Robot 'Apps'/Functions Database 325), and that application carry a stipulation that particular surveillance data (e.g. with respect to time, date or location) be relayed to the Server 300 for analysis, processing, storage, etc. A Communications Module 302 may facilitate the transmissions between the Server 300 and remote robots, devices or vehicles. A Tasks/Activities/Programs Module 312 may then route (after, for example, filtering) relevant, appropriate or value data to a Surveillance Database 330.

331 Clearance Code Database

[00144] A Clearance Code Database 331 may list or store all historical or currently active codes issued and their respective assignment, operation or function particulars (which robot it was issued to, the user involved, time/date, etc.) and is run by a Clearance Code Module 306. The Clearance Code Database 331 can also be used for the purposes of ensuring that particular codes are not reused again, or are only recycled following suitable quarantine periods.

[00145] Figure 4 to 7 are flowcharts illustrating the process of issuing clearance code(s) to robots before they may operate (at a particular time or in a particular manner or space). This embodiment adopts 'public' spaces as an example, but the broader inventive concept extends to any physical or virtual space.

[00146] Referring to Figure 4, there is shown a typical process flow for a registry in accordance with the registries shown generally at Figure 3 (i.e. server 300) and with the server system generally shown at Figure 2 (i.e. server cluster 100a).

[00147] At step 402, a user typically wishes to utilize a robot for a particular function. If the consumer does not have a robot, the consumer may wish to purchase or otherwise obtain a robot at step 404, before proceeding to step 406, where a user makes a determination as to whether the robot will be used in a public space.

[00148] If the consumer wishes to operate their robot in a public space, the process flow continues to step 412, where a determination is made as to whether the consumer possesses a valid robot account. If the consumer does not have an account, a further determination is made at step 414 to determine whether the consumer is eligible for an account. If the consumer is not

eligible for an account, the consumer may register to determine whether they may be eligible for an account at a later date at step 416.

[00149] If the consumer is eligible for an account, at step 418, the consumer obtains a valid account.

[00150] Once the system has determined that the consumer has a valid account, a check is made to determine whether the consumer's robot is registered at step 420. If the robot is not registered, then at step 422, a determination is made as to whether the consumers robot is registration eligible. If the robot is not registrable for registration, the consumer may obtain a robot at step 424, and the eligible robot can then proceed through the flow process at step 406. If the consumers robot is registration eligible, the consumer registers the robot at step 426 and the process flow may continue as shown in Figure 5.

[00151] Referring now to Figure 5, once it is determined that the consumer is authorised to operate the robot and that the robot is registered and authorised to carry out the action, then at step 428, a determination is made as to whether the consumers robot has outstanding orders. If so, the process flow continues to step 430 where the consumer is informed, the consumer complies at step 430 and the orders are satisfied and the robot reinstated at step 434. Thereafter, the robot is ready to receive future orders and the process flow continues at step 440, where the consumer conveys an assignment or function instructions to the robot.

[00152] Referring to Figure 5a, there is shown a diagram illustrating the concepts of a software application in accordance with the present invention.

[00153] Referring to Figure 5b, there is described a process flow for the manner in which a command is generated, processed and received by the robotic device. At step A001, external command or request generator 1 (e.g. a user and/or user's 'smart' device or robot pendant) generates a command or request (including any metadata).

[00154] At step A002, the command or request (which includes any attached information or metadata) is communicated 8 to the remote server 2 (or Robot Registry). At step A003, the remote server 2 receives and assesses the command or request, then generates an assessment determination.

[00155] At step A004 and A005, if the determination was to conditionally approve the command or request subject to approval of results or responses from outstanding assessment requirements, the remote server 2 communicates 9 outstanding requirements or instructions (e.g. assessment, diagnostic or health test instructions) to the robot's 6 receiver/transmitter module 10.

[00156] Therefore, in one embodiment, the command or request (e.g. operation mission) is first approved, in-principle, then the robot may need to be vetted (e.g. to ensure it is up to the task) before it is authorised to effect the command or request (e.g. like a two-part procedure or assessment).

[00157] The receiver/transmitter module 10 transmits the requirements or instructions to the robot's 6 regulating 'chip' 3 (e.g. a robot-local Robot Registry device, which may be software, hardware and/or firmware, and may comprise one or more devices functioning together, separately, dependently or independently; such devices may be integrated into robot modules or units, e.g. central processing units, CPUs).

[00158] At step A006 and A007, the regulating chip 3 facilitates and/or supervises robot testing or querying, communicating 9 results or responses to the remote server 2 (e.g. via the robot's 6 receiver/transmitter module 10).

[00159] At step A008, the remote server 2 receives and assesses the results or responses, then generates an assessment determination. (Note: steps A004 to A008 may go through numerous rounds or be repeated e.g. to facilitate further querying or testing following receipt, assessment and determination of prior query or test results or responses).

[00160] At step A009, if a determination was to approve the command or request following receipt and assessment of the robot's 6 results or responses, then the remote server 2 communicates 9 the command or request to the robot's 6 receiver/transmitter module 10. The receiver/transmitter module 10 transmits the command or request to the robot's 6 regulating chip 3.

[00161] At step A010, the regulating chip 3 facilitates the command or request, transmitting to the robot's 6 output 5, which essentially results in the command or request being effected.

[00162] Referring to Figure 5c, there is another example of a command and control sequence. At step B001, external command or request generator 1 generates a command or request.

[00163] In another embodiment, an internal command or request generator 7 (e.g. the robot's 6 autonomous logic or 'brain') generates a command or request. In one example, the robot detects something in its environment such as unfavourable or bad weather, which upon internal logic assessment results in the robot needing to generate a request such as permission to implement a detour to the destination, i.e. to avoid the bad weather.

[00164] Since the detour would involve a new travel path the robot would first need it approved before the robot is permitted to pursue the new route. At step B002, the command or request is communicated 12 (or transmitted 11, according to the other embodiment in step B001) to the robot's 6 input module 4. The robot's 6 input module 4 transmits the command or request to the robot's 6 regulating 'chip' 3.

[00165] At step B003, the robot's 6 regulating chip 3 assesses the command or request, then generates an assessment determination. At step B004 and B005, if the determination was to conditionally approve the command or request subject to approval of results or responses from outstanding assessment requirements, the regulating chip 3 then facilitates and/or supervises robot testing or querying to establish said results or responses.

[00166] At step B006, should the results or responses be satisfactory , in conjunction with the command and request, then the regulating chip 3 communicates 9 this data information to the remote server 2 (e.g. via the robot's 6 receiver/transmitter module 10) for further or final assessment and determination. In other words, the regulating chip 3 may pre-vet the command or request and/or robot's results or responses, i.e. before communicating with the remote server 2.

[00167] An advantage of this includes reducing the probability of the remote server 2 receiving and processing extraneous, redundant or purposeless data information traffic, e.g. the regulating chip 3 may act as a 'first screen', rejecting any commands or requests (which may be in conjunction with the robot's results or responses) that do not pass muster or are determined as not (likely) to be approved by the remote server 2.

[00168] At step A007, the remote server 2 receives and assesses the command or request and/or results or responses, then generates an assessment determination. At step A008, if the determination was to approve the command or request, the remote server 2 communicates 9 the command or request approval to the robot's 6 receiver/transmitter module 10.

[00169] The receiver/transmitter module 10 transmits the command or request approval to the robot's 6 regulating chip 3. At step A009, the regulating chip 3 facilitates the command or request, transmitting to the robot's 6 output 5, which equates to the command or request being effected by the robot 6. Note, as described in Scenario 1, the Scenario 2 process may also involve steps the same as or similar to steps 4 to 7 in Scenario 1, e.g. the remote server 2 may dictate further robot querying or testing before approving the command or request.

[00170] Referring to Figure 5d, there is shown another example of a command and control state. At step C001, external command or request generator 1 (or internal command or request generator 7) generates a command or request.

[00171] At step C002, the command or request is communicated 12 (or transmitted 11) to the robot's 6 input module 4. The robot's 6 input module 4 transmits the command or request to the robot's 6 regulating 'chip' 3.

[00172] At step C003, the robot's 6 regulating chip 3 assesses the command or request, then generates an assessment determination. At step C004 and C005, if the determination was to conditionally approve the command or request subject to approval of results or responses from outstanding assessment requirements, the regulating chip 3 then facilitates and/or supervises robot testing or querying to establish said results or responses.

[00173] At step C006, it is here that the process may differ from Scenario 2, in that the regulating chip 3 may determine that there is no communication with a remote server 2 (e.g. the robot 6 may be 'out of range', in a wireless signal denied environment or not 'permanently' online), so the regulating chip 3 assesses to the best of its ability and/or programming the command or request and/or results or responses (e.g. it may take on the same or similar role as what the remote server 2 would have performed).

[00174] In one embodiment, the regulating chip 3 may occasionally communicate 9 with a remote server 2, e.g. via the robot's 6 receiver/transmitter module 10, and in doing so may facilitate the renewal of the robot's regulatory chip service subscription (or licence key) and/or the updating of relevant software, patches or flashes such as the latest Orders and/or Protocols that are to be obeyed or complied with by the robot 6.

[00175] In a further embodiment, should the robot's 6 regulating chip 3 not communicate with the remote server 2 within a specified time period or in respect of a currently proposed command or request the robot's 6 regulating chip 3 may cause commands or requests to not be approved in whole or in part—essentially, limiting or restricting the robot 6 or preventing it from operating.

[00176] A limitation or restriction example includes the command or request being 'travel around [this] location, taking surveillance footage'; however, since the robot had not been in communication with the remote server within a specified period of time the command or request was reduced or limited, for example, as follows: the robot was only permitted to travel within a specified radius of its 'home base' (or registered address) or was not permitted to travel within public spaces.

[00177] At step C007, if the determination was to approve the command or request, the regulating chip 3 facilitates the command or request, transmitting to the robot's 6 output 5, which equates to the command or request being effected by the robot 6.

[00178] Upon receiving the instructions, at step 445, the robot commences diagnostic tests and subsequently, at step 450, the robots test data is sent to the registry where, at step 455, a determination is made to determine whether the robot has successfully completed the diagnostic tests. If not, the process is terminated at step 460 as the consumers robot is not issued a clearance code required to execute assignment and/or perform a restrictive function in a public space. If the robot successfully completes the diagnostic tests, the registry issues the consumers robot with the appropriate instructions or clearance codes at step 465 and at step 470 the consumer's robot executes the assignment or function. Subsequent to the assignment or function being executed, the registry may optionally be updated at step 475 and a further determination is made to determine whether the consumer has other assignments or function instructions for the robot at step 480. If not, the process ends at step 485, but if there are further instructions, the process returns to step 406 at Figure 4.

Profile Updating

[00179] Referring now to Figure 6 there is shown a flowchart depicting a manner in which a profile may be updated. At step A505, a customer obtains profile capture products and ultimately at step A510 the customer obtains a subscription account and is invoiced accordingly if a subscription model is used.

[00180] Once the customer has obtained profile capture products and a subscription account, at step A515 the customer forms their profile. Once the profile is formed at step A520 the customer logs onto their account and subsequently at step A525 the customer may upload their profile update (or alternatively, the profile may be updated automatically).

[00181] In some embodiments, the file updates may be sent to a master profile and added to the master profile as shown at step A530. Subsequently, the customers updated master profile is distributed.

[00182] Referring now Figure 7, there is shown a shorter description of how a master profile is updated. At step 419b, a determination is made as to whether profiles are maintained. If not, at step 419c the user is informed it is required to update their profile. The user subsequently updates their profile at 419d and the process ends at step 419e. If the profile has been correctly maintained, no further steps are necessary and the process ends at step 419e.

Conditions or Constraints

[00183] In the previous section, and with reference to Figures 5a-5d, there are described various examples of a methodology for the command and control structure. One step in the process is the imposition of "conditions or constraints" on the operation of the robotic device. Example embodiments are described with reference to Figure 7a, each path defined by the flowchart route chosen.

[00184] Figure 7b may conform to a similar structure of the broad process steps of:

(1) generating;
(2) assessing (optional);
(3) responding; and

(4) amending (optional).

[00185] With reference to Figure 7c and 7b, the following summarises two example processes of generating, assessing and imposing a condition or constraint. With regard to Scenario 1 in Figure 7c, at step D01, the condition/constraint creator CC10 generates a condition or constraint (including any metadata).

[00186] At step D02, the condition or constraint (which includes any attached information or metadata) is communicated to the remote server CC11 (or Robot Registry). At step D03, the remote server CC11 receives and assesses the condition or constraint, then generates an assessment determination.

[00187] At step D04, the remote server CC11 may approve the condition or constraint being imposed. At step D05, the remote server CC11 communicates the condition or constraint to the robot's CC12 one or more 'regulating chips'. At step D06, the robot's CC12 regulating chip facilitates the condition or constraint being imposed.

[00188] At step D07, the condition or constraint may be amended or revoked for one or more reasons, e.g. the condition/constraint creator CC10 may no longer require the condition or constraint to be active, so it may be cancelled.

[00189] With regard to Scenario 2 in Figure 7c, at step E01, the condition/constraint creator CC20 generates a condition or constraint (including any metadata). At step E02, the condition or constraint is communicated to the robot's CC22 one or more regulating chips. At step E03, the robot's CC22 regulating chip receives and facilitates assessment of the condition or constraint, then generates an assessment determination. At step E04, the regulating chip may approve the condition or constraint. At step E05, the regulating chip facilitates the condition or constraint being imposed. At step E06, the condition or constraint may be amended or revoked.

Privacy Issues and Ghosting

[00190] Figures 8 to 11 illustrate some examples of the techniques utilised by the server 300 to prevent users from capturing, viewing or recording surveillance data from any device, machine or robot, either due to being unregistered, the user unlicensed, it operating or functioning within or near a particular space, and so on. However, robots, for example, may still be able to use cameras or other surveillance functionalities for navigation or other purposes, but their users would not be approved or able to access, view or record such footage or data.

[00191] Privacy constraints may take the form of software code downloaded onto the robot, which then self-regulates its navigation movements. In one embodiment, the robot's navigation system may have 'blocks' or 'no go' zones placed upon its 'internal' map. These no go zones may be added, subtracted or amended accordingly, from time to time. Compatible navigation software code may utilise or feature multi-dimensional (geographical) coordinate systems/techniques. Such as, the robot's system is informed to avoid or not to travel within certain zones.

[00192] For example, unregistered robots would not typically receive clearance codes but they may receive privacy constraints. Being able to receive these constraints despite not being registered may be due to robot manufacturers supporting the 'privacy protocol standard', thereby, by default, designing robots to automatically receive these relevant transmissions—in

whatever form they may be relayed to the robot (and whether from the registry or another party)—irrespective of the user being aware of such receipt.

[00193] In an alternative example, a registered robot may receive clearances codes; however not receive any privacy constraints. One reason for this may be because the consumer's instructed assignment or function did or would not cause the robot to venture in, on or near an exclusion zone (a zone that may be registered with the Register or another party).

[00194] In more detail, the steps for facilitating exclusion zones (e.g. adjust travel path or plan):

(1) condition or constraint position data information is received (e.g. by robot or by remote server);

(2) prior to an Intention execution or approval, robot's travel plan or path is queried for conflicts with received condition or constraint position data information;

(3) if there are conflicts, plan or path is adjusted to avoid (collision with) the space (or subject within that space) as defined by the condition or constraint position data information.

[00195] The broad steps for facilitating shrouding or ghosting (e.g. augmenting of surveillance data and regulating disclosure):

(1) condition or constraint position data information is received (e.g. by robot or by remote server);

(2) prior to an Intention execution or approval (including the transmission of surveillance data for viewing and/or storing in non-buffer/volatile memory; or the disclosure of data information, e.g. subject 'tagging'), robot's sensor field(s) of capture are queried for conflicts with received condition or constraint position data information;

(3) if there are conflicts, robot's sensor field of capture is conditioned or constrained (e.g. augmented) such as by obstructing the sensor data feed or by blurring, censoring, blacking or whiting-out the capture field corresponding with the received condition or constraint data information. In one embodiment, this shrouding mechanism may be facilitated similar to creating 3D models in augment reality environments, i.e. upon the recognition of a profile in the scene, the profile is virtually substituted with a 'blank' shape, obstructing the profile.

[00196] Condition or constraint position data information is received by robot and/or remote server in the following manners:

- For pre-defined position data information (e.g. fixed coordinates + altitude) with reference to Scenario 1 (or 2) shown in Figure 7c, the remote server (or robot's regulating chip) receives the generated condition or constraint, e.g. D03 (or E03), usually, in advance.
- For real-time position data information (e.g. collocated location module), the robot may receive the broadcasting device's transmission.

- For real-time profile recognition: robot may capture the profile, it be recognised locally (e.g. by regulating chip), then a determination made whether the profile is conditioned or constrained. In another embodiment, the robot captures but then communicates the capture data information to a remote server for processing (i.e. recognition or query); if the profile is conditioned or constrained then a regulated response may be issued or no response.

[00197] The systems, methods, computer programs, data signals and apparatuses which may facilitate exclusion zones include those technologies deployed for Airborne Collision Avoidance Systems ( ). Examples (non-limiting), include:

(1) Traffic alert and Collision Avoidance System (TCAS) ;

(2) Portable Collision Avoidance System (PCAS) ;

(3) FLARM ;

(4) Terrain Awareness and Warning System (TAWS) ;

(5) Obstacle Collision Avoidance System (OCAS)

Profile Recognition

[00198] The main differences with exclusion zones being facilitated via Profiles rather than collocated location module or fixed coordinates + altitude include the substitution of position announcing transmitting devices and signals with Profile recognition technology and the generation of a prescribed exclusion zone around that recognised Profile, which may be facilitated within the robot's Geospatial Information System (GIS), navigation and path planning system.

[00199] Returning now to Figure 8, there is shown a diagram illustrating a number of clients, user devices and robots. A client 111 selects privacy constraints, which are transmitted via a communication network 60 and, through server 100a, to a plurality of robots 210a, 210b and 210n. The privacy constraints are filtered by the system such that only robots that are participants in the network receive the privacy constraints. As can be seen, non participant robot 210c does not receive the imposed privacy constraints.

[00200] Similarly, user device 110b which is a non participant does not receive the imposed privacy constraints. However, user devices 110a and 110n do receive the privacy constraints.

[00201] Referring now to Figure 9, there is shown an example of how exclusion, shrouding or ghosting operates in practice. The registry may utilise its resources to exclude spaces from being travelled (or traversed) by robots, essentially by enacting 'no go' or 'no fly' zones, for example, that robots obey. Additionally, other devices or machines may also be regulated, by not being permitted to operate unencumbered within or near these exclusion zones. These devices or machines may be caused to switch off or reduce functionality.

[00202] In one embodiment, the Registry's server implements an exclusion zone and all robots must adjust their subsequent travel plans and tracks accordingly.

[00203] This is implemented by a software application for robots that prevent any (on-board) equipment (e.g. cameras) from surveillance operations when faced or encountered with a shrouded zone to protect, for example, public privacy.

[00204] In more detail, before explaining the process flow of Figure 9, it will be understood that when a participating robot or device captures a registered Profile (not limited to a tangible object, such as a person) the data captured would trigger, upon processing, that it is privacy registered and then that subject is instantly shrouded (e.g. blurred). Profiles may be stored and processed locally, on participating robots or devices (reducing lag or latency times), or remotely, stored and processed on, for example, the Registry's cloud servers. Not storing such data on non-registry devices or robots would be preferred in order to securely maintain (client's) sensitive Profile data.

[00205] In another embodiment, select Profile data is stored (and processed) locally of user's devices or robots. For example, the registry may transmit to participating robots and devices Profile data of registered clients (subscribers) present in the vicinity of those participating robots and devices. So if they were to encounter each other (i.e. come into capture view) then these privacy measures could be effected. Then, once participating robots or devices have moved away from a registered client that client's Profile data is deleted from those robots and devices. This embodiment would help ease the latency problem, by storing and processing locally, and slightly solve the issue of having sensitive Profile data (of others) stored and processed locally, rather than just by the Registry's servers.

[00206] Profile data is stored, processed and filtered (with respect to database queries) in any number of manners. For example, the end-user's device or robot may locally store a copy (and receive relevant updates) of all database Profiles; and the device or robot may subsequently process and filter such queries as well.

[00207] In one embodiment of the invention, the business may be presented with a map (that is at least one-dimension), however, preferably a three-dimensional mapping computer program like one or more of the following: Bing 3D Maps; Placebase; Google Tour Guide or Maps GL, 3D Maps Mobile; Amazon's UpNext app; Whereis 3D City Models; Uniden TRAX 5000; Aviation Mapper; Nokia 3D Maps (e.g. Ovi), and so on.

[00208] The business would be presented with the opportunity to select in the map (by directing a mouse cursor or equivalently operable pointer) areas or spaces, perhaps, by dragging the cursor or pointer across a screen or by using gesture control, voice commands or other effecting action that may be or become applicable methods from time to time.

[00209] One example of shrouding would be a resident wishing to shroud their apartment's windows and balconies from robot surveillance (perhaps, aerial robotic devices), would access the system, locate their property's windows and balconies, drag the cursor over those areas or spaces to shroud (that may be illustrated on-screen by a size-changing rectangle or rectangular prism), confirm selection, enter and accept payment terms, confirm transaction, shrouding effected with specified timeframe.

[00210] Only applicable or allowable zones may be available for selection by the business. For example, parties may not have the option available to select a space that they do not have

control over, do not own or are not named on the land's title. If a party selects a zone for exclusion (i.e. to prevent other robots from travelling in this space or on this area) and this zone not be a space legally associated with the party, for example, then to prevent robots that are related to a party legally associated with that space due to the exclusion imposed by the other disassociated party those robots may be approved to override such imposition. [Need to account for antagonists, i.e. dissociated parties that may attempt to prevent other parties' robots from genuinely accessing or travelling in a particular space.]

[00211] Referring now to Figure 9, at step 1, an augmented reality device or a robot with surveillance captures data, which may be image or voice data at step 2. At step 3 the captured data is transmitted to a remote server for processing via the communications network 60a. The captured data is received at step 5 by at least one server such as server 300a and the data is stored and compared against privacy constraints. At step 6 the data is uploaded through the communication network. At step 7 the processed data is transmitted to the robot or device, so that appropriate action may be taken by the robot or device at step 8.

[00212] Referring now to Figure 9a, there is described an example of how exclusion zones be created (e.g. how specific areas/volumes of a town are designated as non-operational areas to robots).

[00213] The remote server (Robot Registry) is responsible for ensuring all exclusion zone data is updated and maintained. This data arrives from various sources such as public aviation departments, defence departments, LEO groups, corporations and individuals. An exclusion zone (e.g. 'no fly zone') consists of various pieces of metadata that includes the following:

- Geo-location data that defines a three-dimensional volume mapped against the surface of the earth;
- Times that the condition or constraint is in place;
- Dates that the condition or constraint is in place;
- Specifications of what the exclusion zone applies to. For instance robots over a certain size/speed capability;
- Explanation for the condition or constraint; and
- Body/individual that requested the condition or constraint.

[00214] The remote server allows data to be submitted via secure web forms or via automated Application Programming Interfaces, within the remote server web form interface individuals could enter data in several ways. Data is entered as a series of GPS locations creating a closed loop or a map could be displayed allowing the individual to plot the closed loop over the map. Once submitted a remote server validates geo-data and approve it for submission to the exclusion zone database. Additional screens allow for the editing and configuration of this data as required by remote server staff. Alternatively, once submitted, the remote server's automated assessment programs may determine suitability for approval.

[00215] To create an accurate three-dimensional volume all data is GPS based including altitude values. A default height may be applied to the zone.

[00216] The user can use any tool that creates a valid set of GPS coordinates which form a loop, or alternatively they could utilise an online mapping interface provided by a remote server (Robot Registry).

[00217] One example of an online mapping interface is Google Maps developer API. Specific information on the capabilities can be found here .

[00218] A user or service provider sends to the remote server the Intention request which holds the GPS location of the target landing site. This data is presented in a JSON compatible format and matches the remote server API requirements or is rejected. A typical request looks as follows:

```
{
    "recipient": "Mr Craig Smith",
    "address": [
        {"address1":"1 John St"},
        {"address2":"Craig's farm"}
        ],
    "geo": {
        "lat": "-32.118056",
        "long": "141.923447"
    },
    "payload": {
        "lot":"of data"
    }
}
```

[00219] The remote server processes this request to identify if it exists within its known database of exclusion zones.

[00220] If the destination is within an exclusion zone a rejection is sent and alternatives offered, such as nearest possible safe point or choice to abandon the request. If the destination is approved then a confirmation is sent approving the request.

[00221] This process is described further with reference to Figure 10. Figure 10 illustrates a process flow, where a client wishes to apply for exclusion zone, shrouding or ghosting services at step 505. At step 510 the client creates a registry account if one does not exist and at step 515 the client logs onto their account. At step 520 the client is given the option or proposing exclusion zone, shrouding and/or ghosting options, which may be facilitated via the use of selecting, on a map, the area the client wishes to shroud, the area the client wishes to set as an exclusion zone.

[00222] At step 525, the client confirms their choices and any payments necessary. At step 530 the registry receives the client's application and step 535 the registry reviews the application and consults with third parties if relevant.

[00223] At step 540 the registry may approve, deny or propose amendments the client's application and, once all relevant parties accept the application at step 545, the client is invoiced and the application finalised.

[00224] At step 550 upon payment receipt, the registry takes the necessary action to update the database to exclude, shroud or ghost the area, device, machine or robot.

[00225] The devices, machines or robots are informed and begin obeying the updated privacy constraints.

[00226] In very select circumstances, waivers are obtainable to allow robots and participating devices to not be constrained by the 'privacy protocol'. In one embodiment, 'exclusion zones', 'shrouding (fixed)' and 'Profile shrouding (mobile)' may be waived for approved parents (running approved dedicated apps), so parents may monitor their children, for example:

(i) Parents would apply to the registry for a waiver;
(ii) Optional: parents would provide registry their child's Profile;
(iii) Parents' granted waiver.

[00227] Another aspect of the invention to ultimately restrict unencumbered operation or function (e.g. surveillance) opportunities.

[00228] It will be understood that the user may be provided with a time-limiting camera viewing (perhaps, when travelling in a particular class of exclusion zone). After the permissible time has expired a latency period may apply before the user is permitted another timed viewing, for example.

[00229] Turing to Figure 11, the process flow for privacy constraints is described in more detail. At step 565, the user logs onto their account and at step 570 the user initiates assignment or function instructions to the device, machine or robot. At step 575 the device, machine or robot instructions are relayed to the registry and consequently at step 580 the registry may process and regulate any instructions.

[00230] At step 585, the registry may relay clearance codes and relevant privacy constraints if any to the devices, machines or robots and at step 590 the user's device, machine or robot executes the assignment or function and conforms to any privacy constraints.

[00231] It will be understood that in other embodiments, indicated generally by arrows 2, 3, and 4, variations on the process flow are possible. For example, in accordance with process flow 2, when a user initiates an assignment or function instructions, at step 570 the relevant privacy constraints may be relayed to the user's device, machine or robot directly, at step 584 and the robot subsequently executes the assignment or function, conforming to any privacy constraints at step 590.

[00232] Alternate embodiments are also envisaged, where the user is not required to log into their account or to initiate an assignment or function. As shown generally by process flows 3 and 4, privacy constraints may be relayed to the user's device, machine or robot. These privacy constraints may then be utilised to either perform a function as shown at step 590 or may simply

be added to the robots door of information, for future use. The process flows shown generally by process flows 3 and 4 may be used in embodiments where instructions may be issued directly to the robot and not sent via the registry.

[00233] Referring to Figures 11a through to 11k, there are disclosed several computer implemented processes through which the policing process may operate. Figure 11a describes a Broad Process for Policing. The process steps are described briefly below.

Broad Process Steps (Policing)

1. Generate

   Generate Policing Initiative

   Firstly, a template is generated through the use of 'robometrics' (i.e. the collection of data when the when robot was enrolled at certification). Testing is preferred to detect the presence of an illicit substance or object (e.g. chemical, molecular or tangible signature), such as a weapon or dangerous device. Thereafter, a 'hail' signal is generated (e.g. identification request). Thirdly, a 'scene screen' is generated (e.g. search for or identify non-participants or 'rogue' robots). This step is explained in more detail with Figures 14, 15 and 16.

2. Assess (Optional)

   The enrolled template is tested to see if it matches a newly captured sample. For example, if a sample matches an enrolled template for an illicit or unapproved substance or object, or abnormal or unacceptable robometric, then this results in an enforcement trigger event.

   In another example, if a sample matches an enrolled normal or acceptable robometric, then this does not result in an enforcement trigger event.

   In yet another example, if a sample does not match an enrolled normal or acceptable robometric i.e. is outside tolerance or exceeding threshold, then this results in an enforcement trigger event.

   Secondly, has a satisfactory reply response been received? If no satisfactory reply, an enforcement trigger event occurs. Trigger events could include the fact that the robot is unregistered, has unapproved operations, or is operationally unworthy (e.g. faulty).

   Thirdly, is the extraneous robots in a scene? For example, no transponder signal results in an enforcement trigger event.

3. Respond

   Respond with Enforcement and/or Notify

   Passive enforcement strategies may include:

   - seizing the robot (e.g. generate performance/functionality/capability conditions/constraints such as do not operate further, remain at rendezvous location/position); or
   - launching a policing robot, track/trace/follow (e.g. to facilitate locating and apprehending user).

Active enforcement strategies may include:

- launching a policing robot, rendezvous with or near subject robot, capture (e.g. Grab or Net); or
- launching a policing robot, rendezvous with or near subject robot, disable/disarm (e.g. Jammer, Spoof, EMP or Projectile); and
- notify relevant stakeholders.

4. Amend (Optional)

Amending or revoking enforcement may include cancel enforcement pursuit (e.g. 'call off the chase'), call in reinforcements (e.g. more policing robots to assist), and/or revert to enforcement (e.g. trigger event)

Broad Process Steps (Conditions)

1. Generate

Generating condition/constraint may include generating performance/ functionality/capability constraint (e.g. regulations may stipulate constraints due to licence class, inadequate supporting infrastructure, network or systems, emergency provision trigger event and/or enforcement trigger event generates constraint).

Generated exclusion zone conditions may include:

- collocated location modules or transmission (fixed or mobile) (real-time or 'space teach');
- profile captures (fixed or mobile) (upload templates or PA/eL Profiles);
- coordinates + altitude (fixed); and/or
- 'no fly zone' or do not operate zone (in full or in part);

Generated shrouding conditions may include:

- 'do not watch' or no surveillance;
- collocated location module or transmission (fixed or mobile) (real-time or 'space teach');
- profile capture (fixed or mobile) (upload templates or PA/eL Profiles); and/or
- automatically recognise windows; similar to blurring out faces in Google Street View.

Generated ghosting conditions may include:

- 'do not ID' or no on-screen or HUD 'tagging';
- collocated location module or transmission (fixed or mobile) (real-time or 'space teach');
- profile capture (fixed or mobile) (upload templates or PA/eL Profiles); and/or
- coordinates + altitude (fixed).

Generated condition/constraint waiver or exemption may include:

- registered parties registered to that address/location/position;
- parents wishing to supervise their children;
- special permission (research purposes, government, etc.);
- stakeholder gives operation approval (e.g. for pick-up/delivery, agricultural surveillance, etc.); and/or
- 'condition' and 'constraint' can generally be used interchangeably.

2. Assess (Optional)

Assessing generated condition/constraint may include detecting:

- Is the constraint consistent with others?
- Is the exclusion zone suitable?
- Is the shrouding suitable?
- Is the ghosting suitable?
- Is the waiver or exemption suitable?

3. Respond

Responding by imposing condition/constraint may include determining:

- performance/functionality/capability constrained;
- exclusion zone parameters imposed;
- shrouding conditions imposed;
- ghosting conditions imposed; and/or
- waiver or exemption imposed.

[00234] With reference to Figures 12 and 13, there may be provided mechanisms to allow for robots to be initially detected through a sense/scan protocol and to be subsequently seized using a seizure protocol.

[00235] Referring now to Figure 12, there is shown a process flow for the process that occurs if a sense/scan protocol is initiated. A sense/scan protocol may be initiated as a result of the robot performing a function, such as the function process flow shown generally at Figure 11 or a sense/scan protocol may be initiated independently of any user instructions to the robot at step 605.

[00236] At step 608 or 610, the user's robot becomes aware of a situation where a sense/scan operation is required.

[00237] If a positive result is achieved, at step 615 a seizure protocol may be initiated. If a seizure protocol is initiated at step 617 then the process of sense/scan ends at step 630. If a seizure protocol is not initiated then the users robot proceeds as normal at step 620 and the users robot may complete the user assignment or function at step 625 or alternatively the users

robot may return to the location prior to the sense/scan protocol being initiated at step 623 prior to the process ending at step 630.

[00238] Referring now to Figure 13, there is shown a process flow for a seizure protocol, such as the seizure protocol referred to in Figure 12. At step 555 or 705, a seizure protocol is initiated as a result of either an independent request or as a result of a sense/scan operation as shown Figure 12. This may result in the user robot travelling to a designated seizure position at step 708 or the user's robot deviating from travel plans to execute seizure protocol at step 710. Once the seizure has been performed, the process ends at step 715.

[00239] A system that allows the registry to police the environment of robots that may be unregistered, unlawful, a danger to the public, an invasion to people's privacy or operating improperly, perhaps, even stolen. Herewith these robots will be referred to as 'rogue robots'.

[00240] The Registry's system utilises its monitoring, controlling and managing capabilities (not limited to the fact that it may oversee the travel paths and tracks of a vast variety of robots)—may, in one embodiment, grant it special abilities or opportunities to police the environment for rogue robots.

[00241] In another embodiment, the registry may 'discover' rogue robots by employing the assistance of non-registry robots (e.g. consumers' robots) operating in or near particular spaces. Preferably, consumers' robots may feed environmental data back to the registry or process environment locally then send results to the registry. In either method, the registry may utilise the on-board sensors and scanners of consumers' robots, specifically monitor their travel environment for rogue robots, i.e. robots that should not be encountered, perhaps, by the consumers' robot's 'anti-collision and avoid' detector or module.

[00242] This initiative of employing the help of consumer's robots may also allow the tracking of rogue robots that are initially detected. In one embodiment, as each consumer robot detects the presence or signature of a particular rogue robot the current position of each respective consumer robot that detected the rogue robot and/or the position the rogue robot was detected as being by each consumer robot may allow track plotting (and this may be in multiple dimensions).

[00243] However, ghosting may also be applied to, preferably, tangibles that are recognised via other means, that is, not by Profile recognition methods. For example, a tangible may not be identified or tagged if it is located within a zone that has been excluded (perhaps, by a client selecting it on a 3D map) or if it is associated (e.g. collocated) with a location module device (e.g. smartphone with geo-location features).

[00244] In other words, the Registry's system may, in a first instance, 'spot' or identify all robots in a particular environment, then eliminate from its electronic field of view all robots that are registered or that are known to be operating there following the issue of clearance codes (i.e. removing robots that are not rogues). Thus, if there are any robots remaining after this elimination process, by deduction, the remaining robots may be deemed 'off the grid' or rogue operators.

[00245] In addition, the registry may conduct such investigations using a variety of methods. In one method, the registry deploys at least one robot of its own to track the rogue robot to its destination (hopefully, to where the user is located) or, perhaps, to (safety) deactivate the rogue

robot using a number of means (e.g. one ideal embodiment may be overriding or 'spoofing' its communications system to inflict the Registry's 'seizure protocol').

[00246] The registry, over time, builds up a library or inventory of signatures (not limited to acoustic) for a variety of robots, such signatures may be assigned to particular robot types.

[00247] Referring to Figure 14, there is shown an example of a two-dimensional environment with all detected robots identified pictorially by the Registry's system.

[00248] Referring to Figure 15, there is shown an example of a two-dimensional environment with all registered or non-rogue robots eliminate from view (selectively removed) in order to show any remaining (rogue) robots.

[00249] Robots 735 and 740 remain in view. These robots are deemed not registered. Further, rogue robot 740 has been listed as having an unrecognisable signature (illustrated by its unique symbol). Whereas 735 was detected as having a familiar signature, was listed as being a 'Concentric Circle' Type robot, according to the Registry's database analysis.

[00250] Referring to Figure 16, there is shown an example situation, which is a streetscape with various participants 803, 805, 807, 809, 811, 813, 817, 819, 821, 823 and 825 and non-participants 801 and 815 present.

[00251] Participants may act as detector nodes and/or (mobile) repeater stations—respectively, facilitating detection of non-participants and assisting to relay any alert notices or other relevant data to other participants. The mechanism of action may resemble (signal) propagation. [In the figure, 'R' may equate to a 'registered' status.]

[00252] In the first instance, 803 captures a greater than partial match of a non-participating device, machine or robot 801. This match percentage value is deemed significant enough to warrant an alert be transmitted (in)directly to nearby participants 805 and 807, which both are positioned with the alert radius.

[00253] In another instance, multiple participants 809, 811 and 813 capture only partial matches of a non-participating device, machine or robot 815. Individually these partial matches may not be enough to elicit an alert be distributed, however considering there are multiple, these matches synergistically equate to a percentage value deemed significant enough to warrant an alert be transmitted (in)directly to nearby participants 819 and 817, which both are positioned with the alert radius; further, original detectors 809, 811 and 813 would similarly be alerted, advising them that, yes, their partial matches were relevant.

[00254] Meanwhile, participants 821, 823 and 825, since outside any alert radius or positioned away from any non-participant, have not been involved in any of the above instances.

Advantages

[00255] One of the advantages of the embodiments and broader invention described herein is that the invention removes the onus or control from consumers (i.e. owners of the robots) to assume full responsibility for the actions of the robots at any given time. So long as the commands are filtered or processed through a central server system, then illegal, immoral or accidental use of autonomous and robotic devices is greatly reduced.

[00256] If robots were unrestricted in their activities (operations or functions), were able to venture into particular spaces unhindered (with or without explicit instructions or control from the

user), then this would cause or provoke contentious issues—some of which include, privacy, safety, security, liability, technical and ethical issues. Therefore, the system provides a mechanism and framework by which robots and/or their controllers are required to obtain the relevant clearance before an operation is allowed, particularly if that operation is to occur in a public space.

[00257] Moreover, as consumers are required to register and identify themselves, the system provides an ability to monitor, control or manage the actions or activities of consumers, in so far as it is related to their robot use. This reflects society's general interest in requiring people to obtain licenses to drive cars, pilot aircraft or own and use firearms.

[00258] That is, there is a public interest in preventing users from allowing their robots to be used by unapproved users, or from having their robots unknowingly used by unapproved users. Such robots may possess the capacity and capabilities to perform restricted (e.g. dangerous) functions. These occurrences would first and foremost present safety issues, e.g. robots (owned by parents) being used by underage children that are not listed as or approved to be registered users.

[00259] As a corollary, there are fewer onuses on robot and autonomous system provides from being responsible for facilitating vital robot updates. Instead, all updates would be processed by and issued from the system described herein, irrespective of the robot's origin of manufacture, country or space of operation. This ameliorates the legal liability of robot and autonomous system providers.

[00260] Advantages of the embodiments described herein where the embodiment is fulfilled by a separate device to the robot or by a remote server include:

(1) potential for the robot to have more frequent communication with an external regulating server (e.g. providing a greater assurance or security level of third party regulation or supervision);

(2) potential for a remote server to process or facilitate remote diagnostic services; and

(3) more frequent receipt by the robot of software, updates and/or flashes from the remote server.

[00261] Further advantages of a user and/or the user's 'smart' device or robot pendant communicating indirectly, or not at all, with the robot, e.g. via the remote server, include no 'lost in translation' events as the remote server (Robot Registry) receives proposed commands or operation requests, directly from the source, i.e. the user or the user's device. In other words, the remote server acts as an intermediary between the user (or their device) and the robot.

Disclaimers

[00262] Throughout this specification, unless the context requires otherwise, the word "comprise" or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated inte.g.er or group of integers but not the exclusion of any other inte.g.er or group of integers.

[00263] Those skilled in the art will appreciate that the invention described herein is susceptible to variations and modifications other than those specifically described. The invention includes

all such variation and modifications. The invention also includes all of the steps, features, formulations and compounds referred to or indicated in the specification, individually or collectively and any and all combinations or any two or more of the steps or features.

[00264] Other definitions for selected terms used herein may be found within the detailed description of the invention and apply throughout. Unless otherwise defined, all other scientific and technical terms used herein have the same meaning as commonly understood to one of ordinary skill in the art to which the invention belongs.

[00265] Although not required, the embodiments described with reference to the method, computer program, data signal and aspects of the system can be implemented via an application programming interface (API), an application development kit (ADK) or as a series of program libraries, for use by a developer, for the creation of software applications which are to be used on any one or more computing platforms or devices, such as a terminal or personal computer operating system or a portable computing device, such as a smartphone or a tablet computing system operating system, or within a larger server structure, such as a 'data farm' or within a larger transaction processing system.

[00266] Generally, as program modules include routines, programs, objects, components and data files that perform or assist in the performance of particular functions, it will be understood that the functionality of the software application may be distributed across a number of routines, programs, objects or components to achieve the same functionality as the embodiment and the broader invention claimed herein. Such variations and modifications are within the purview of those skilled in the art.

[00267] It will also be appreciated that where methods and systems of the present invention and/or embodiments are implemented by computing systems or partly implemented by computing systems then any appropriate computing system architecture may be utilised. This includes standalone computers, network computers and dedicated computing devices (such as field-programmable gate arrays).

[00268] Where the terms "computer", "computing system" and "computing device" are used in the specification, these terms are intended to cover any appropriate arrangement of computer hardware for implementing the inventive concept and/or embodiments described herein.

[00269] Where the terms "robotic device", "autonomous device" and "smart device" are used in the specification, these terms are intended to cover any appropriate device which is capable of receiving a command and utilising the command to perform a function, which may be either a "physical" function (i.e. movement) or a "virtual" function (e.g. interact with another device via electronic commands).

[00270] Where reference is made to communication standards, methods and/or systems robots or devices may transmit and receive data via a variety of forms: 3G, 4G (CDMA/GSM), Wi-Fi, Bluetooth, other radio frequency, optical, acoustic, magnetic, GPS/GPRS, or any other form or method of communication that may become available from time to time.

CLAIMS

1. A system for controlling at least one robotic device, comprising a computing device capable of communication with at least one robotic device and arranged to receive at least one command from a command module, the command being arranged to contain at least one instruction which is arranged to effect an operation on the robotic device and identification information to identify the at least one robotic device, wherein the computing device includes a processor and a database, the processor being arranged to receive the command and review the command against information in the database to determine whether the command is suitable for execution by the at least one robotic device, wherein the command is provided to the robotic device if the command is suitable for execution.

2. A system in accordance with Claim 1, wherein the processor determines whether the command is associated with at least one authorisation code.

3. A system in accordance with Claim 2, wherein the at least one authorisation code is received independently of the at least one command.

4. A system in accordance with Claim 1, 2 or 3, wherein the processor determines whether the command is one of a predetermined set of commands by accessing a set of predetermined commands stored in the database.

5. A system in accordance with any one of Claims 1 to 5, wherein at least one of the at least one command, the authorisation code and the identification code is encrypted.

6. A system in accordance with Claim 5, comprising the further step of decrypting the at least one of the at least one command, the authorisation code and the identification code prior to reviewing the command to determine whether the command is suitable for execution.

7. A system in accordance with any one of Claims 1 to 6, wherein at least one of the at least one command, the authorisation code and the identification code includes a checksum, wherein the checksum is utilised to determine the correctness of the at least one command, the authorisation code and the identification code.

8. A system in accordance with any one of the preceding claims, wherein the robotic device is a programmable device.

9. A system in accordance with any one of the preceding claims, wherein the robotic device includes at least one processor arranged to receive and execute the at least one command.

10. A system in accordance with any one of the preceding claims, wherein the robotic device is capable of performing at least one physical function.

11. A system for controlling a robotic device, comprising a computing device capable of receiving at least instruction, a processor capable of generating a command based on the at least one instruction, wherein the command is one of communicated via the computing device to initiate a response based on the at least one generated command.

12. A system in accordance with Claim 11, wherein the processor requests further information to further assess the instruction, prior to initiating a response.

13. A method for controlling a robotic device, comprising the steps of, receiving at a computing device at least one command arranged to effect an operation on the robotic device, reviewing the command to determine whether the command is suitable for execution, wherein the command is provided to the device only if the command is suitable for execution.

14. A system in accordance with Claim 13, wherein the step of reviewing the command includes the step of determining whether the command is associated with at least one authorisation code.

15. A system in accordance with Claim 14, wherein the at least one authorisation code is received independently of the at least one command.

16. A method in accordance with Claim 13, 14 or 15, wherein the step of reviewing the command includes the further step of determining whether the command is one of a predetermined set of commands.

17. A method in accordance with any one of Claims 13 to 16, comprising the further step of the computing device receiving at least one identification code arranged to identify the robotic device.

18. A method in accordance with Claim 17, comprising the further step of receiving the identification code with the at least one command.

19. A method in accordance with any one of Claims 13 to 18, wherein at least one of the at least one command, the authorisation code and the identification code is encrypted.

20. A method in accordance with Claim 19, comprising the further step of decrypting the at least one of the at least one command, the authorisation code and the identification code prior to reviewing the command to determine whether the command is suitable for execution.

21. A method in accordance with any one of Claims 13 to 20, wherein at least one of the at least one command, the authorisation code and the identification code includes a checksum, wherein the checksum is utilised to determine the correctness of the at least one command, the authorisation code and the identification code.

22. A method in accordance with any one of Claims 13 to 21, wherein the robotic device is a programmable device.

23. A method in accordance with any one of Claims 13 to 22, wherein the robotic device includes at least one processor arranged to receive and execute the at least one command.

24. A method in accordance with any one of Claims 13 to 23, wherein the robotic device is capable of performing at least one physical function.

25. A system for controlling a robotic device, comprising a computing device in communication with the robotic device and arranged to receive at least one command which is arranged to effect an operation on the robotic device, wherein the computing device reviews the command to determine whether the command is suitable for execution, and the command is provided to the device only if the command is suitable for execution.

26. A computer program including at least one command, which, when executed on a computing system, is arranged to perform the method steps of at least one of Claims 13 to 24.

27. A computer readable medium incorporating a computer program in accordance with Claim 26.

28. A data signal encoding at least one command and being arranged to be receivable by at least one computing device, wherein, when the encoded command is executed on the computing system, the computing system performs the method steps of at least one of Claims 13 to 24.

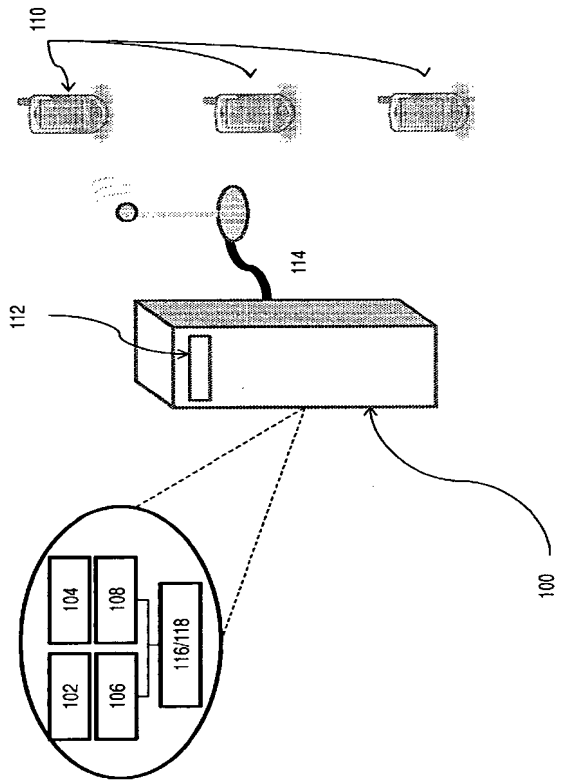


Figure 1

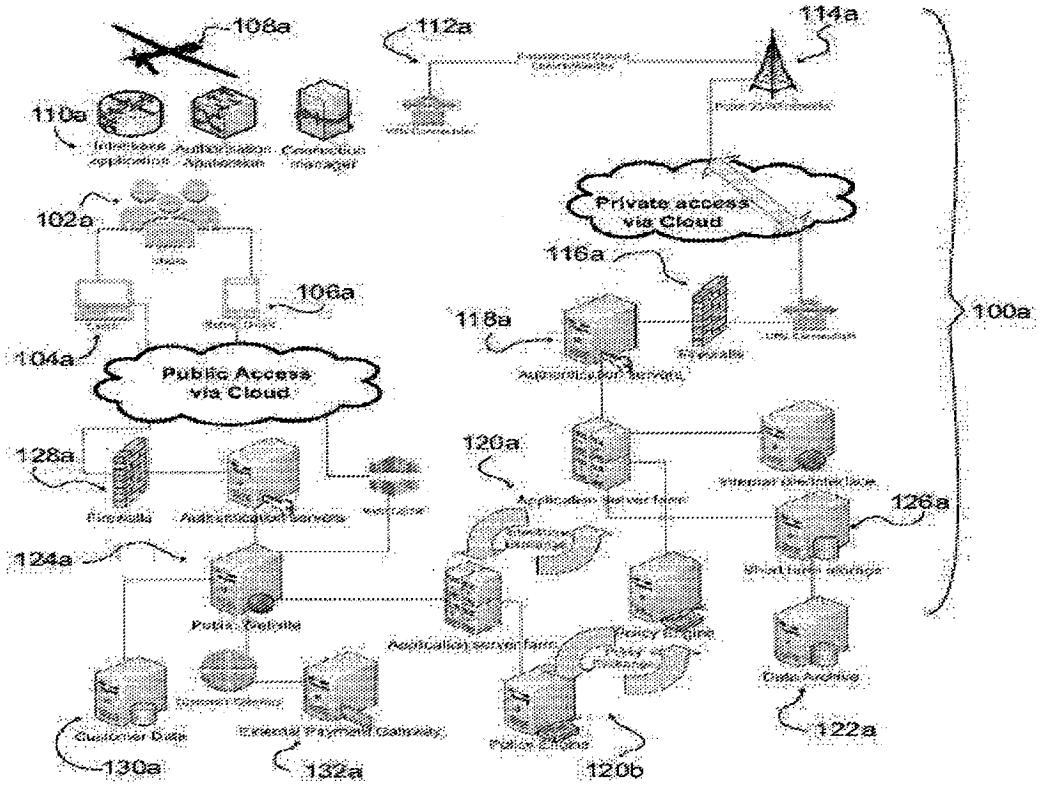

108a
112a
114a
110a
102a
Private access via Cloud
116a
106a
118a
100a
104a
Public Access via Cloud
128a
120a
126a
124a
122a
130a
132a
120b

Figure 2

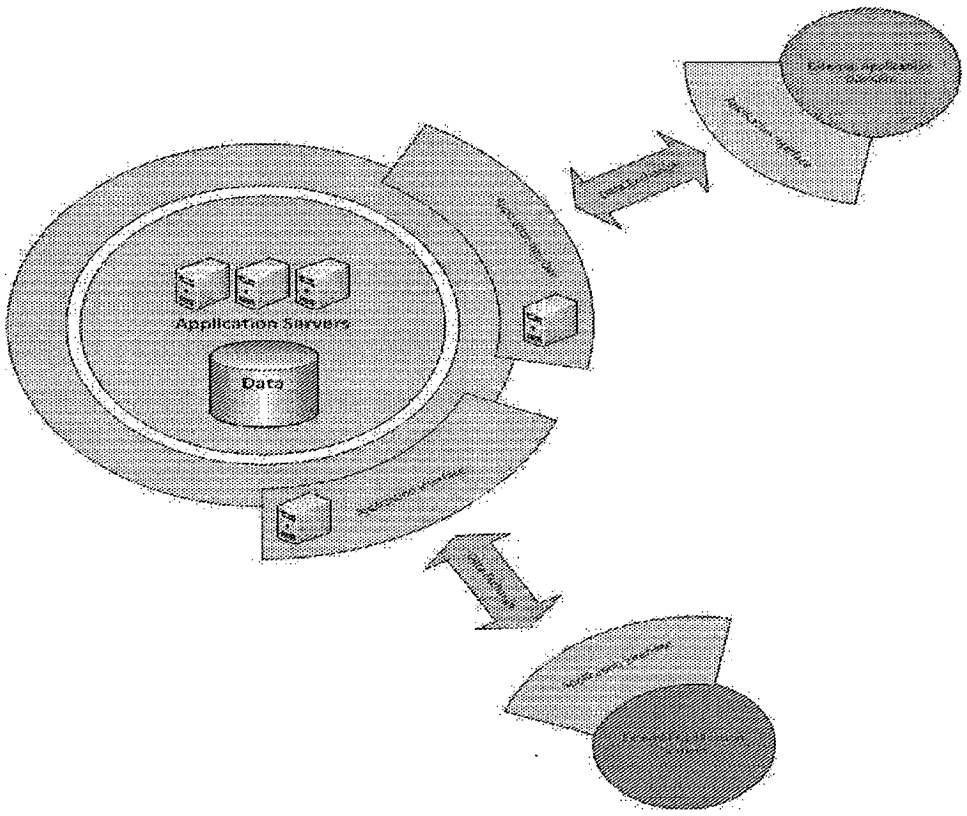


Figure 2a

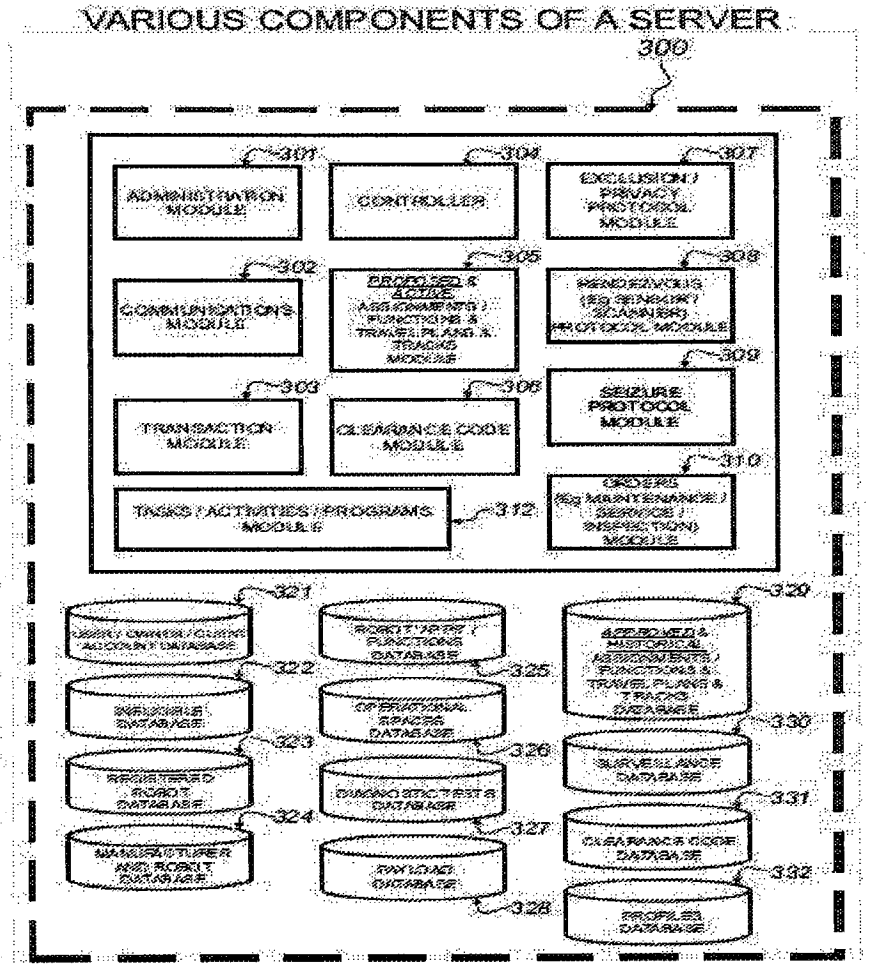

VARIOUS COMPONENTS OF A SERVER
300
301
ADMINISTRATION MODULE
304
CONTROLLER
307
EXCLUSION / PRIVACY PROTOCOL MODULE
302
COMMUNICATIONS MODULE
305
PROFILED & ACTIVE ASSIGNMENTS / FUNCTIONS & TRAVEL PLANS & TRACKS MODULE
308
HAND DEVICES (Eg SENSOR / SCANNER) PROTOCOL MODULE
309
SEIZURE PROTOCOL MODULE
303
TRANSACTION MODULE
306
CLEARANCE CODE MODULE
310
ORDERS (Eg MAINTENANCE / SERVICE / INSPECTION) MODULE
TASKS / ACTIVITIES / PROGRAMS MODULE
312
321
322
323
324
325
326
327
328
329
330
331
332

Figure 3

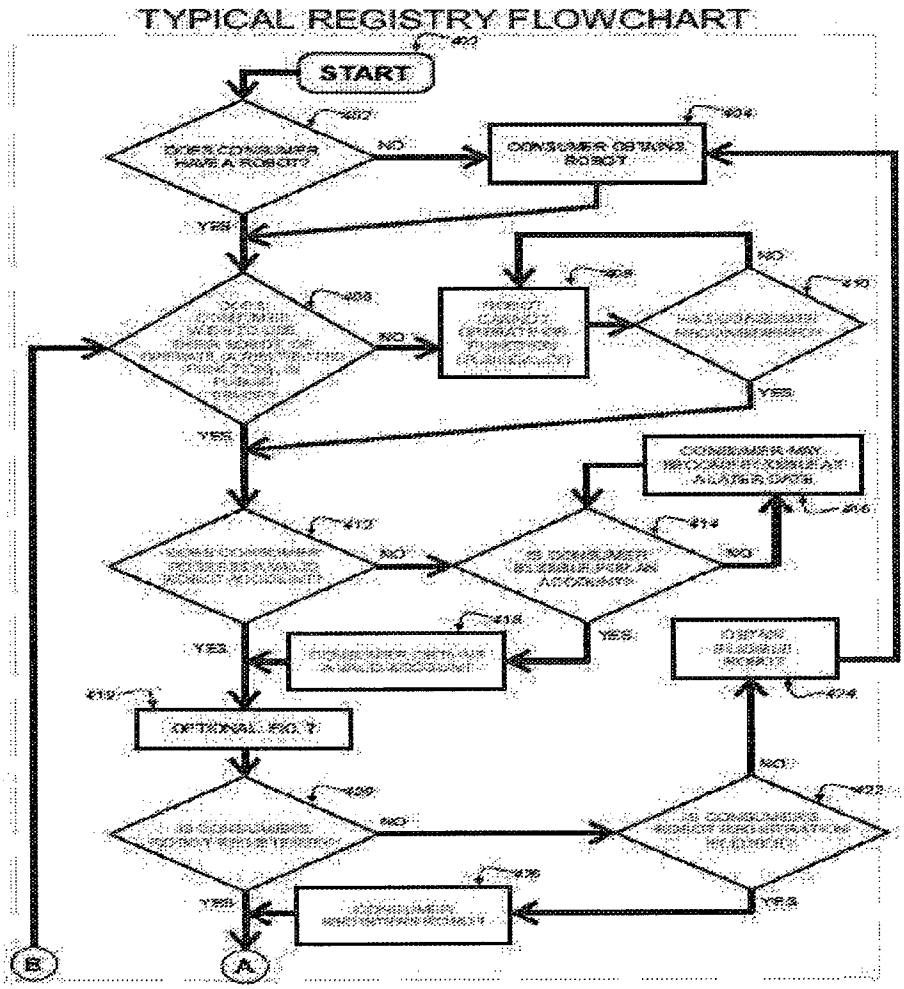


Figure 4

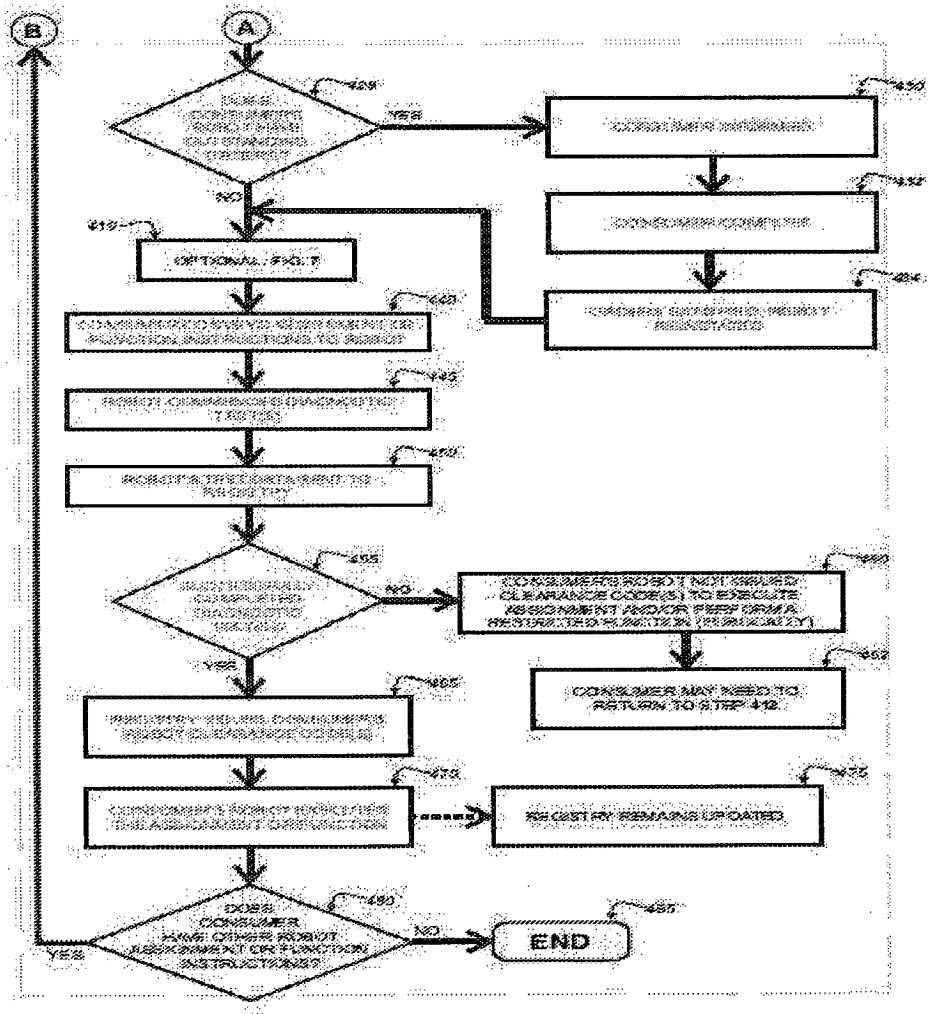


Figure 5

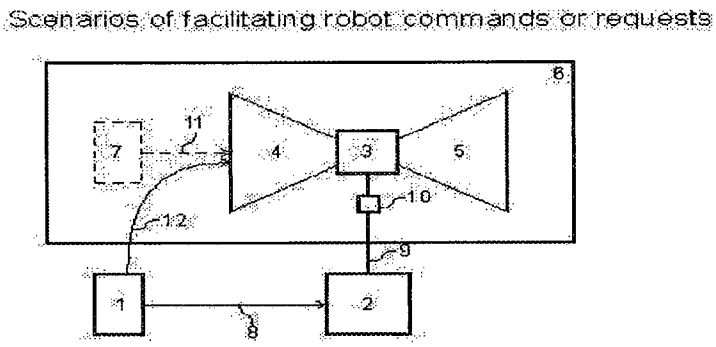

Scenarios of facilitating robot commands or requests
6
7
11
4
3
5
10
12
9
1
2
8

Figure 5a

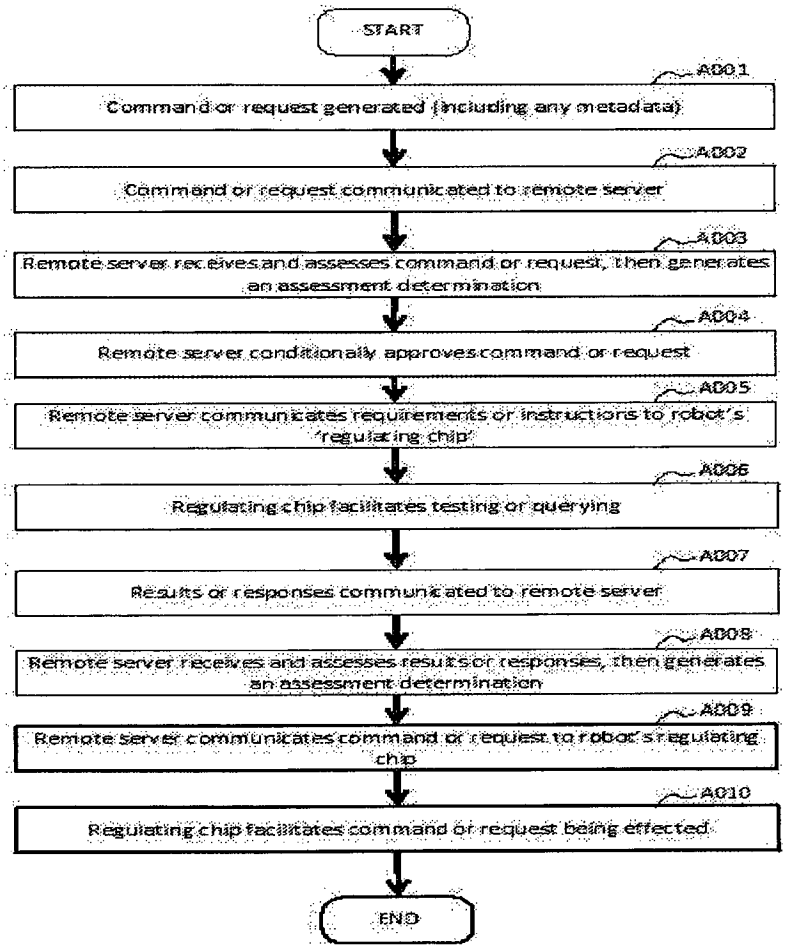

START
A001
Command or request generated (including any metadata)
A002
Command or request communicated to remote server
A003
Remote server receives and assesses command or request, then generates an assessment determination
A004
Remote server conditionally approves command or request
A005
Remote server communicates requirements or instructions to robot's regulating chip
A006
Regulating chip facilitates testing or querying
A007
Results or responses communicated to remote server
A008
Remote server receives and assesses results or responses, then generates an assessment determination
A009
Remote server communicates command or request to robot's regulating chip
A010
Regulating chip facilitates command or request being effected
END

Figure 5b

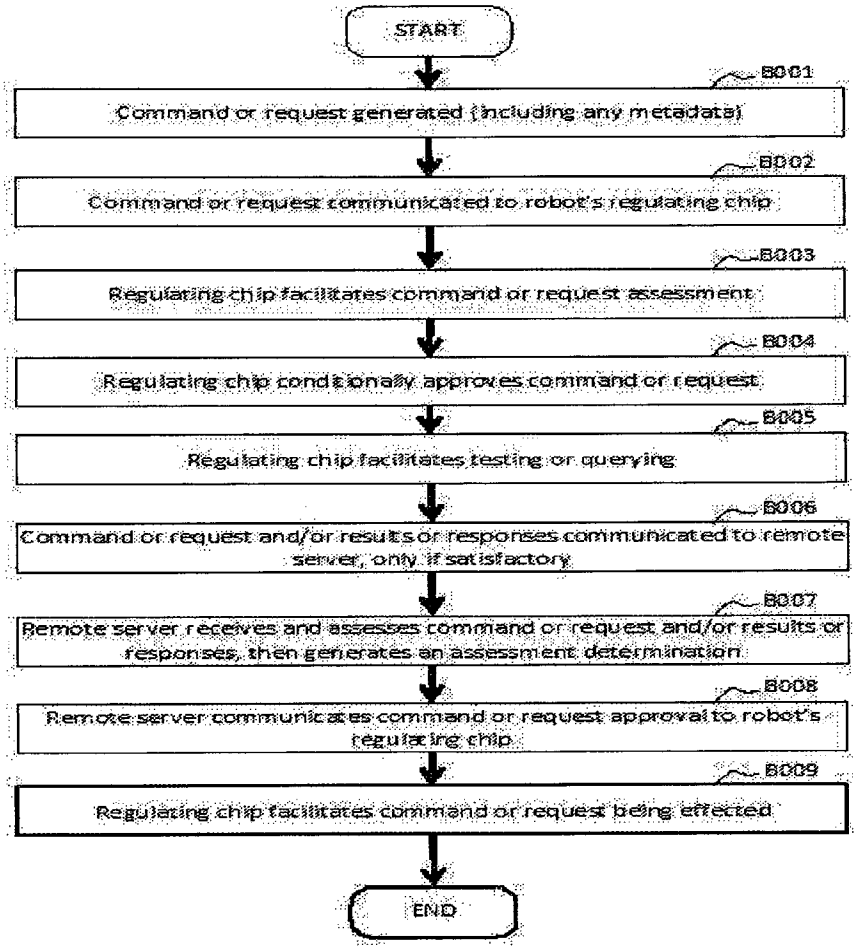

START
B001
Command or request generated (including any metadata)
B002
Command or request communicated to robot's regulating chip
B003
Regulating chip facilitates command or request assessment
B004
Regulating chip conditionally approves command or request
B005
Regulating chip facilitates testing or querying
B006
Command or request and/or results or responses communicated to remote server, only if satisfactory
B007
Remote server receives and assesses command or request and/or results or responses, then generates an assessment determination
B008
Remote server communicates command or request approval to robot's regulating chip
B009
Regulating chip facilitates command or request being effected
END

Figure 5c

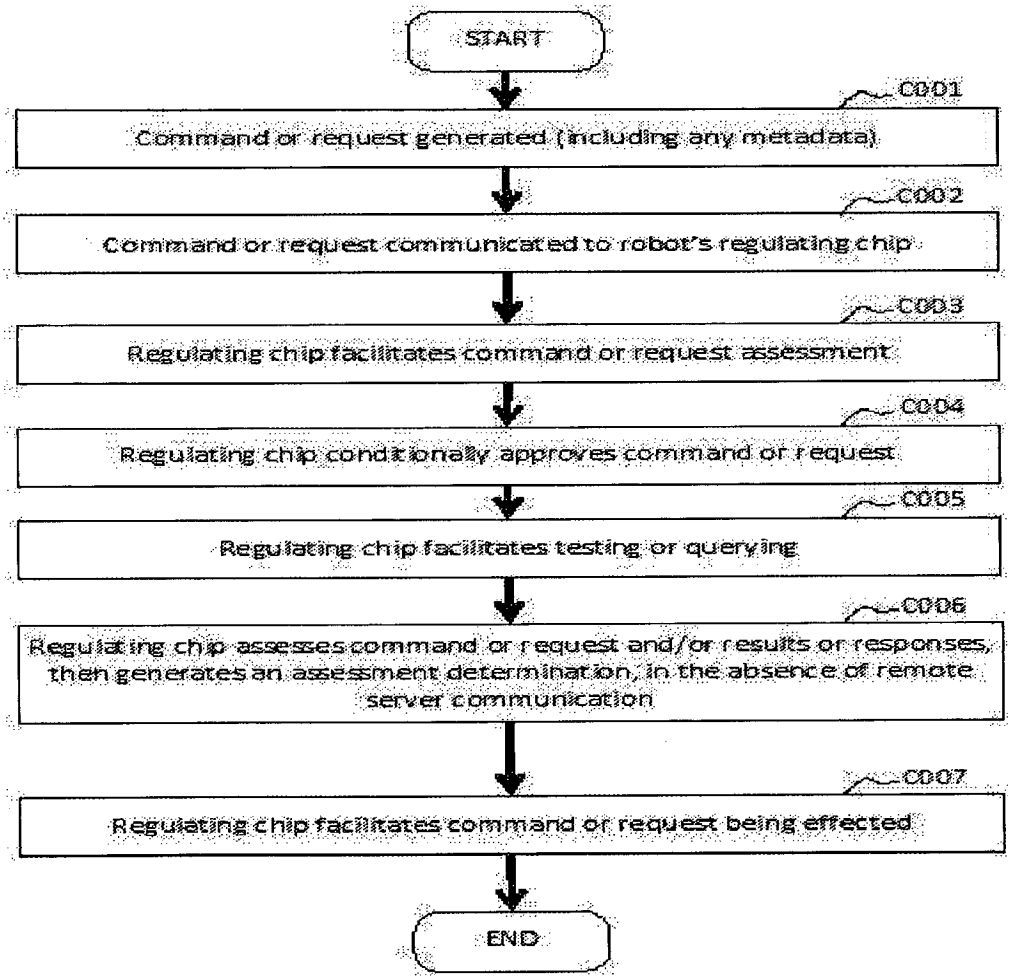

START
C001
Command or request generated (including any metadata)
C002
Command or request communicated to robot's regulating chip
C003
Regulating chip facilitates command or request assessment
C004
Regulating chip conditionally approves command or request
C005
Regulating chip facilitates testing or querying
C006
Regulating chip assesses command or request and/or results or responses, then generates an assessment determination, in the absence of remote server communication
C007
Regulating chip facilitates command or request being effected
END

Figure 5d

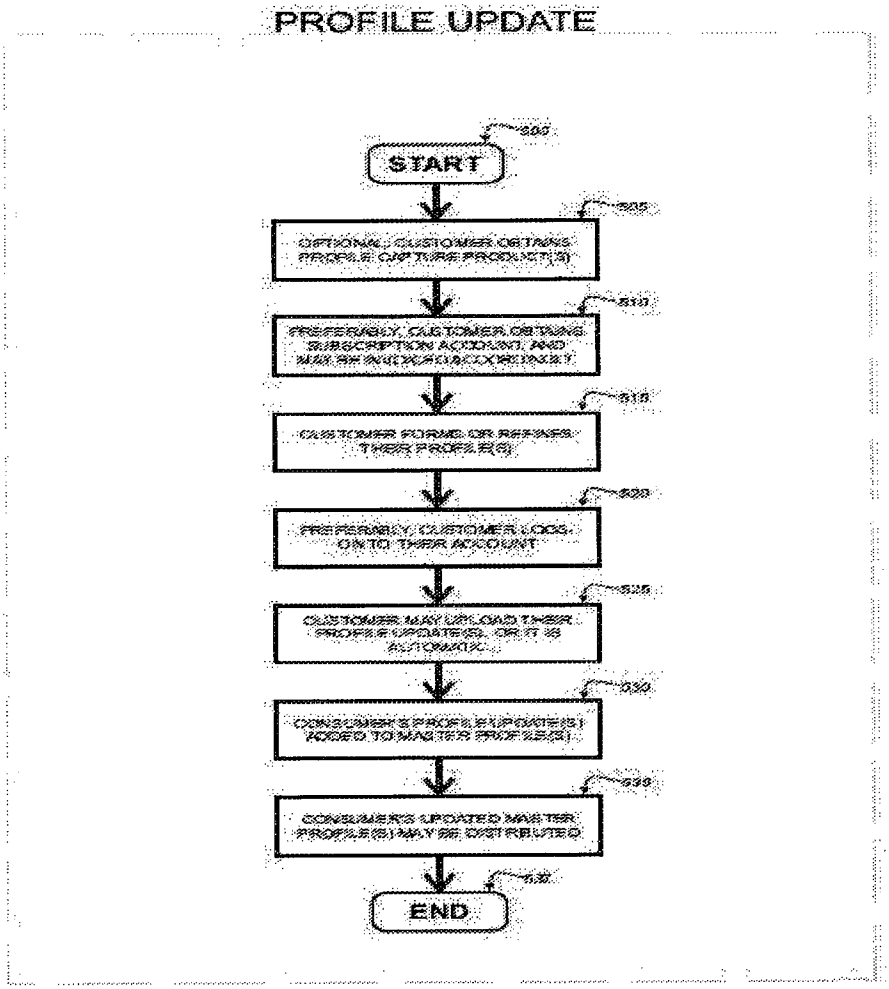


Figure 6

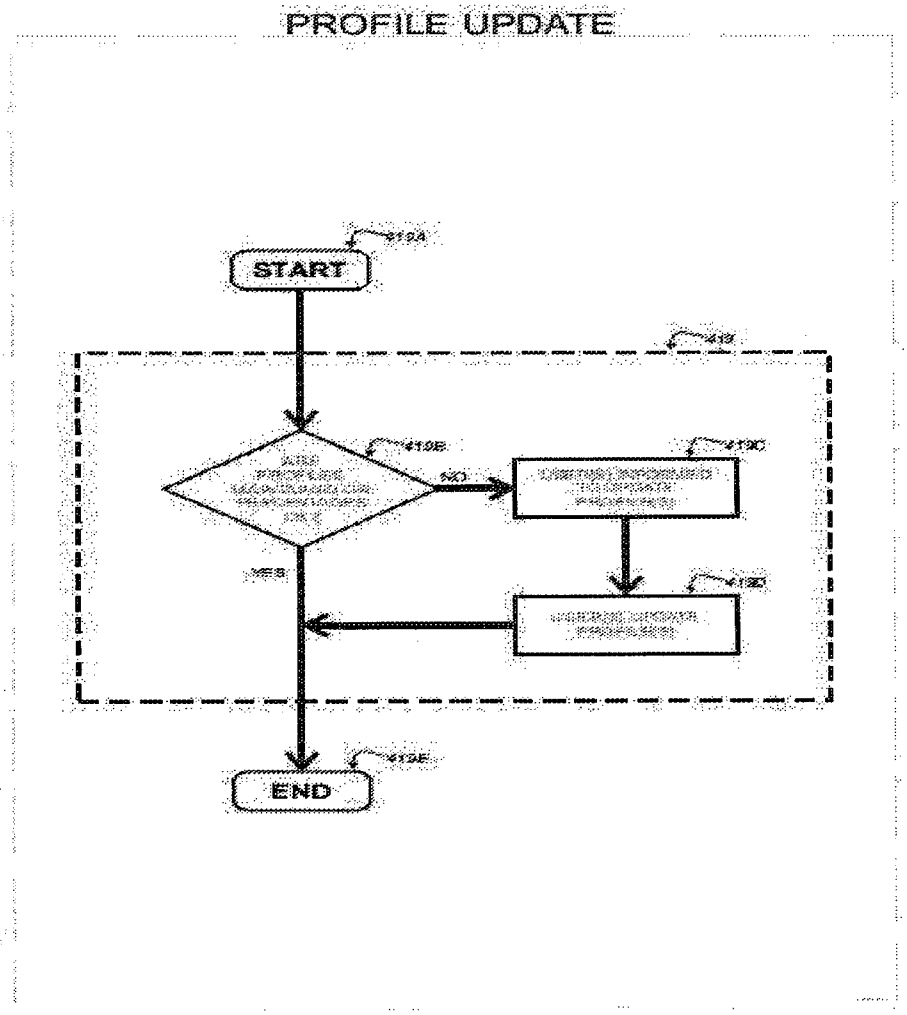


Figure 7

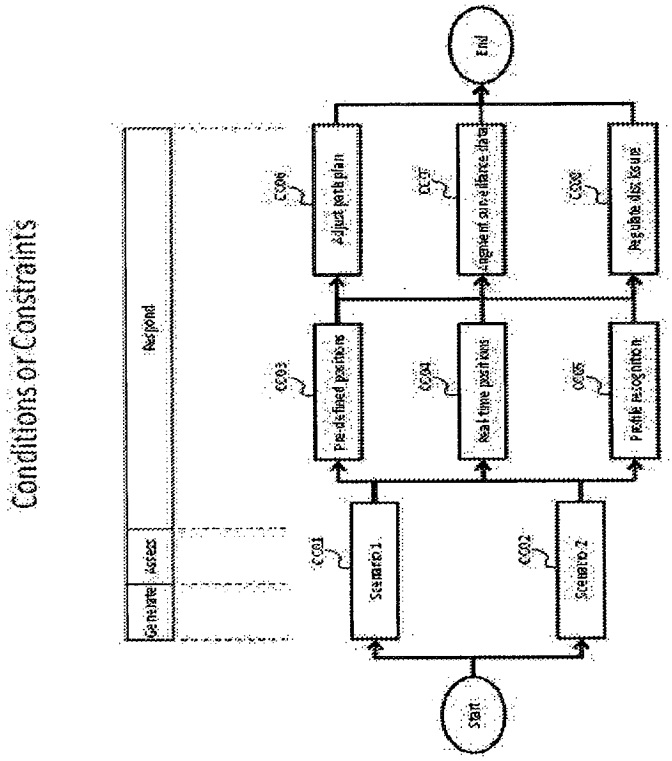

Conditions or Constraints
Respond
Assess
Generate
End
Start
Scenario 1
Scenario 2
Pre-defined positions
Real-time positions
Pirate recognition
Adjust path plan
Regulate distribute
CC01
CC02
CC03
CC04
CC05
CC06
CC08

Figure 7a

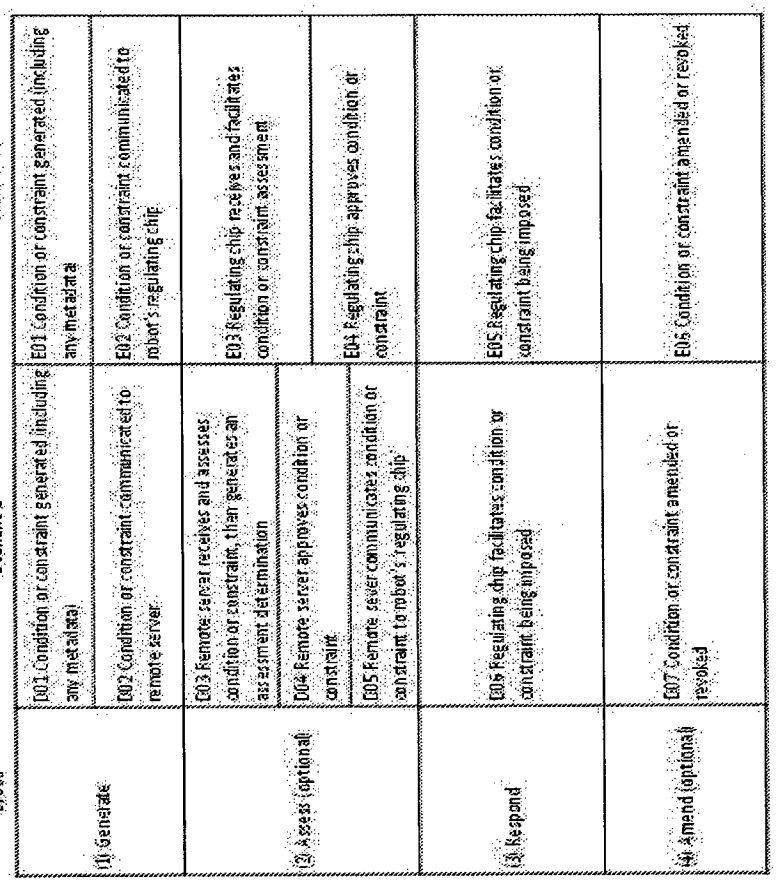

Scenario 1 and 2
Broad
Scenario 1
Scenario 2
(1) Generate
E01 Condition or constraint generated (including any metadata)
E02 Condition or constraint communicated to robot's regulating ship
(2) Assess (optional)
E03 Remote server receives and assesses condition or constraint, then generates an assessment determination
E04 Remote server approves condition or constraint
E05 Remote server communicates condition or constraint to robot's regulating ship
E03 Regulating ship receives and facilitates condition or constraint assessment
E04 Regulating ship approves condition or constraint
(3) Respond
E06 Regulating ship facilitates condition or constraint being imposed
E06 Regulating ship facilitates condition or constraint being imposed
(4) Amend (optional)
E07 Condition or constraint amended or revoked
E08 Condition or constraint amended or revoked

Figure 7b

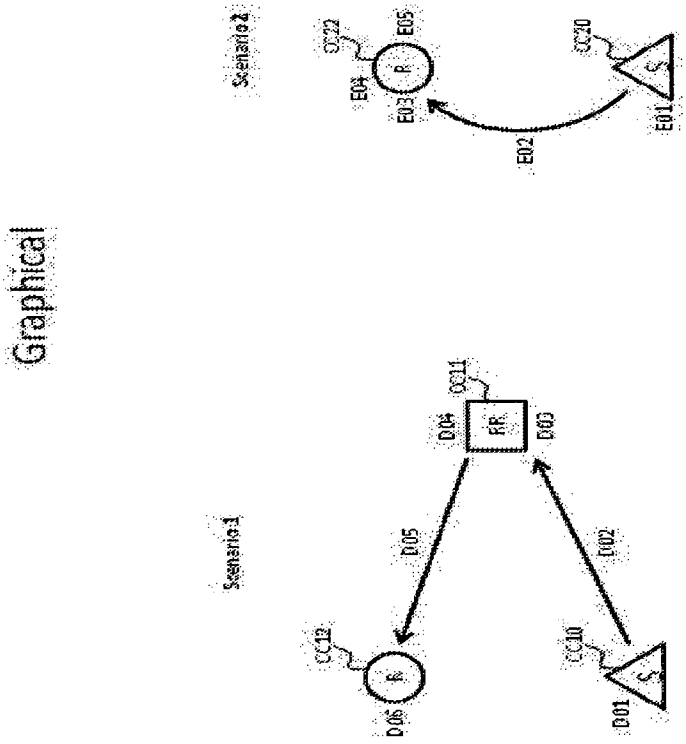

Graphical
Scenario 4
CC22
E05
E04
R
E03
E02
CC20
S
E01
Scenario 3
CC11
D04
RR
D03
D05
D02
CC12
R
D06
CC10
S
D01

Figure 7c

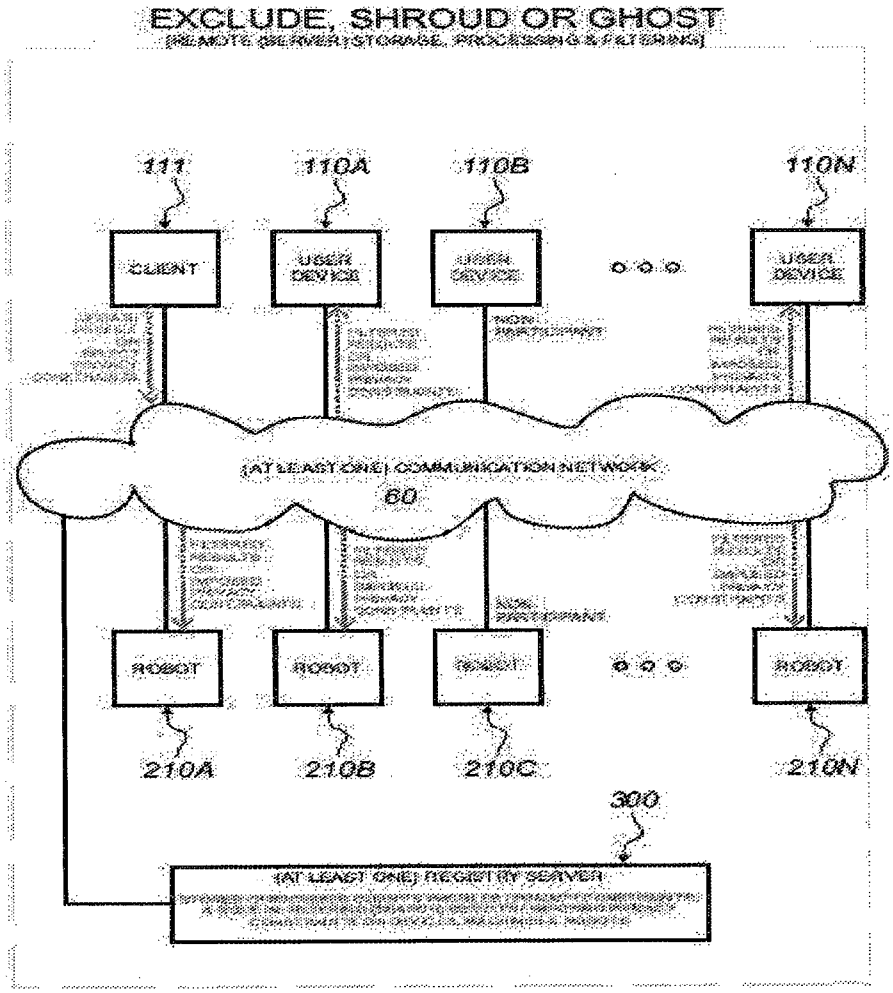

EXCLUDE, SHROUD OR GHOST
111
110A
110B
110N
CLIENT
USER DEVICE
USER DEVICE
USER DEVICE
(AT LEAST ONE) COMMUNICATION NETWORK
60
ROBOT
ROBOT
ROBOT
ROBOT
210A
210B
210C
210N
300
(AT LEAST ONE) REGISTRY SERVER

Figure 8

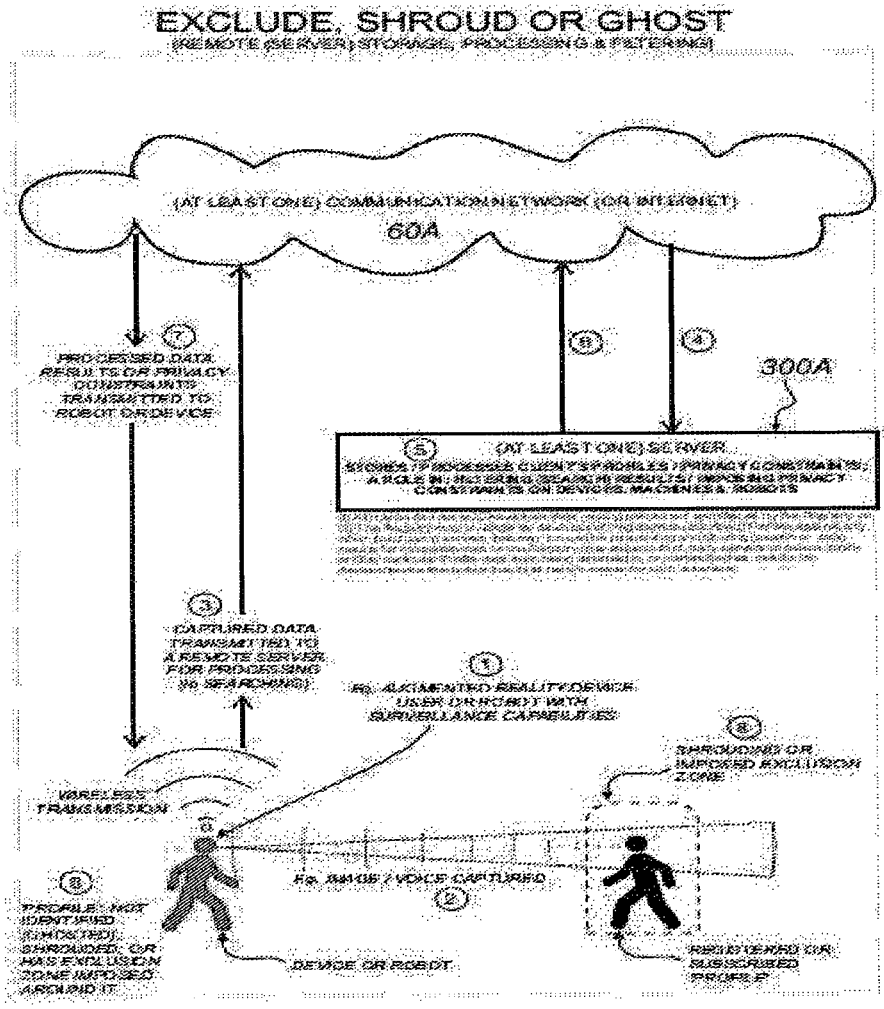

EXCLUDE, SHROUD OR GHOST
(REMOTE (SERVER) STORAGE, PROCESSING & NETWORK)
(AT LEAST ONE) COMMUNICATION NETWORK (OR INTERNET)
60A
300A
(AT LEAST ONE) SERVER
PROCESSED DATA RESULTS OR PRIVACY CONSTRAINTS TRANSMITTED TO ROBOT OR DEVICE
CAPTURED DATA TRANSMITTED TO A REMOTE SERVER FOR PROCESSING (IN SEARCHING)
WIRELESS TRANSMISSION
SHROUDING OR IMPOSED EXCLUSION ZONE
IMAGE / VOICE CAPTURED
DEVICE OR ROBOT
RFID TAGGED OR MUSCRUBED PROFILE

Figure 9

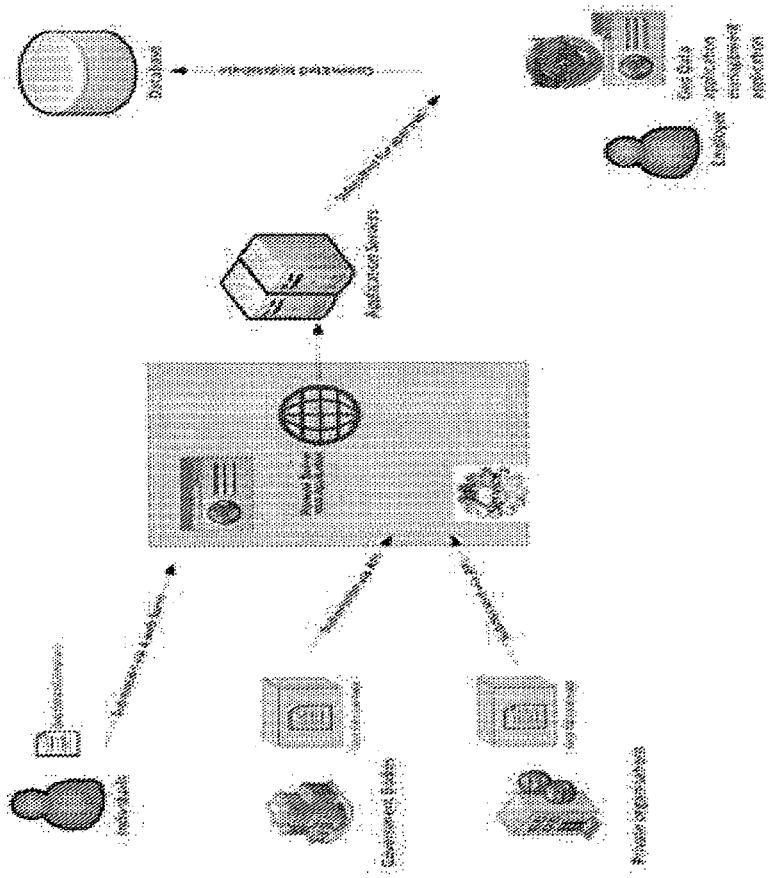


Figure 9a

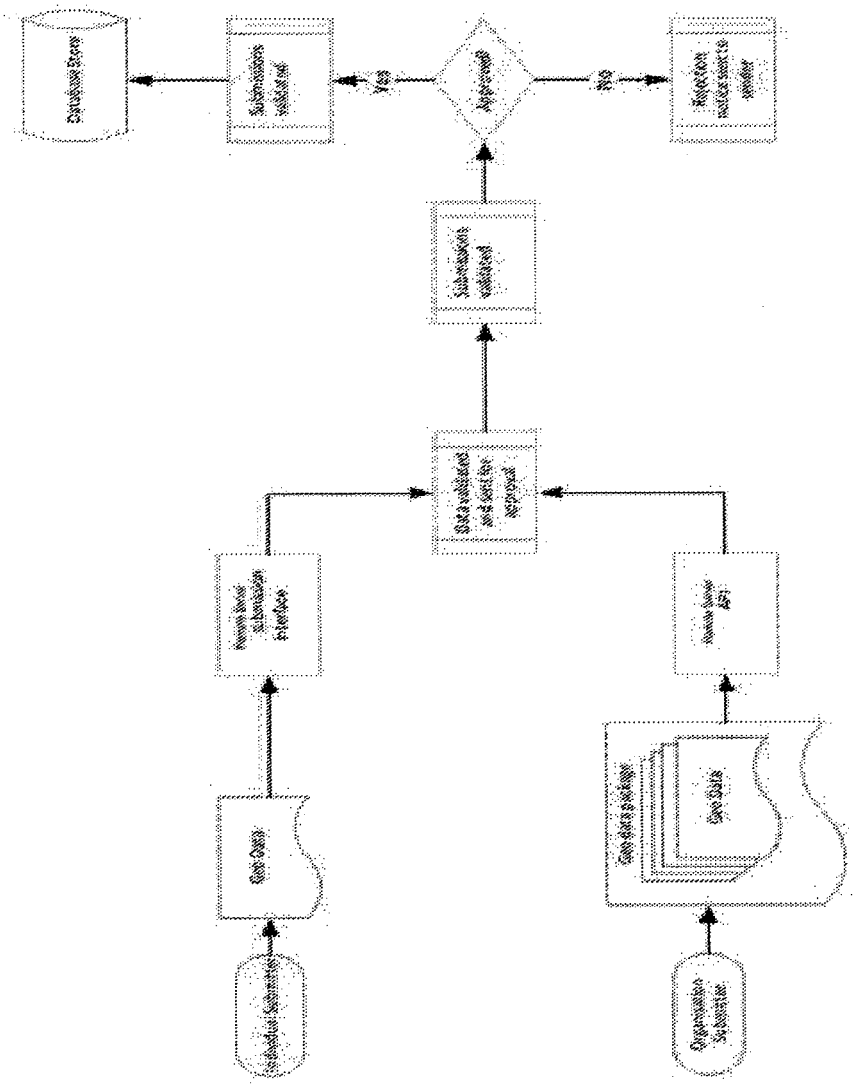


Figure 9b

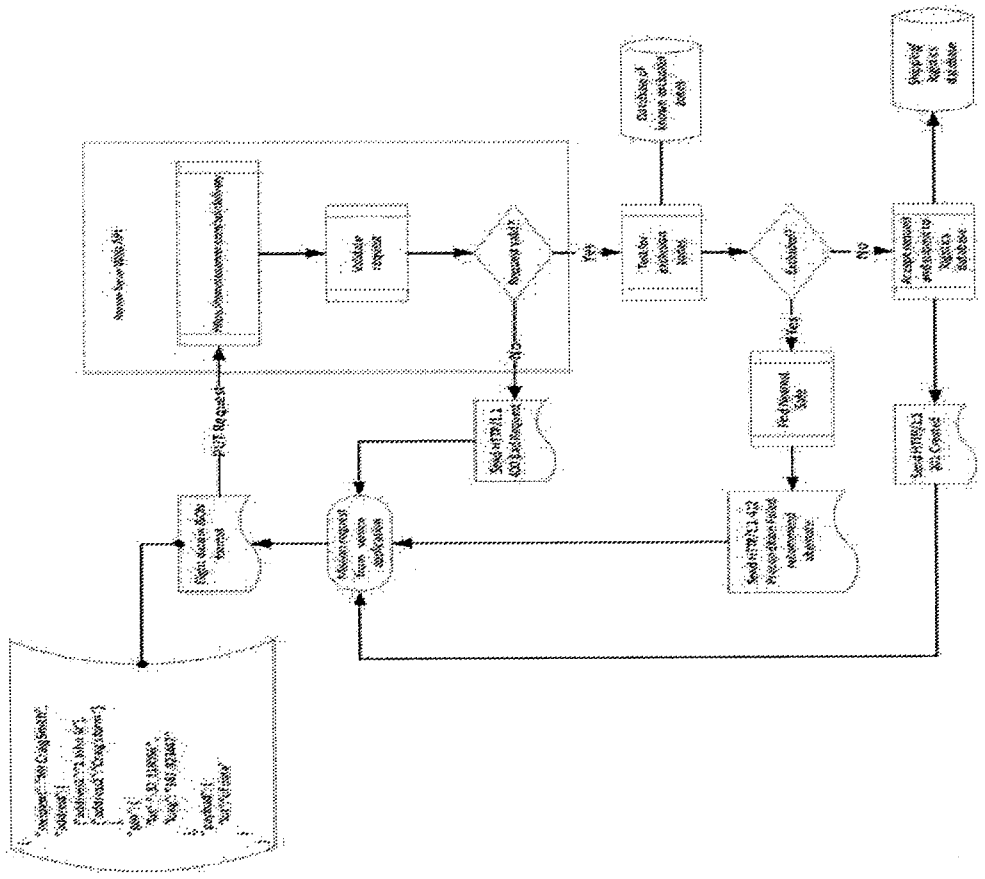


Figure 9c

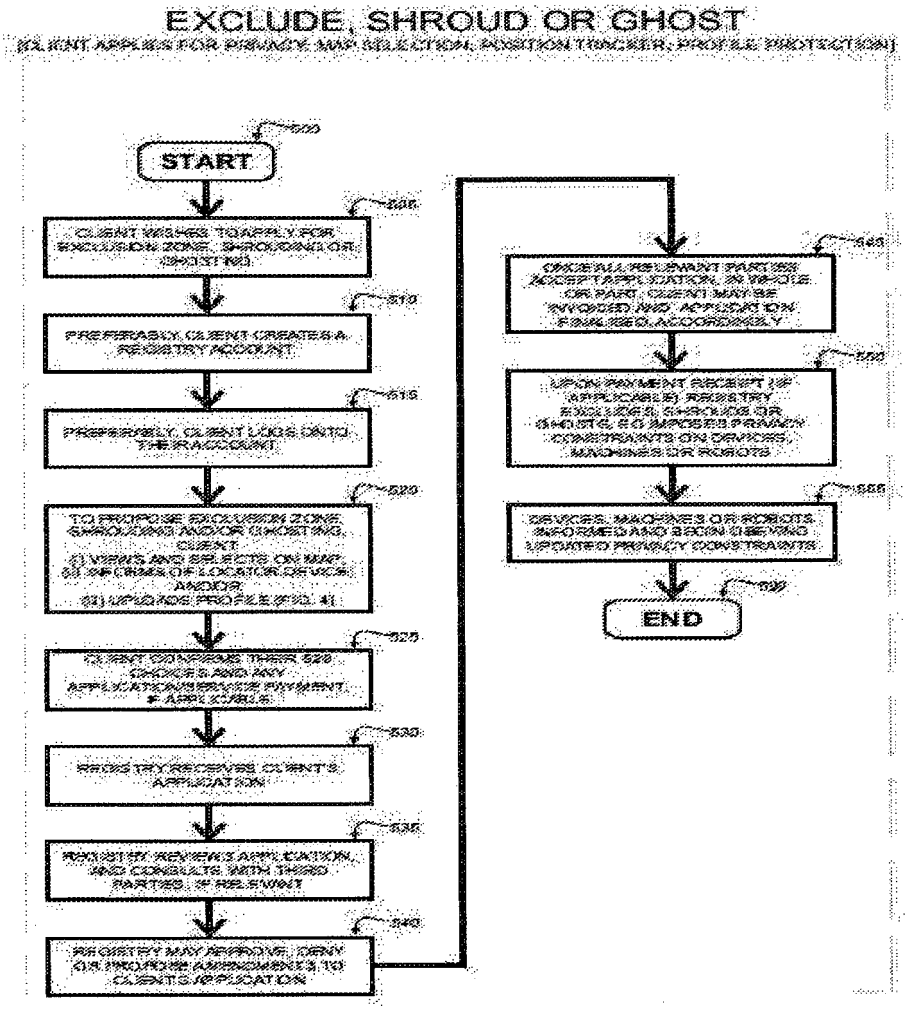


Figure 10

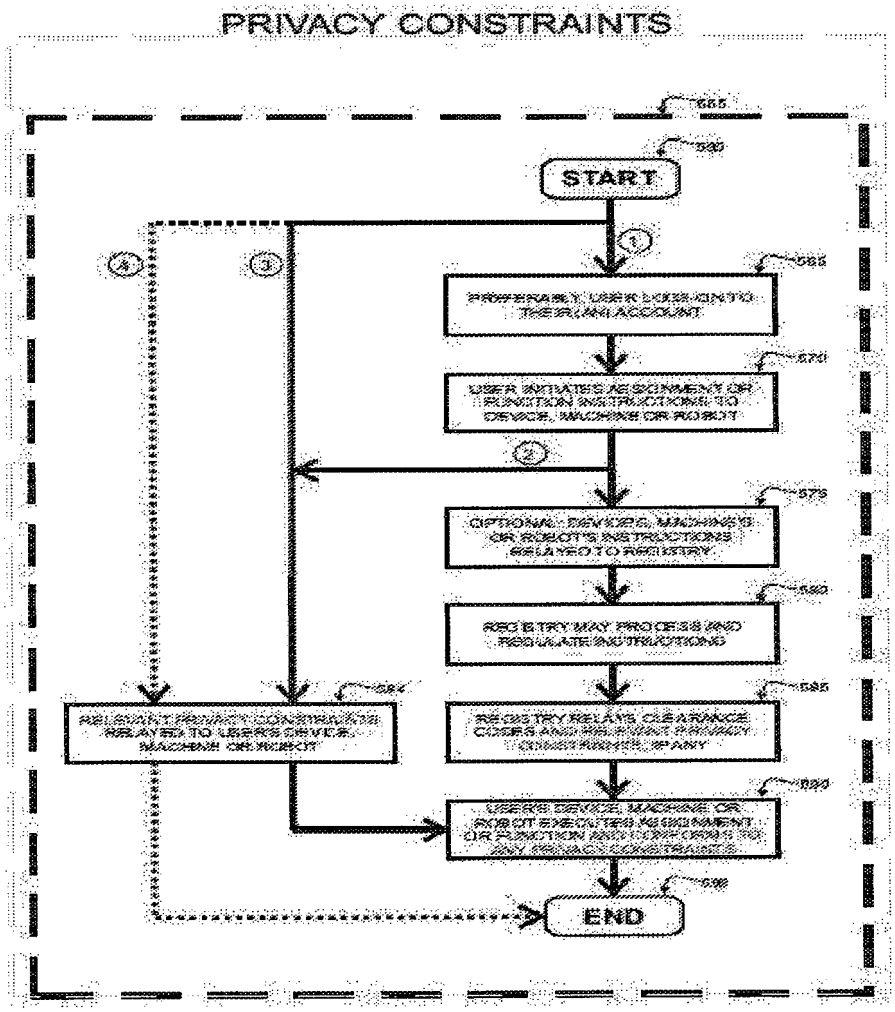


Figure 11

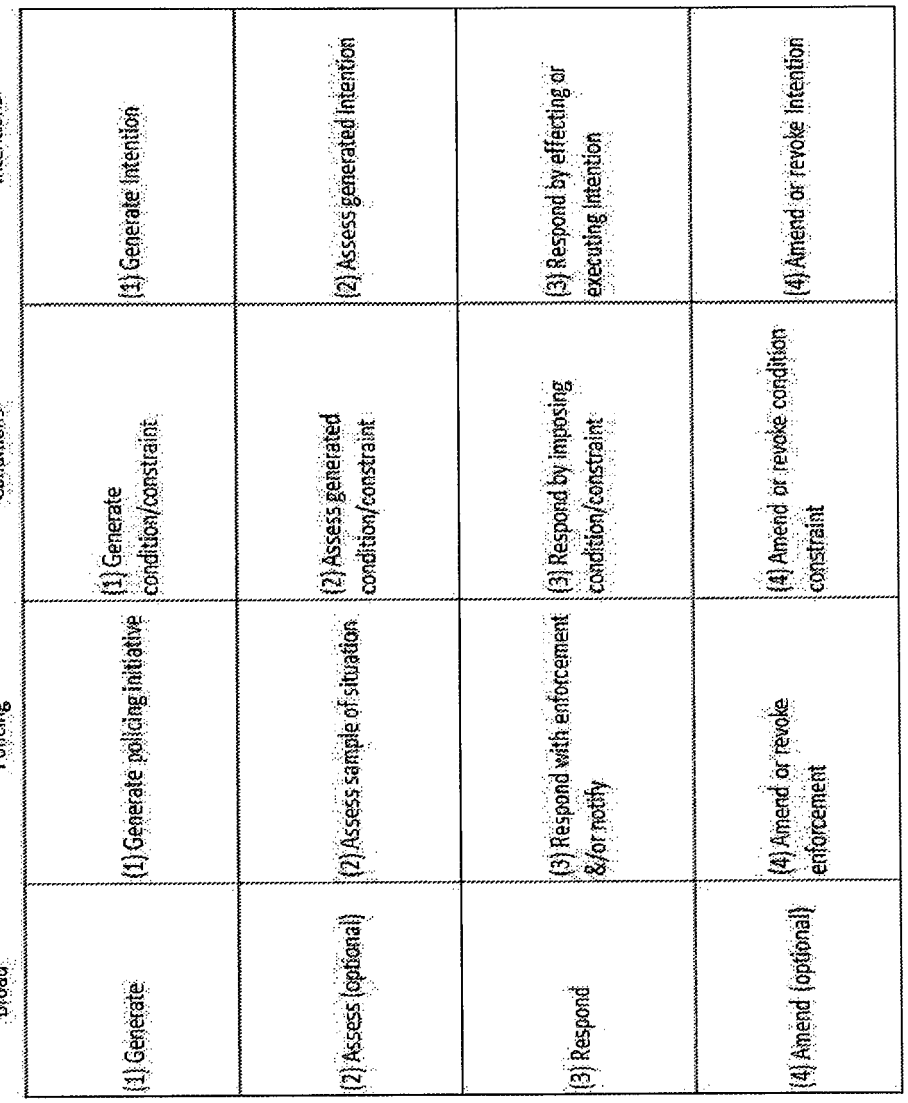

Broad
Policing
Conditions
Intentions
(1) Generate
(1) Generate policing initiative
(1) Generate condition/constraint
(1) Generate intention
(2) Assess (optional)
(2) Assess sample of situation
(2) Assess generated condition/constraint
(2) Assess generated intention
(3) Respond
(3) Respond with enforcement &/or notify
(3) Respond by imposing condition/constraint
(3) Respond by effecting or executing intention
(4) Amend (optional)
(4) Amend or revoke enforcement
(4) Amend or revoke condition constraint
(4) Amend or revoke intention

Figure 11a

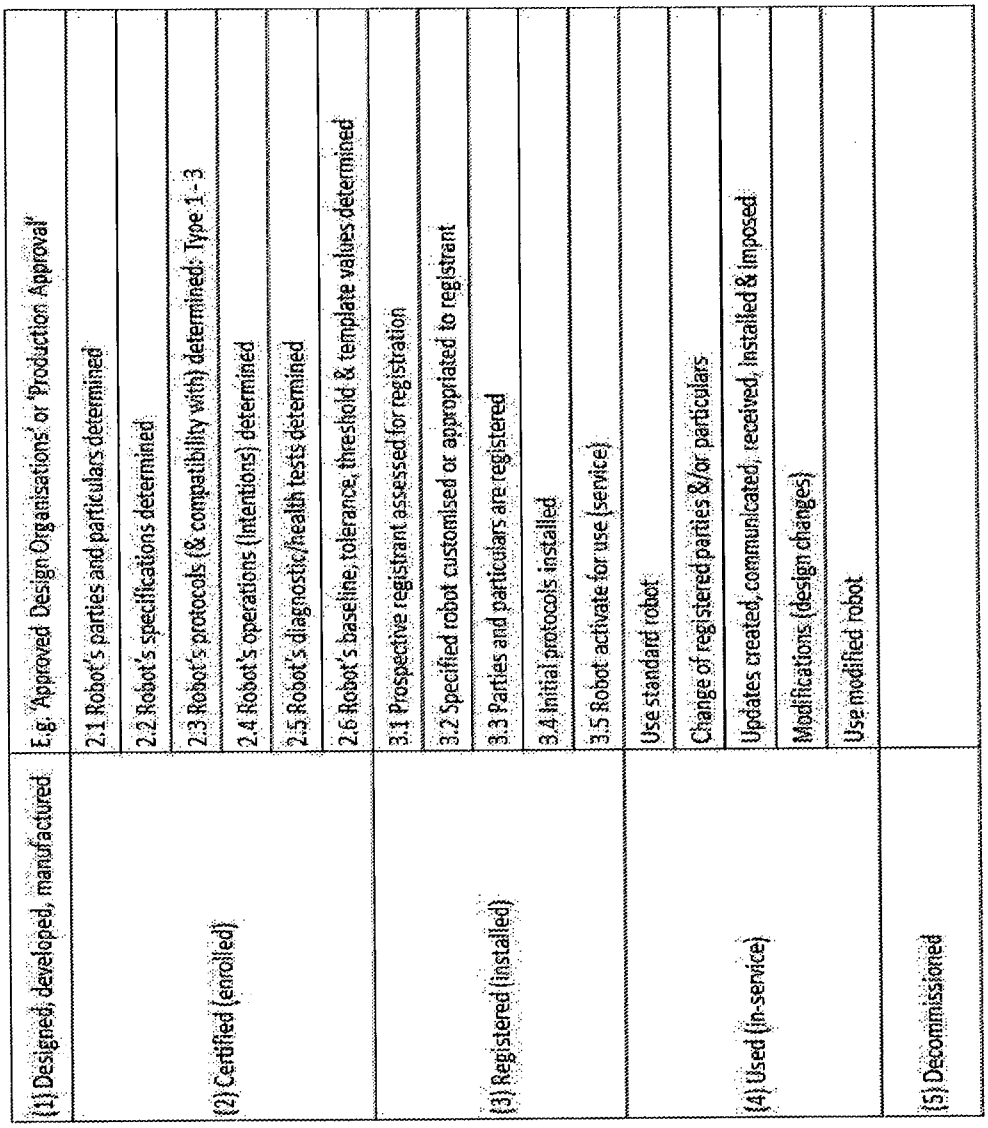

(1) Designed, developed, manufactured
E.g. 'Approved Design Organisations' or 'Production Approval'
(2) Certified (enrolled)
2.1 Robot's parties and particulars determined
2.2 Robot's specifications determined
2.3 Robot's protocols (& compatibility with) determined: Type 1 - 3
2.4 Robot's operations (intentions) determined
2.5 Robot's diagnostic/health tests determined
2.6 Robot's baseline, tolerance, threshold & template values determined
(3) Registered (installed)
3.1 Prospective registrant assessed for registration
3.2 Specified robot customised or appropriated to registrant
3.3 Parties and particulars are registered
3.4 Initial protocols installed
3.5 Robot activate for use (service)
(4) Used (in-service)
Use standard robot
Change of registered parties &/or particulars
Updates created, communicated, received, installed & imposed
Modifications (design changes)
Use modified robot
(5) Decommissioned

Figure 11b

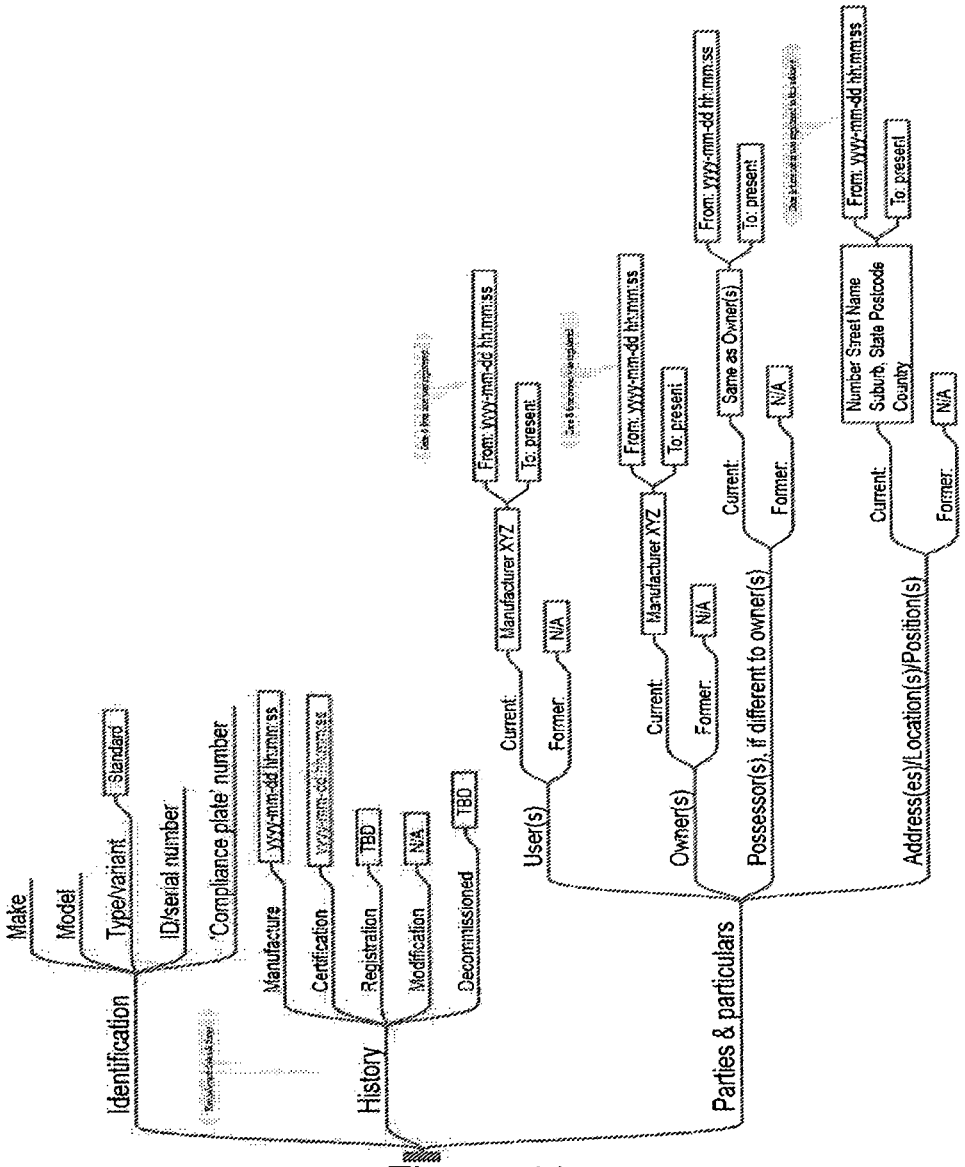

Identification
Make
Model
Type/variant
Standard
ID/serial number
'Compliance plate' number
History
Manufacture
yyyy-mm-dd hh:mm:ss
Certification
yyyy-mm-dd hh:mm:ss
Registration
TBD
Modification
N/A
Decommissioned
TBD
Parties & particulars
User(s)
Current:
Manufacturer XYZ
From: yyyy-mm-dd hh:mm:ss
To: present
Former:
N/A
Owner(s)
Current:
Manufacturer XYZ
From: yyyy-mm-dd hh:mm:ss
To: present
Former:
N/A
Possessor(s), if different to owner(s)
Current:
Same as Owner(s)
From: yyyy-mm-dd hh:mm:ss
To: present
Former:
N/A
Address(es)/Location(s)/Position(s)
Current:
Number Street Name
Suburb, State Postcode
Country
From: yyyy-mm-dd hh:mm:ss
To: present
Former:
N/A

Figure 11c

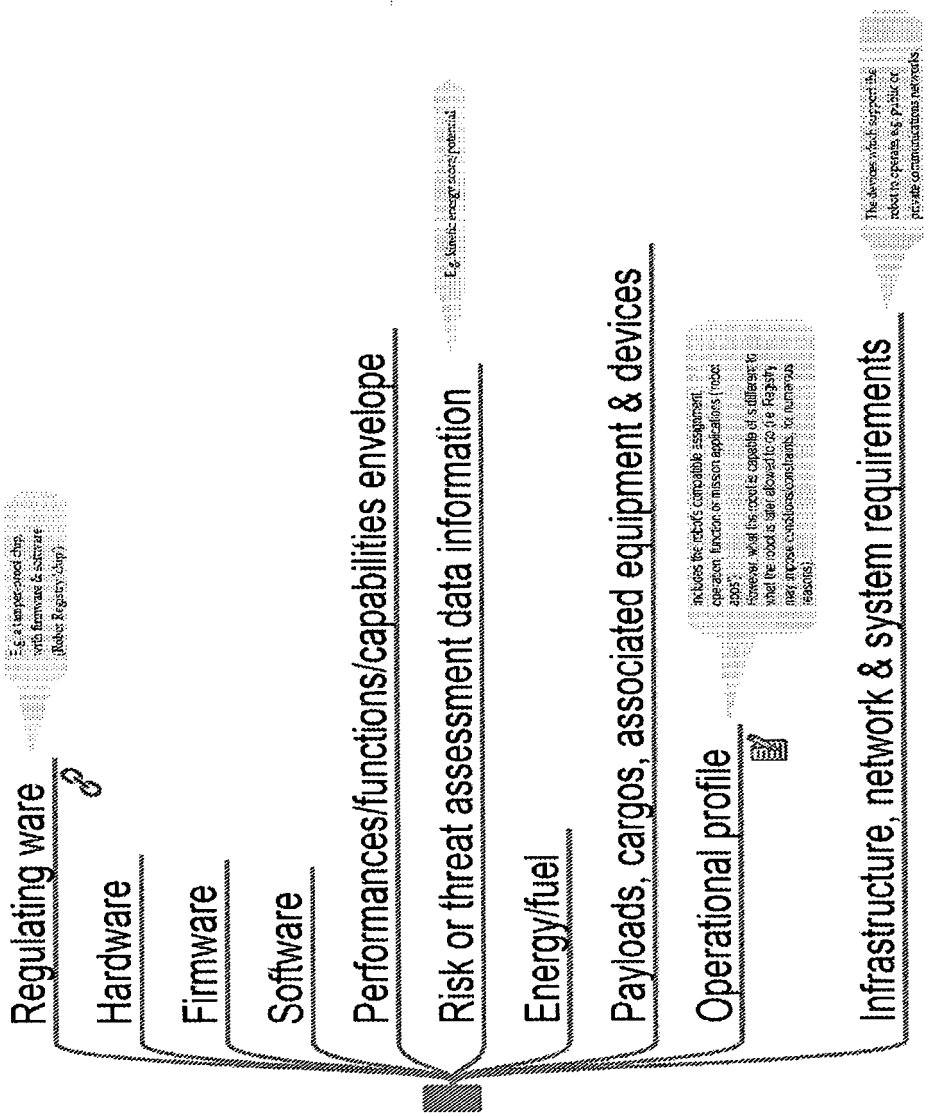

Regulating ware
Hardware
Firmware
Software
Performances/functions/capabilities envelope
Risk or threat assessment data information
Energy/fuel
Payloads, cargos, associated equipment & devices
Operational profile
Infrastructure, network & system requirements

Figure 11d

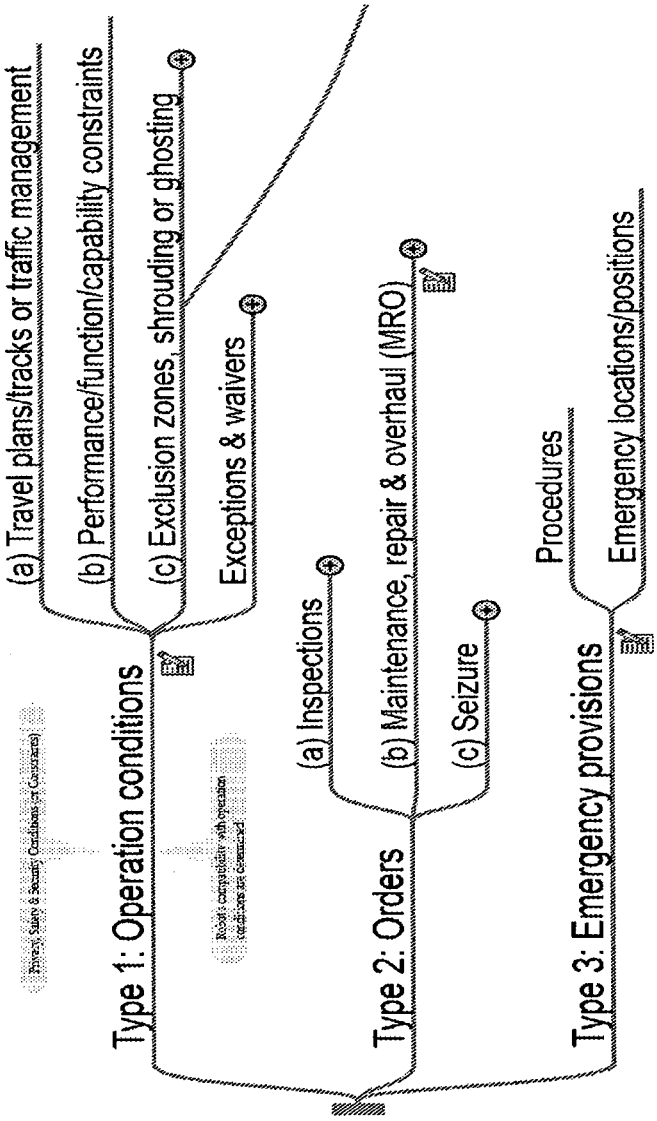

(a) Travel plans/tracks or traffic management
(b) Performance/function/capability constraints
(c) Exclusion zones, shrouding or ghosting
Exceptions & waivers
Type 1: Operation conditions
(a) Inspections
(b) Maintenance, repair & overhaul (MRO)
(c) Seizure
Type 2: Orders
Procedures
Emergency locations/positions
Type 3: Emergency provisions

Figure 11e

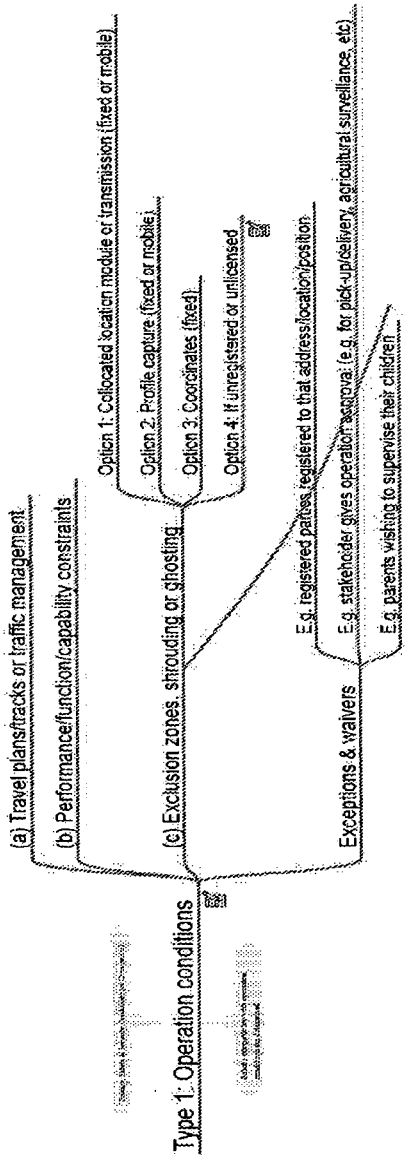

Type 1: Operation conditions
(a) Travel plans/tracks or traffic management
(b) Performance/function/capability constraints
(c) Exclusion zones, shrouding or ghosting
Option 1: Collocated location module or transmission (fixed or mobile)
Option 2: Profile capture (fixed or mobile)
Option 3: Coordinates (fixed)
Option 4: If unregistered or unlicensed
Exceptions & waivers
E.g. registered parties registered to that address/location/position
E.g. stakeholder gives operation approval (e.g. for pick-up/delivery, agricultural surveillance, etc)
E.g. parents wishing to supervise their children

Figure 11f

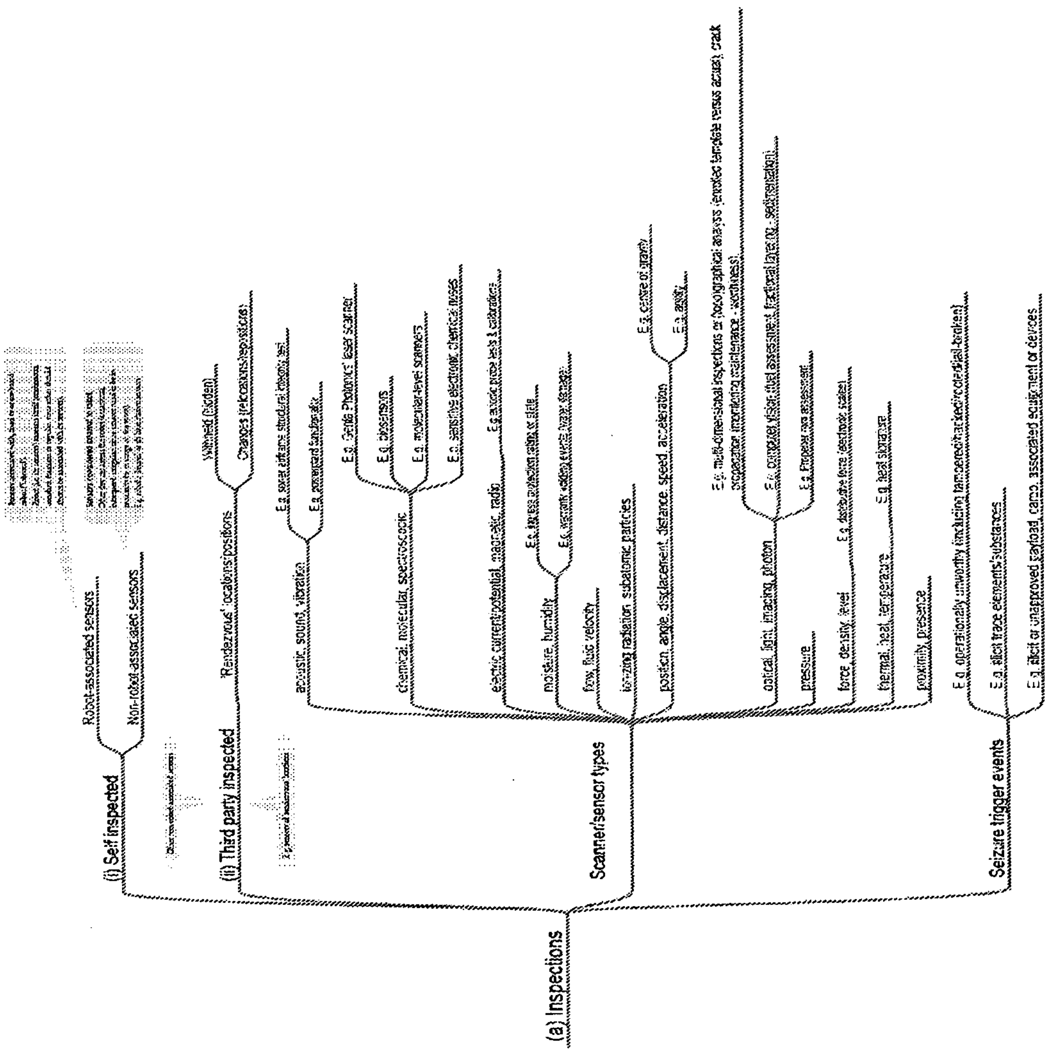

(a) Inspections
(i) Self inspected
Robot-associated sensors
Non-robot-associated sensors
(ii) Third party inspected
'Rendezvous' locations/positions
Witnessed (hidden)
Changes (relocations/repositions)
Scanner/sensor types
acoustic, sound, vibration
chemical, molecular, spectroscopic
E.g. Gentle Photonics' laser scanner
E.g. biosensors
E.g. molecular-level scanners
E.g. sensitive electronic chemical noses
electric current/potential, magnetic, radio
E.g. avionic probe tests & calibrations
moisture, humidity
E.g. ingress protection rating or state
E.g. warranty-voiding events (water damage)
flow, fluid velocity
ionizing radiation, subatomic particles
position, angle, displacement, distance, speed, acceleration
E.g. centre of gravity
E.g. agility
optical, light, imaging, photon
pressure
force, density, level
thermal, heat, temperature
E.g. heat signature
proximity, presence
Seizure trigger events
E.g. illicit trace elements/substances
E.g. illicit or unapproved payload, cargo, associated equipment or devices

Figure 11g

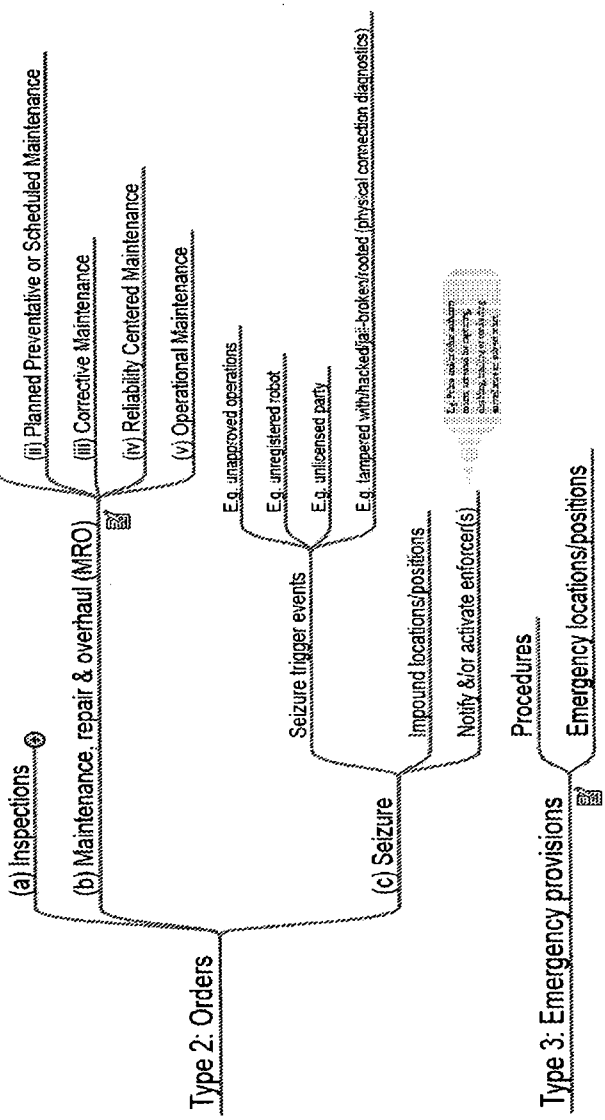

Type 2: Orders
(a) Inspections
(b) Maintenance, repair & overhaul (MRO)
(i) Predictive Maintenance
(ii) Planned Preventative or Scheduled Maintenance
(iii) Corrective Maintenance
(iv) Reliability Centered Maintenance
(v) Operational Maintenance
(c) Seizure
Seizure trigger events
E.g. unapproved operations
E.g. unregistered robot
E.g. unlicensed party
E.g. tampered with/hacked/jail-broken/rooted (physical connection diagnostics)
Impound locations/positions
Notify &/or activate enforcer(s)
Type 3: Emergency provisions
Procedures
Emergency locations/positions

Figure 11h

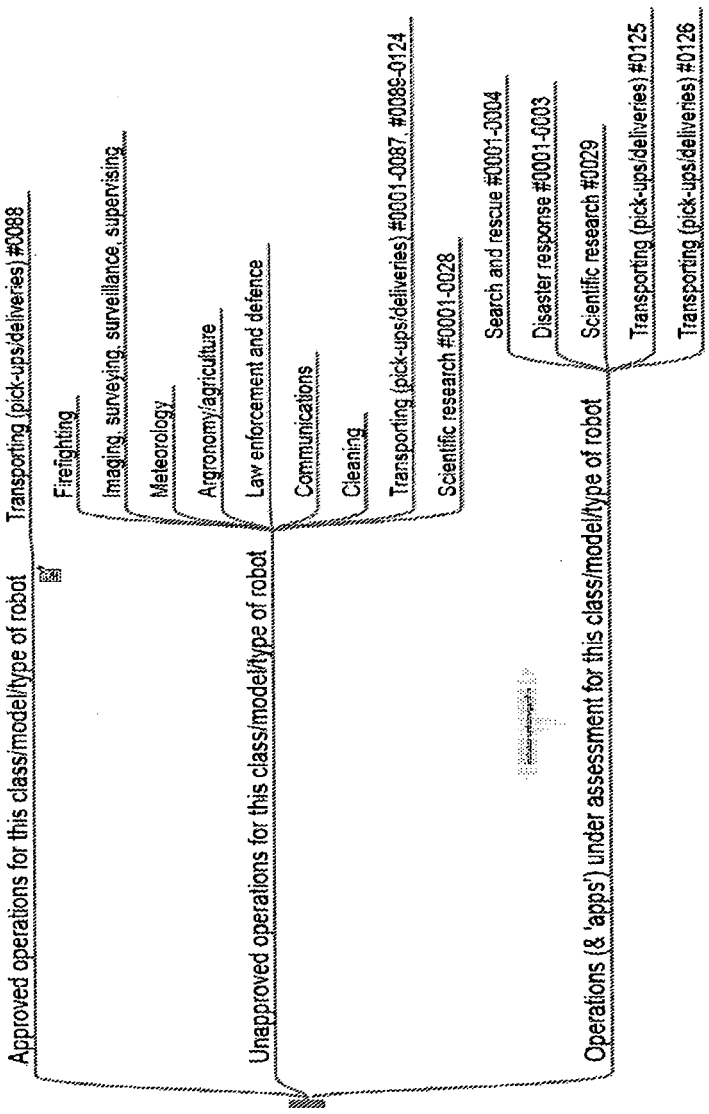

Operations (& 'apps') under assessment for this class/model/type of robot
Approved operations for this class/model/type of robot
Transporting (pick-ups/deliveries) #0088
Unapproved operations for this class/model/type of robot
Firefighting
Imaging, surveying, surveillance, supervising
Meteorology
Agronomy/agriculture
Law enforcement and defence
Communications
Cleaning
Transporting (pick-ups/deliveries) #0001-0087, #0089-0124
Scientific research #0001-0028
Search and rescue #0001-0004
Disaster response #0001-0003
Scientific research #0029
Transporting (pick-ups/deliveries) #0125
Transporting (pick-ups/deliveries) #0126

Figure 11i

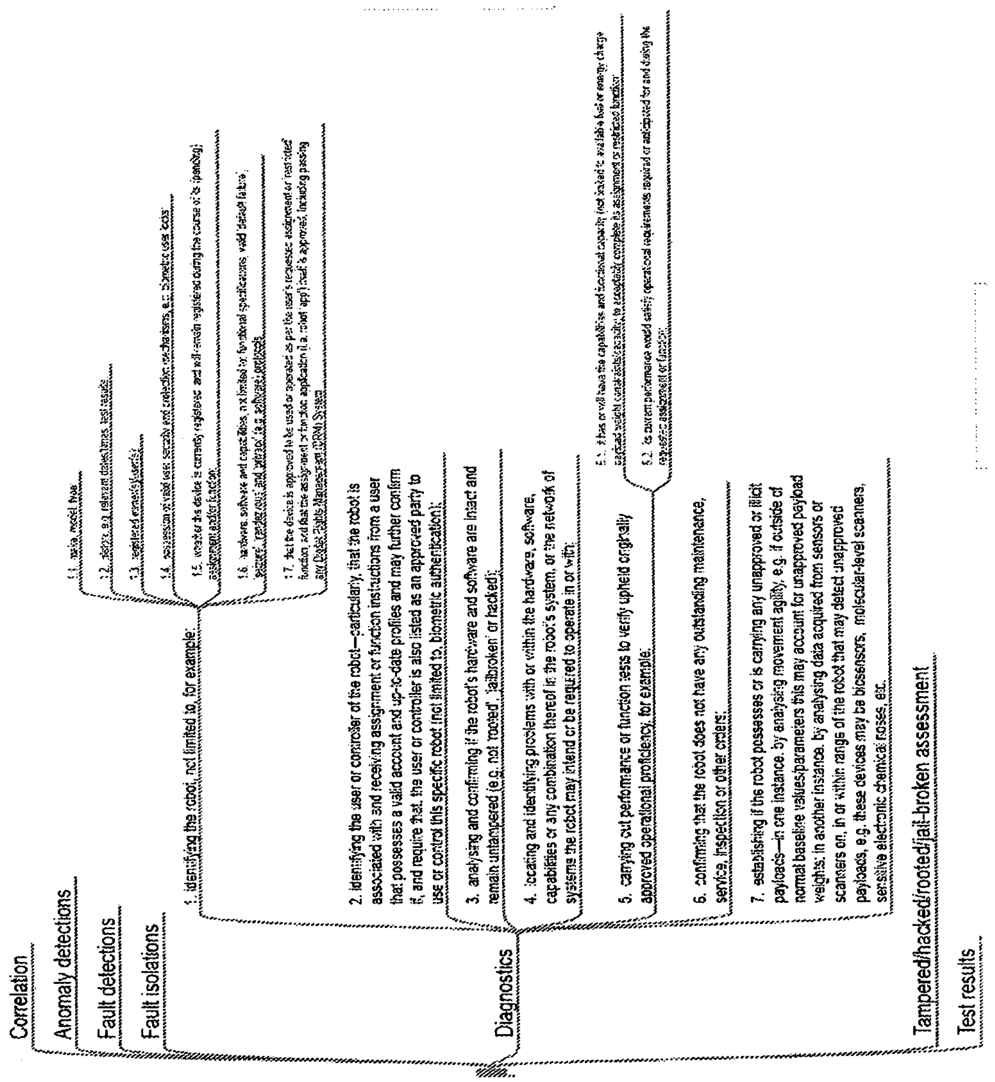

Correlation
Anomaly detections
Fault detections
Fault isolations
Diagnostics
1. identifying the robot, not limited to, for example:
2. identifying the user or controller of the robot—particularly, that the robot is associated with and receiving assignment or function instructions from a user that possesses a valid account and up-to-date profiles and may further confirm it, and require that, the user or controller is also listed as an approved party to use or control this specific robot (not limited to, biometric authentication);
3. analysing and confirming if the robot's hardware and software are intact and remain untampered (e.g. not 'rooted', 'jailbroken' or hacked);
4. locating and identifying problems with or within the hardware, software, capabilities or any combination thereof in the robot's system, or the network of systems the robot may intend or be required to operate in or with;
5. carrying out performance or function tests to verify upheld originally approved operational proficiency, for example:
6. confirming that the robot does not have any outstanding maintenance, service, inspection or other orders;
7. establishing if the robot possesses or is carrying any unapproved or illicit payloads—in one instance, by analysing movement agility, e.g. if outside of normal baseline values/parameters this may account for unapproved payload weights; in another instance, by analysing data acquired from sensors or scanners on, in or within range of the robot that may detect unapproved payloads, e.g. these devices may be biosensors, molecular-level scanners, sensitive electronic chemical noses, etc.
Tampered/hacked/rooted/jail-broken assessment
Test results

Figure 11j

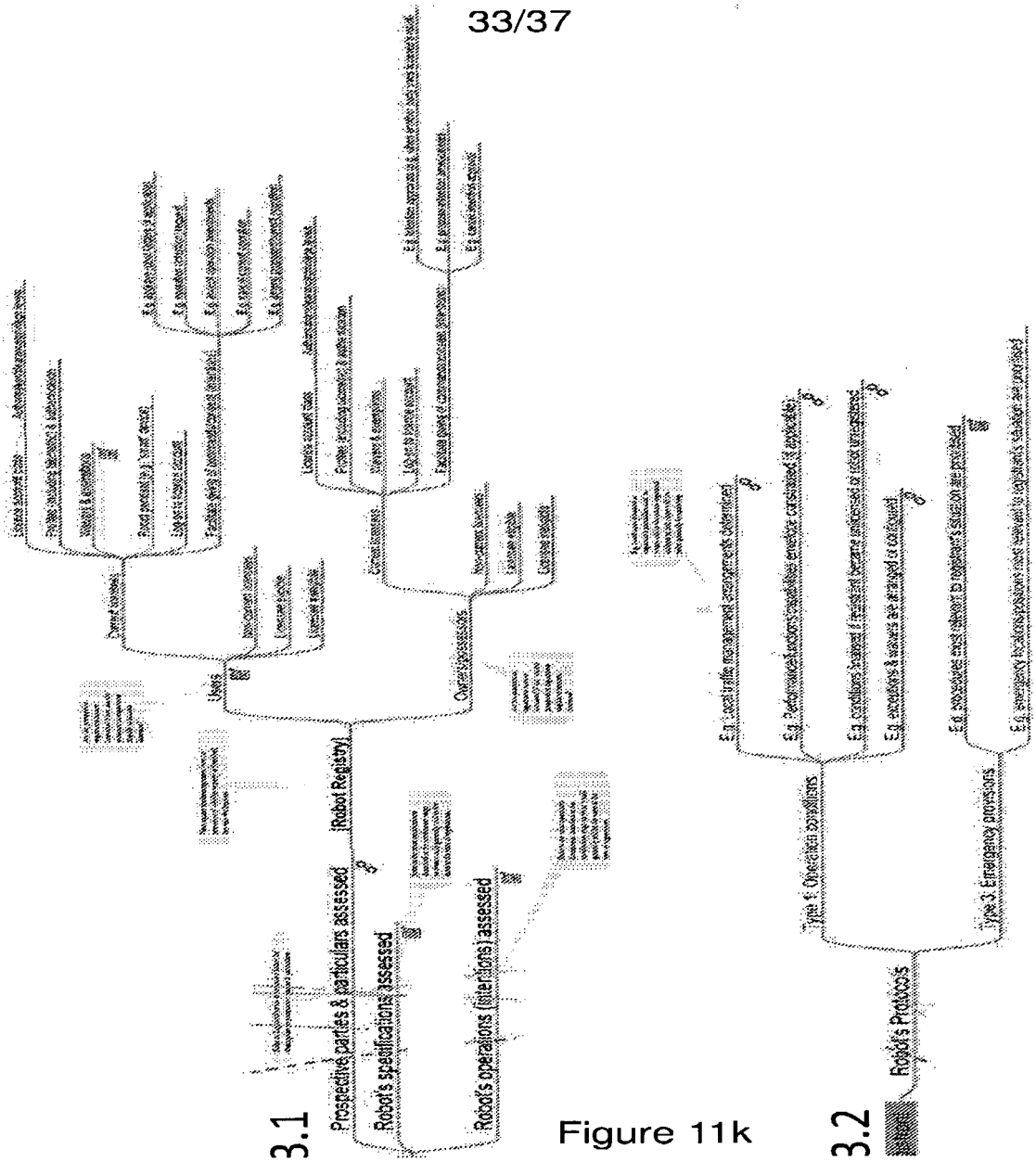

Prospective parties & particulars assessed
Robot's specifications assessed
Robot's operations (intentions) assessed
Type 1: Operational conditions
Type 3: Emergency provisions
Robot's Protocols
3.1
3.2

Figure 11k

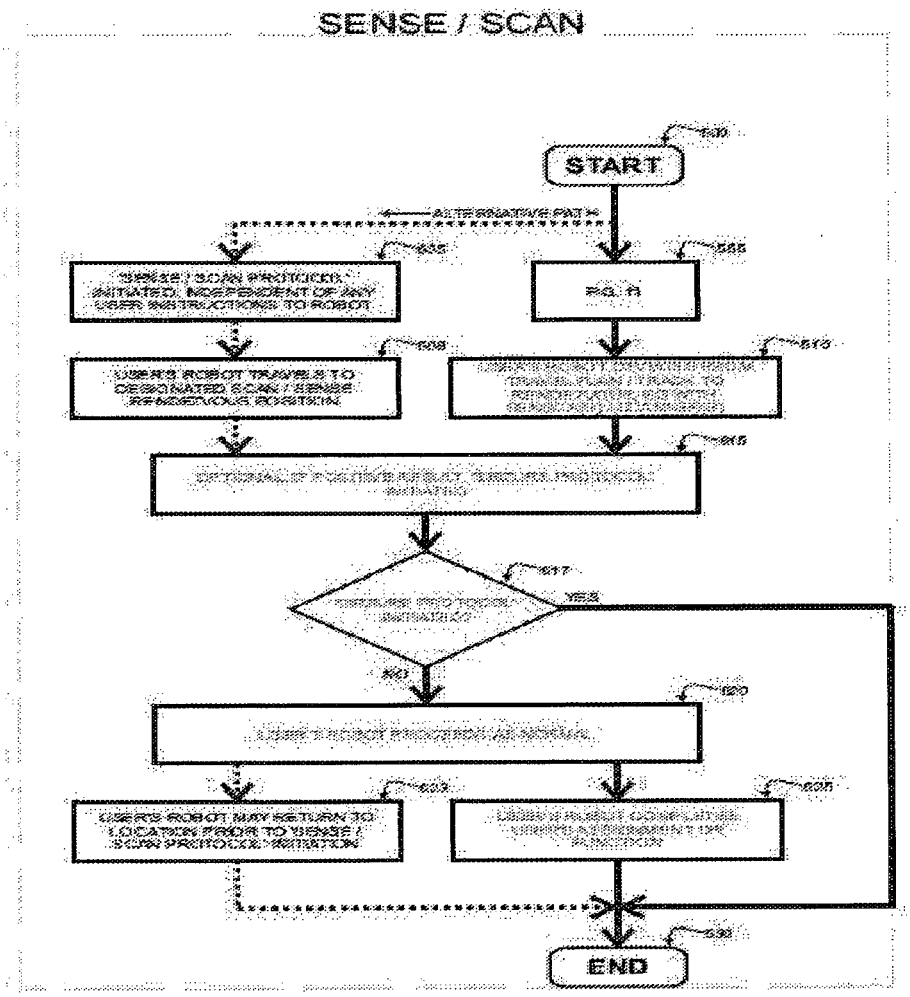


Figure 12

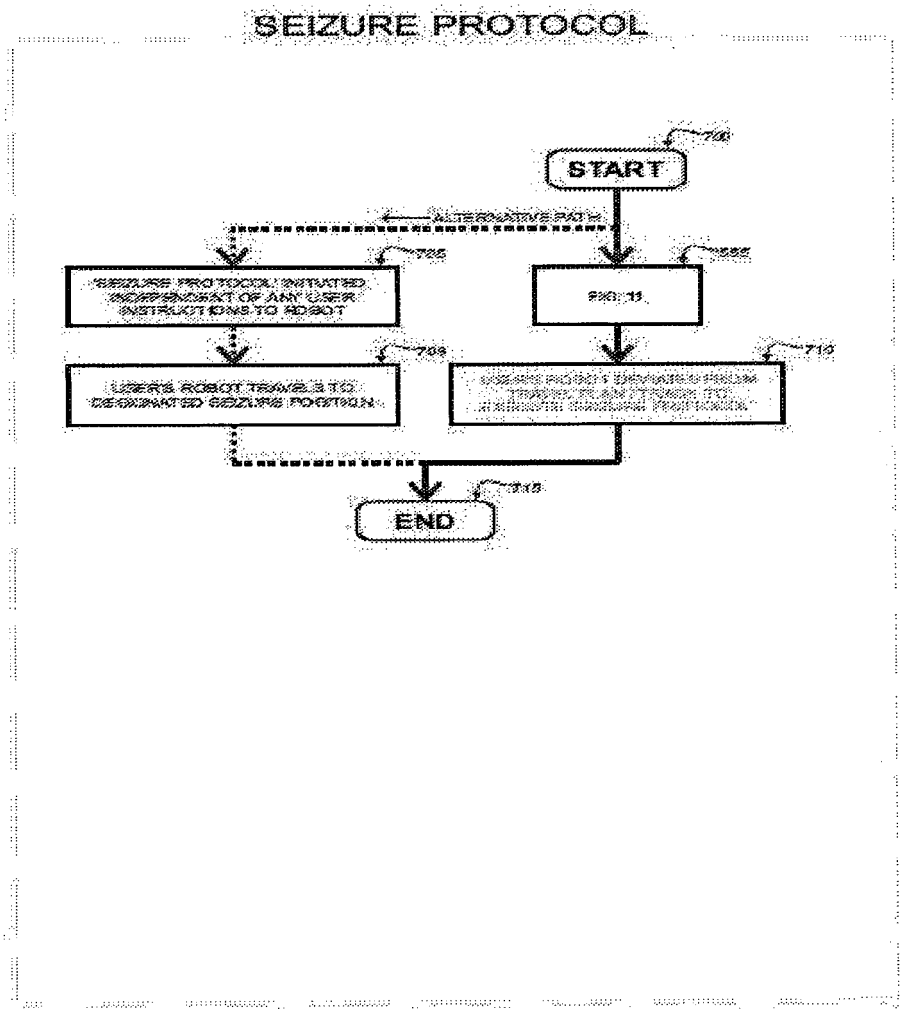

SEIZURE PROTOCOL
START
ALTERNATIVE PATH
SEIZURE PROTOCOL INITIATED INDEPENDENT OF ANY USER INSTRUCTIONS TO ROBOT
USER'S ROBOT TRAVELS TO DESIGNATED SEIZURE POSITION
END

Figure 13

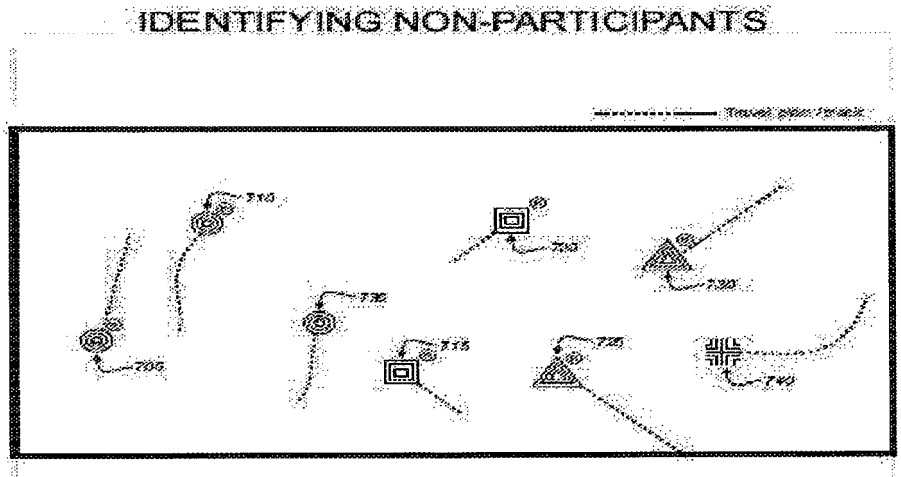


Figure 14

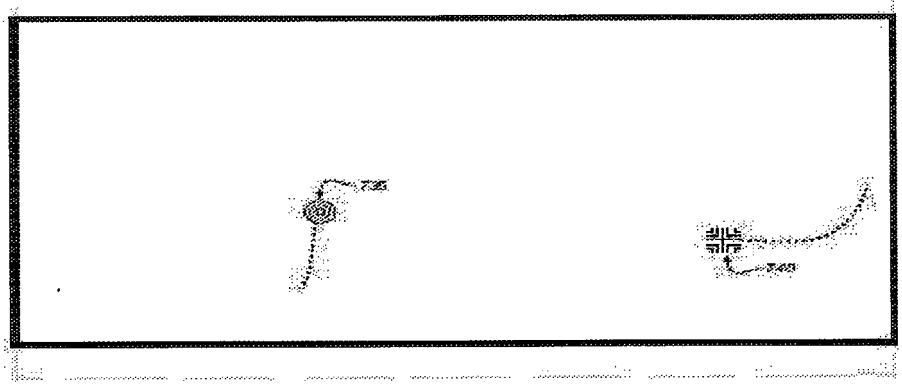


Figure 15

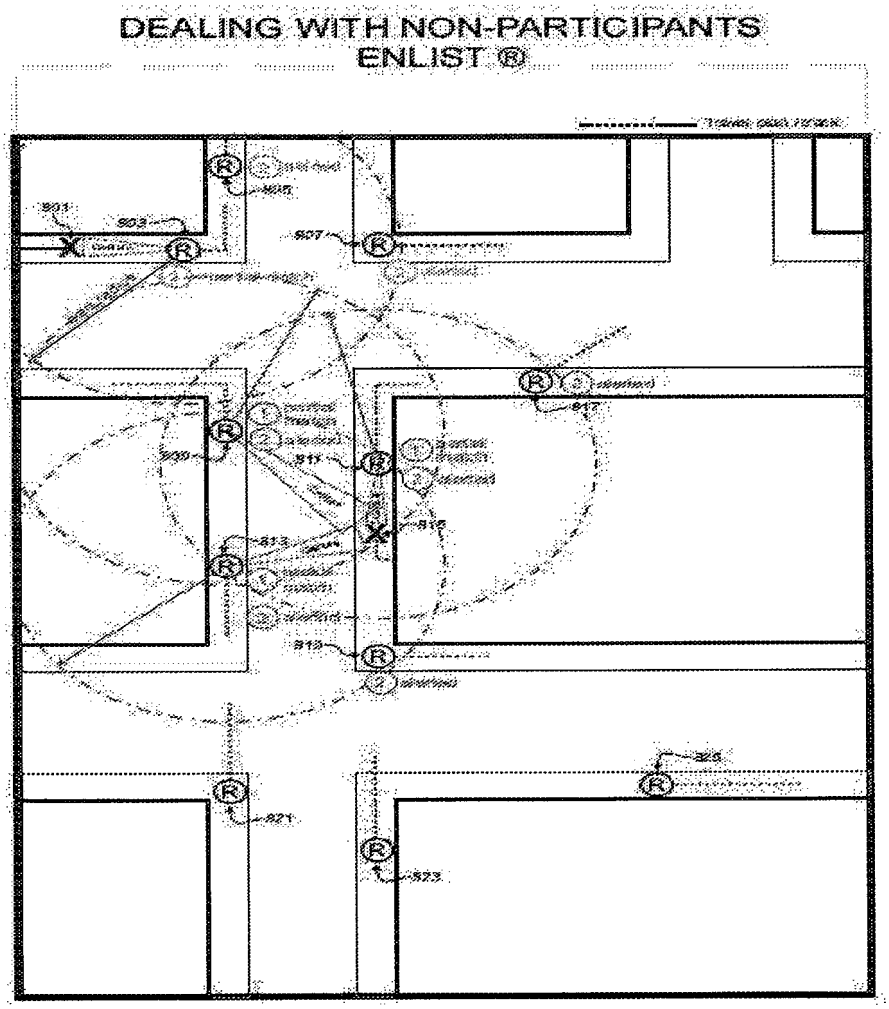


Figure 16

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2013/001303

A. CLASSIFICATION OF SUBJECT MATTER

G06F 19/00 (2011.01)

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)

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)

EPODOC, WPI, ESPACE, Google Patents. Search terms: robot, control, validate, authenticate, command, database, and other similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	

[X] Further documents are listed in the continuation of Box C [X] 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	Date of mailing of the international search report
20 December 2013	20 December 2013
Name and mailing address of the ISA/AU	**Authorised officer**
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA Email address: pct@ipaustralia.gov.au Facsimile No.: +61 2 6283 7999	Kim Ung AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. 0399359621

INTERNATIONAL SEARCH REPORT		International application No.
C (Continuation).	DOCUMENTS CONSIDERED TO BE RELEVANT	**PCT/AU2013/001303**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/0120361 A1 (KUROKI et al.) 29 August 2002 abstract; paragraphs [0063]-[0067]; Figures 4, 7	1-28
A	US 2005/0080799 A1 (HARNDEN et al.) 14 April 2005	

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/AU2013/001303**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		Patent Family Member/s	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
US 2002/0120361 A1	29 Aug 2002	JP 2001277163 A	09 Oct 2001
		US 2002120361 A1	29 Aug 2002
		US 6556892 B2	29 Apr 2003
		WO 0174549 A1	11 Oct 2001
US 2005/0080799 A1	14 Apr 2005	None	

End of Annex

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104919462 A
(43)申请公布日 2015.09.16

(21)申请号 201380070101.X
(22)申请日 2013.11.12
(30)优先权数据
2012904989 2012.11.12 AU
2013204965 2013.04.12 AU
(85)PCT国际申请进入国家阶段日
2015.07.10
(86)PCT国际申请的申请数据
PCT/AU2013/001303 2013.11.12
(87)PCT国际申请的公布数据
WO2014/071465 EN 2014.05.15
(71)申请人 希图系统有限公司
地址 中国香港湾仔
(72)发明人 詹姆斯·罗伯特·斯托尔
(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 宁晓 郑霞
(51)Int.Cl.
G06F 19/00(2011.01)

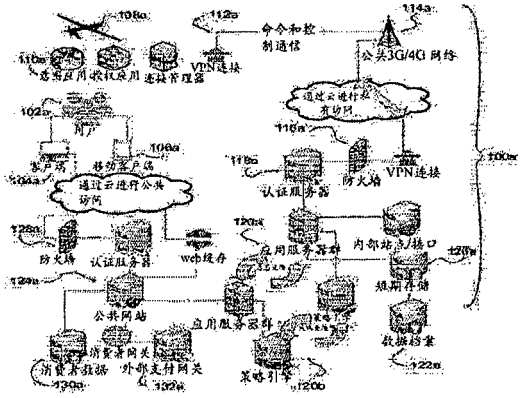
权利要求书2页 说明书31页 附图35页

(54)发明名称

用于对机器和装置进行注册、监测和控制的系统、方法、计算机程序和数据信号

(57)摘要

本发明提供了一种用于控制机器人装置的方法，该方法包括以下步骤：在一个计算装置处接收被安排成用于在该机器人装置上实现一个操作的至少一条命令、审核该命令以便确定该命令是否适合于执行，其中，只有在该命令适合于执行时才将该命令提供给该装置。



CN 104919462 A

1. 一种用于控制至少一个机器人装置的系统，该系统包括一个计算装置，该计算装置能够与至少一个机器人装置进行通信并且被安排成用于从一个命令模块接收至少一条命令，该命令被安排为包含至少一条指令以及标识该至少一个机器人装置的标识信息，该至少一条指令被安排成用于在该机器人装置上实现一个操作，其中，该计算装置包括一个处理器和一个数据库，该处理器被安排成用于接收该命令并且针对该数据库中的信息审核该命令以便确定该命令是否适合于由该至少一个机器人装置执行，其中，如果该命令适合于执行，将该命令提供给该机器人装置。

2. 根据权利要求 1 所述的系统，其中，该处理器确定该命令是否与至少一个授权码相关联。

3. 根据权利要求 2 所述的系统，其中，独立于该至少一条命令来接收该至少一个授权码。

4. 根据权利要求 1、2 或 3 所述的系统，其中，该处理器通过访问存储在该数据库中的一组预定的命令来确定该命令是否是一组预定的命令之一。

5. 根据权利要求 1 至 5 中任一项所述的系统，其中，对该至少一条命令、该授权码和该标识码中的至少一项进行加密。

6. 根据权利要求 5 所述的系统，包括在审核该命令以便确定该命令是否适合于执行之前对该至少一条命令、该授权码和该标识码中的该至少一项进行解密的进一步步骤。

7. 根据权利要求 1 至 6 中任一项所述的系统，其中，该至少一条命令、该授权码和该标识码中的至少一项包括一个校验和，其中，该校验和用于确定该至少一条命令、该授权码和该标识码的正确性。

8. 根据前述权利要求中任一项所述的系统，其中，该机器人装置是一个可编程装置。

9. 根据前述权利要求中任一项所述的系统，其中，该机器人装置包括被安排为用于接收并执行该至少一条命令的至少一个处理器。

10. 根据前述权利要求中任一项所述的系统，其中，该机器人装置能够执行至少一项物理功能。

11. 一种用于控制机器人装置的系统，该系统包括能够接收至少指令的一个计算装置、能够基于该至少一条指令生成一条命令的一个处理器，其中，该命令是通过该计算装置进行传送之一以便基于该至少一条所生成的命令发起一个响应。

12. 根据权利要求 11 所述的系统，其中，在发起一个响应之前，该处理器请求进一步的信息以便进一步评估该指令。

13. 一种用于控制机器人装置的方法，该方法包括以下步骤：在一个计算装置处接收被安排成用于在该机器人装置上实现一个操作的至少一条命令、审核该命令以便确定该命令是否适合于执行，其中，只有在该命令适合于执行时才将该命令提供给该装置。

14. 根据权利要求 13 所述的系统，其中，审核该命令的步骤包括确定该命令是否与至少一个授权码相关联的步骤。

15. 根据权利要求 14 所述的系统，其中，独立于该至少一条命令来接收该至少一个授权码。

16. 根据权利要求 13、14 或 15 所述的方法，其中，审核该命令的步骤包括确定该命令是否是一组预定的命令之一的进一步步骤。

17. 根据权利要求 13 至 16 中任一项所述的方法，包括该计算装置接收被安排成用于标识该机器人装置的至少一个标识码的进一步步骤。

18. 根据权利要求 17 所述的方法，包括与该至少一条命令一起接收该标识码的进一步步骤。

19. 根据权利要求 13 至 18 中任一项所述的方法，其中，对该至少一条命令、该授权码和该标识码中的至少一项进行加密。

20. 根据权利要求 19 所述的方法，包括在审核该命令以便确定该命令是否适合于执行之前的对该至少一条命令、该授权码和该标识码中的该至少一项进行解密的进一步步骤。

21. 根据权利要求 13 至 20 中任一项所述的方法，其中，该至少一条命令、该授权码和该标识码中的至少一项包括一个校验和，其中，该校验和用于确定该至少一条命令、该授权码和该标识码的正确性。

22. 根据权利要求 13 至 21 中任一项所述的方法，其中，该机器人装置是一个可编程装置。

23. 根据权利要求 13 至 22 中任一项所述的方法，其中，该机器人装置包括被安排为用于接收并执行该至少一条命令的至少一个处理器。

24. 根据权利要求 13 至 23 中任一项所述的方法，其中，该机器人装置能够执行至少一项物理功能。

25. 一种用于控制机器人装置的系统，该系统包括一个计算装置，该计算装置与该机器人装置进行通信并且被安排成用于接收至少一条命令，该至少一条命令被安排成用于在该机器人装置上实现一个操作，其中，该计算装置审核该命令以确定该命令是否适合于执行，并且只有在该命令适合于执行时才将该命令提供给该装置。

26. 一种包括至少一条命令的计算机程序，当在一个计算系统上执行时，该计算机程序被安排成用于执行权利要求 13 至 24 中至少一项所述的方法步骤。

27. 一种计算机可读介质，该计算机可读介质结合有根据权利要求 26 所述的计算机程序。

28. 一种数据信号，该数据信号对至少一条命令进行编码并且被安排成可由至少一个计算装置接收，其中，当在该计算系统上执行该编码的命令时，该计算系统执行权利要求 13 至 24 中至少一项所述的方法步骤。

用于对机器和装置进行注册、监测和控制的系统、方法、计算机程序和数据信号

技术领域

[0001] 本发明涉及一种用于对机器和装置进行注册、监测和控制的系统、方法、计算机程序和数据信号。本发明的实施例发现了在机器人装置、自主车辆、“智能”装置以及其他可编程和计算机控制装置的注册、监测和控制中的具体但非排他的使用。

背景技术

[0002] 以下对背景技术的讨论仅旨在促进理解本发明。这个讨论不是承认或确认所提及的任何资料是或者曾经是至本申请的优选权日的普通公知常识的一部分。

[0003] 科幻小说预言了被安排成用于自主地执行一个或多个功能的机器人装置和“智能”装置的最终发展。在过去，由于在计算能力和生产可靠的、具有成本效益的电子设备的能力上的限制，机器人装置已经被广泛地用于非常专业的应用中（比如在制造应用中）或用作“展览品”（例如，ASIMO 的开发，由本田 (Honda) 公司所开发的一款仿人机器人）。

[0004] 然而，现在电信和计算技术（比如蜂窝电话技术、互联网、无线互联网、消费者使用的全球定位系统技术的发布以及小型化计算技术的发展）的爆发和极速发展为消费者机器人的开发和生产提供了平台。

[0005] 例如，机器人真空吸尘器、小型远程控制机器人装置（例如直升飞机和多旋翼飞行器）以及更近期的开发自主“无人驾驶”车辆都是普通消费者可获得的实用且逐渐可使用的机器人和智能装置的示例。

[0006] 在此背景下，已经发展了本发明的实施例。

发明概述

[0007] 在第一方面，本发明提供了一种用于控制至少一个机器人装置的系统，该系统包括计算装置，该计算装置能够与至少一个机器人装置进行通信并且被安排成用于从命令模块接收至少一条命令，该命令被安排为包含至少一条指令以及标识该至少一个机器人装置的标识信息，该至少一条指令被安排成用于在该机器人装置上实现操作，其中，该计算装置包括处理器和数据库，该处理器被安排成用于接收该命令并且针对该数据库中的信息审核该命令以便确定该命令是否适合于由该至少一个机器人装置执行，其中，如果该命令适合于执行，将该命令提供给该机器人装置。

[0008] 在一个实施例中，该处理器确定该命令是否与至少一个授权码相关联。

[0009] 在一个实施例中，独立于该至少一条命令来接收该至少一个授权码。

[0010] 在一个实施例中，该处理器通过访问存储在该数据库中的一组预定的命令来确定该命令是否是一组预定的命令之一。

[0011] 在一个实施例中，其中对该至少一条命令、该授权码和该标识码中的至少一项进行加密。

[0012] 在一个实施例中，在审核该命令以便确定该命令是否适合于执行之前，该处理器解密该至少一条命令、该授权码和该标识码中的该至少一项。

[0013] 在一个实施例中，该至少一条命令、该授权码和该标识码中的至少一项包括校验和，其中，该校验和用于确定该至少一条命令、该授权码和该标识码的正确性。

[0014] 根据前述权利要求中任一项所述的系统，其中，该机器人装置是可编程装置。

[0015] 在一个实施例中，该机器人装置包括被安排为用于接收并执行该至少一条命令的至少一个处理器。

[0016] 在一个实施例中，该机器人装置能够执行至少一项物理功能。

[0017] 在第二方面，本发明提供了一种用于控制机器人装置的系统，该系统包括能够接收至少指令的计算装置、能够基于该至少一条指令生成命令的处理器，其中，该命令是通过该计算装置进行传送之一以便基于该至少一条所生成的命令发起响应。

[0018] 在一个实施例中，在发起响应之前，该处理器请求进一步的信息以便进一步评估该指令。

[0019] 在第三方面，本发明提供了一种用于控制机器人装置的方法，该方法包括以下步骤：在计算装置上接收被安排成用于在该机器人装置上实现操作的至少一条命令，审核该命令以确定该命令是否适合于执行，其中，只有在该命令适合于执行时才将该命令提供给该装置。

[0020] 在一个实施例中，审核该命令的步骤包括确定该命令是否与至少一个授权码相关联的步骤。

[0021] 在一个实施例中，独立于该至少一条命令来接收该至少一个授权码。

[0022] 在一个实施例中，审核该命令的步骤包括确定该命令是否是一组预定的命令之一的进一步步骤。

[0023] 在一个实施例中，本发明提供了该计算装置接收被安排成用于标识该机器人装置的至少一个标识码的进一步步骤。

[0024] 在一个实施例中，本发明提供了与该至少一条命令一起接收该标识码的进一步步骤。

[0025] 在一个实施例中，对该至少一条命令、该授权码和该标识码中的至少一项进行加密。

[0026] 在一个实施例中，本发明提供了在审核该命令以便确定该命令是否适合于执行之前的对该至少一条命令、该授权码和该标识码中的该至少一项进行解密的进一步步骤。

[0027] 在一个实施例中，该至少一条命令、该授权码和该标识码中的至少一项包括校验和，其中，该校验和用于确定该至少一条命令、该授权码和该标识码的正确性。

[0028] 在第四方面，本发明提供了一种用于控制机器人装置的系统，该系统包括计算装置，该计算装置与该机器人装置进行通信并且被安排成用于接收至少一条命令，该至少一条命令被安排成用于在该机器人装置上实现操作，其中，该计算装置审核该命令以确定该命令是否适合于执行，并且只有在该命令适合于执行时才将该命令提供给该装置。

[0029] 在第五方面，本发明提供了一种包括至少一条命令的计算机程序，当在计算系统上执行时，该计算机程序被安排成用于执行根据本发明的第三方面的方法步骤。

[0030] 一种计算机可读介质，该计算机可读介质结合有根据本发明的第五方面的计算机程序。

[0031] 在第六方面，本发明提供了一种数据信号，该数据信号对至少一条命令进行编码

并被安排成可由至少一个计算装置接收，其中，当在该计算系统上执行该经编码的命令时，该计算系统执行根据本发明的第三方面的方法步骤。

附图简要说明

[0032] 以下若干个非限制性实施例的描述中更充分地描述了本发明的其他特征。这个描述仅为了例示本发明的目的被包含。不应被理解成为对本发明的广泛概括、披露或描述（如以上列）的限制。将参照附图进行描述，在附图中：

图 1 是根据本发明的实施例能够操作装置、系统、方法和 / 或计算机程序的示例计算系统；

图 2 和图 2a 是根据本发明的实施例的示例系统；

图 3 是服务器模块的示例，该服务器模块包括软件 / 硬件模块和数据库、被安排成用于实现本发明的实施例；

图 4 是描绘根据本发明的实施例的计算机实现的注册过程的流程图；

图 5 是描绘根据本发明的实施例的计算机实现的许可过程的流程图；

图 5a 至图 5d 是根据本发明的实施例的计算机实现的过程；

图 6 是描绘根据本发明的实施例的计算机实现的简档创建过程的流程图；

图 7 是描绘根据本发明的实施例的计算机实现的简档更新过程的流程图；

图 7a 至图 7c 是展示根据本发明的实施例的计算机实现的过程的图；

图 8 是描绘根据本发明的实施例的针对于禁止、模糊和覆盖过程的计算机实现的系统指示过程流程图；

图 9 是描绘根据本发明的实施例的针对于禁止、模糊和覆盖过程的一系列计算机实现的过程流程的风格化的图；

图 9a 至图 9c 是展示根据本发明的实施例的计算机实现的过程的图；

图 10 是描绘根据本发明的实施例的用于创建禁止、覆盖或模糊区域的计算机实现的过程的流程图；

图 11 是描绘根据本发明的实施例的计算机实现的隐私约束过程的流程图；

图 11a 至图 11k 是展示根据本发明的实施例的计算机实现的过程的图；

图 12 是描绘根据本发明的实施例的计算机实现的感测 / 扫描过程的流程图；

图 13 是描绘根据本发明的实施例的计算机实现的占用过程的流程图；

图 14 和图 15 是描绘根据本发明的实施例的计算机实现的标识过程的风格化的图；以及

图 16 是展示根据本发明的实施例的计算机实现的标识过程的另一个示例的图。

实施方案描述

总体概述

[0033] 本发明总体上涉及一种用于对机器和装置进行注册、监测和控制的系统、方法、计算机程序和数据信号。具体而言，本发明的实施例涉及机器人装置、自主车辆、“智能”装置以及其他可编程和计算机控制装置的注册、监测和控制。

[0034] 更详细地，本文所描述的实施例的一个方面提供了一种用于控制机器人装置的方法。该方法包括在计算装置处接收被安排成用于在该机器人装置上实现操作的至少一条命令的步骤。当接收到该命令时，对其进行审核以确定该命令是否适合于执行并且将其指向

正确的机器人装置。只有在该命令适合于执行并且指向正确的机器人装置时，才将该命令提供给该装置。

[0035] 换言之，本文所描述的实施例的一个宽泛方面提供了一种用于控制和监测下发给自主或“智能”装置的命令的系统。这种系统对自主或智能装置有待在公共空间中被操作的情况是特别有用的，其中，这类装置的不恰当操作可能会对其他公众成员带来安全、保障和金融风险。

[0036] 该方法的一个实施例被编码在计算系统中，比如图 1 所示的计算系统。

[0037] 在图 1 中，示出了计算系统的示意图，该计算系统在本实施例中是适合于同本发明的实施例一起使用的服务器 100。服务器 100 可以用于执行应用和 / 或多个系统服务，如根据本发明的实施例的便于对命令进行控制、监测和下发的系统和方法。

[0038] 参考图 1，服务器 100 可以包括接收、存储和执行适当的计算机指令所需要的适合的组件。这些组件可以包括处理器 102、只读存储器 (ROM) 104、随机存取存储器 (RAM) 106、输入 / 输出装置（例如磁盘驱动器 108）、远程的或连接的输入装置 110（例如移动计算装置、智能电话或‘桌上’个人计算机）、以及一个或多个通信链路 114。

[0039] 服务器 100 包括多条指令，这些指令可以被安装在 ROM 104、RAM 106 或磁盘驱动器 112 中并且可以由处理器 102 执行。可以提供多个通信链路 114，这些通信链路可以不同方式连接至一个或多个计算装置 110 上，如服务器、个人计算机、终端、无线或手持式计算装置、或移动通信装置（如移动（蜂窝）电话）。多个通信链路 114 中的至少一个可以通过电信网络连接至外部计算网络上。

[0040] 在一个具体实施例中，该装置可以包括可驻留在存储装置 112 上的数据库 116。将要理解的是，该数据库可以驻留在任何适合的存储装置上，该存储装置可以包括固态驱动器、硬盘驱动器、光盘驱动器或磁带驱动器。数据库 116 可以驻留在单个物理存储装置上或可以分布于多个存储装置上。

[0041] 服务器 100 包括适合的操作系统 118，该操作系统也可以驻留在存储装置上或服务器 100 的 ROM 中。操作系统被安排成用于与数据库并与一个或多个计算机程序进行交互，以使服务器执行根据本文所描述的本发明的实施例的步骤、功能和 / 或程序。

[0042] 宽泛地讲，本发明涉及一种计算方法和系统，该计算方法和系统被安排成用于通过通信网络与一个或多个远程装置进行交互。这些远程装置可以采用如上所述的计算装置的形式，但是也可以采用机器人装置的形式，如稍后将更详细描述的。

[0043] 在一个实施例中，系统利用包括数据库的服务器，该数据库被安排成包含关于一个或多个实体的生物或其他标识信息。该数据库被安排成用于通过通信网络从该一个或多个远程装置接收信息并随后将信息传达至一个或多个远程机器人装置。

[0044] 图 2a 展示了适合于与本发明的实施例一起使用的面向服务的架构。

[0045] 该宽泛发明概念的其他方面涉及一种相应的方法、计算机程序、计算机可读介质和数据信号。该方法促进在一个或多个远程装置与集中式数据库之间传送关于有待发送至自主或“智能”装置（也称为“机器人”装置）的所期望的指令的多条命令。该集中式数据库接收请求以向该一个或多个远程装置提供命令，并通过通信网络将信息转发至该一个或多个远程机器人装置。

与系统的初始交互

[0046] 在一个实施例中，为了用户与系统的交互，该用户有必要标识自己并在系统中注册。这通过类似于很多其他消费者产品注册过程（如车辆的注册）的注册过程来实现。

[0047] 优选地，可以要求用户通过进行标识检查来证明或证实他们的身份。

[0048] 在一个实施例中，要求预期用户（“预期注册人”）建立“简档账户”或获得“电子许可证 (eLicence)”。出于本文所描述的更宽泛发明的目的，“简档账户”或“电子许可证”是用来证实用户身份的任何类型的数字和 / 或电子标识手段。在由数字 (ID) 身份有线公司（一家香港公司）提交的共同未决申请中，对电子许可证和简档账户的具有新颖性和创造性的实施例进行了更为详细的描述并通过引用结合在此。

[0049] 用户使用他们的电子许可证或简档账户（与其他标识信息（如密码）一起使用）来将装置（如装置 110) 通过通信网络连接或登录到注册服务器（如服务器集群 110a（图 2) 或注册服务器 300（图 3)。这种连接以及代码输入允许预期用户与服务器集群 110a 进行交互。

[0050] 一旦用户在系统中注册，那么用户就注册了他们的机器人装置。与车辆牌照或船舶牌照一样，优选地，用户仅有一个许可证，但能够注册多个机器人装置，因为该用户可能有不止一个机器人装置。

命令和控制系统

[0051] 每个机器人装置包括内部安全计算装置，该装置被安排成用于验证、认证并执行或者由机器人装置本身或者由外部生成的多个命令。

[0052] 也就是说，每个机器人装置包括内部“逻辑”，其中，在采取动作之前（或者是物理动作或者是其他动作），机器人装置首先接收“意图 (Intention)”。然后必须针对一些内部逻辑或规则（即策略）对该意图进行验证 (Validated)。一旦该意图得到验证，那么该意图就可以被传送 (Communicated) 至机器人装置的相关部分并因此得到批准 (Approved)。

[0053] 现在参考图 2 对命令与控制 (CC) 结构进行更为详细的描述。在图 1a 中，对服务器、计算系统、计算机或其他计算装置的任何引用是指具有类似于图 2 的服务器 100 的功能的服务器。

[0054] 现在参考图 2，示出了总体上标注为 100a 的一系列相互连接的服务器（服务器集群）。用户 102a 可以通过他们的客户端装置 104a 或他们的移动客户端装置 106a 与服务器集群 100a 进行交互。

[0055] 当机器人装置 108a 接收或生成请求（意图）时，该请求源自“意图”应用 110a。意图应用将该意图请求从意图应用 110a 传递至验证控制器（未示出）。验证控制器确保机器人装置和软件尚未被篡改。验证控制器还确保机器人装置的所有物理组件都正常工作并且被批准在策略准则内使用。

[0056] 接着对该请求进行加密并通过安全协议（虚拟专用网络 (VPN) 连接 112a) 传送至服务器集群 100a。如可能需要的，在使用密钥对认证或任何其他适合的加密方法进行传输之前，对所有的数据包进行加密。

[0057] 一旦连接，机器人装置就通过如移动电信网络 114a 等的公共通信网格建立安全虚拟专用网络 (VPN) 通道，其可以利用 3G（第三代 GSM 标准）和 / 或 4G（第四代 GSM 标准）蜂窝网络标准。

[0058] 所有到服务器集群 100a 的通信都经由安全防火墙服务 116a，该安全防火墙服

务限制在 VPN 内可使用的 VPN 端点和端口。对于该通道，使用适当的标准，如安全套接层(SSL)。

[0059] 了加密并且 VPN 通信是安全的且通过了防火墙，机器人装置就进行认证以建立与 CC 系统（即服务器集群 100a）的连接。在本文所描述的实施例中，利用认证服务器 118a 通过证书的交换来对机器人装置进行认证，但是将要理解的是可以利用其他认证方法或系统。

[0060] CC 系统 100a 进一步包括应用平台 120a，该应用平台管理通信、请求、清单分配以及最终对机器人装置的控制。在本文所描述的实施例的上下文中，在不首先通过应用平台 120a 的情况下，机器人装置无法执行动作。

[0061] 应用平台 120a 与策略引擎 120b 进行接口连接，因为每个注册的机器人装置的功能和允许的动作都作为策略存储在系统 100a 中。策略引擎 120b 允许如法律、装置能力和最终用户要求所要求的那样唯一地控制每个机器人装置。策略作为不可违背的基础准则集通过服务器集群 100a 传输至机器人装置。以下对应用平台和策略引擎的工作进行更为详细的描述。

[0062] CC 系统还负责记录对所采取的所有动作和从终端装置所接收的所有数据的审计跟踪。这包括一些数据，如机器人装置的制造商和型号、装置的能力、飞行清单（这种情况下机器人装置能够飞行）、飞行或移动的先前批准、GPS 移动和位置数据（包括相关联的时间和日期）、仪器指标等。这类信息存储在数据档案 (Data Archive) 122a 中，从而使得出于审计的目的可以对该信息进行访问（如果有必要的话）。

[0063] 网站 124a 作为界面被提供，以管理应用逻辑和所有相关联的数据 / 元数据。这包括如更新装置策略、能力清单以及包括特殊服务（如“模糊”和“覆盖”）（下文对其进行更加详细的描述）的其他服务等信息。

[0064] 快速的高输入 / 输出 (I/O) 数据保持服务 126a 对来自机器人装置的传入数据馈送进行缓存。一旦经过缓存，数据随后被移动至数据档案 122a，出于审计的目的，可以根据需要在该数据档案处对该数据进行数据挖掘。

[0065] 返回到最终用户 102a，web 界面提供来自客户端装置 104a 和移动客户端装置 106a 的访问。通过这些界面，最终用户能够安全地指示机器人装置采取动作、接收对装置状态的反馈并跟踪结果。所有进入客户端装置 104a 和移动客户端装置 106a 的通信都经由标准安全 web 协议和防火墙访问 128a 保障安全。

[0066] 一旦建立了连接，如前所述，消费者可以使用密码或生物交换针对平台进行认证以证明他们的身份（即，使用“简档账户”或“电子许可证”）。根据由最终用户和平台设置的策略，认证可以根据需要或严或松。

[0067] 在一系列数据库（总体上用计算系统 130a 表示）中，所有最终用户（消费者）数据都是安全的并且得到保护。在一个实施例中，可以要求用户付费以使用服务器集群 100a 提供的一些服务。在这种实施例中，最终用户可以通过标准的、安全的支付网关 132a 进行购买或现金交易。这种服务采用具有账户管理的购物车风格界面的形式。

[0068] 最终用户与 web 应用进行交互以执行多条机器人装置命令并接收反馈。这种应用提供用于机器人装置管理的一系列界面和逻辑。

[0069] 最终用户无论何时也不会对机器人装置进行直接访问。尽管最终用户会提供关于

他们的机器人装置以及他们希望这些装置在某些情况下做什么的一系列策略，但是这些策略并不会被直接应用，而是由策略引擎的进行审查。

[0070] 也就是说，将所有的策略与策略引擎 120b 进行交换和验证，以确保服务器集群 100a 具有对装置的最终控制权。这样，服务器集群 100a 利用“命令和控制”类型结构来控制机器人装置的移动和动作，以防止未授权的或非法的使用。

内部机器人装置验证

[0071] 每个机器人装置都能够执行一组预定义的动作（物理动作或其他动作），并且该组动作中的每一个动作都与一个或多个指令相关联。合起来，这些可允许的动作和相关联的指令形成了用于机器人装置的“策略”。

[0072] 例如，机器人无人飞机（无驾驶员飞行装置）或许能够在任何方向上飞行，但由于隐私、保障性或安全性原因，可能被限制仅在某些预定飞行空间中飞行。

[0073] 允许机器人装置执行命令所需的一个指令集将在每一次激活机器人装置时进行诊断测试。

[0074] 系统将包括一系列的‘测试’，以定期（例如，固定日期）测试开始。然而，由于问题会发生在定期检查之间（例如，消费者可能无意地或不知不觉地损坏他们的机器人），将要理解的是诊断测试也可能以随机的时间间隔进行。

[0075] 除了进行测试，可以收集测试数据，并且在一个实施例中，将测试数据传送至图 2 所示的服务器集群 100a。

[0076] 以下对在测试期间所收集的数据的类型的示例进行描述：

[0077] 系统已批准的诊断测试由特地为执行以下操作中一项或多项而编写的对象或组件来进行（完成）：

1. 对机器人进行标识，不限于例如：

1.1. 制造商、型号、类型；

1.2. 历史，例如相关日期 / 时间、测试结果；

1.3. 注册的拥有者 / 用户；

1.4. 具备有效的用户安全和保护机制，例如生物用户锁；

1.5. 装置当前是否是注册的，以及是否在其（挂起的）任务和 / 或功能过程期间将保持为注册的；

1.6. 硬件、软件和能力，不限于：功能规格、有效的‘默认故障’、‘占用’、‘约定’以及‘隐私’（例如软件）协议；

1.7. 批准按照用户请求的任务或‘受限的’功能来使用或操作装置，并且批准任务或功能应用（即，机器人‘应用 (app)’）本身，包括传递任何数字权限

2. 标识机器人的用户或控制者——具体而言，机器人关联于并接收来自具备有效账户和最新的简档的用户的任务或多条功能指令并且可以进一步确认该用户或控制者是否也作为被批准方被列出并要求该用户或控制者作为被批准方被列出，以便使用或控制此特定机器人（不限于生物认证）；

3. 分析并确认机器人的硬件和软件是否完好无损并保持未经篡改（例如，未被‘根植’、‘破解’或‘非法入侵’）；

4. 定位并标识机器人的系统中的硬件、软件、能力或其任何组合或机器人可能要或被

要求在其中或与其一起操作的系统的网络中的问题；

5. 进行性能或功能测试以证实最初保持的已批准的操作熟练度，例如：

5.1. 它具有或将要具有这些能力和功能容量（不限于可用的燃料或电费、有效载荷重量约束 / 容量）来可接受地完成它的任务或受限的功能；

5.2. 它当前的性能将满足所请求的任务或功能（以及在这些任务或功能过程期间）所需要的或期望的操作要求；

6. 确认机器人不具有任何未完成的维护、维修、检查或其他订单；

7. 确立机器人处理器是否具有或正在执行任何未批准的或非法的有效载荷—在一个实例中，通过分析移动灵活性，例如是否位于正常的基线值 / 参数以外，可以解释未批准的有效载荷重量；在另一个实例中，通过分析从在机器人范围之上、之中或之内的由可以检测未批准的有效载荷的传感器或扫描器获取的数据，例如这些装置可以是生物传感器、分子级扫描器、灵敏的电子化学鼻等。

[0078] 一旦系统接收到所有的注册、诊断和 / 或健康测试已经成功完成的确认，系统就发布相关的许可码以允许机器人装置执行功能。

更为详细的命令和控制结构

[0079] 图 3 是展示了注册服务器的不同组件的方框图，该注册服务器等同于图 2 中总体上以标号 100a 示出的结构。图 3 中所示的服务器 300 展示了参考图 2 描述的实施例的替代视图，图 3 被分为功能模块而非物理硬件。也就是说，图 3 并未将图 2 所示的应用服务器群 120a 和策略引擎 120b 以及公共访问基础设施的一些方面（例如服务器 130a 和 132a）描绘为分离的组件，而是解释这些组件如何在功能上相互作用。

[0080] 换言之，图 2 是根据更宽泛发明概念的服务器基础设施的一个实施例的图例。图 3 是根据更宽泛发明概念的基础设施的一个实施例的高级“模块”图例。图 2 和图 3 提供了相同发明概念的不同视角并且不应当用于导向不同的发明，而是导向相同宽泛发明概念的不同视图。

[0081] 服务器 300 包括各种模块和数据库，这些模块和数据库提供的功能使机器人装置受到监测、控制和管理，以便支持例如安全性、保障性和隐私性考虑。以下提供每个模块的简短概述：

301 管理模块

[0082] 管理模块 301 用于向一个或多个机器人装置传输系统管理功能命令。这些命令可以包括很多机器人装置共用的命令，这些命令包括电源开和关、设置访问控制、软件更新、性能监测、统计数据收集和 / 或不直接涉及诊断测试、许可码的其他管理功能和 / 或监控‘流氓’机器人。

302 通信模块

[0083] 系统进一步提供通信模块 302，该模块能够在机器人装置和注册服务器 300 和 / 或其他注册服务器（未示出）之间生成通信。

[0084] 进一步地，在通信模块 302 的另一种使用方法中，许可码（可以在许可码数据库 331 中生成、输出或存储）可以传输至用户的机器人、装置或车辆。

[0085] 另外，通信模块 302 还可以通过其他实体（或相同实体）促进与服务器 300 的通信，以促进操作、活动或任务，诸如：

■维护，该操作可以结合订单模块 310 进行，订单模块访问注册机器人数据库 323 以确定需要处理的任何未完成订单；

■软件更新，在发布给在注册机器人数据库 323 中列出的注册机器人、装置或车辆之前，软件更新被分配给并存储在制造商和机器人数据库 324 中，任务 / 活动 / 程序模块 312 实现这种发布；

■简档上传，该操作来自用户 / 所有者 / 客户账户数据库 321，随后存储在简档数据库 332 中；

■机器人注册应用上传，该操作由任务 / 活动 / 程序模块 312 与机器人数据库 324 以及注册机器人数据库 323 合作提供；

■用户、应用上传，该操作来自用户 / 所有者 / 客户账户数据库 321；

■监视数据上传，该操作来自用户的机器人或装置，来自用户 / 所有者 / 客户账户数据库 321 和机器人 'App' / 功能数据库 325，以便例如确认用户或所有者是否被授权进行监视操作；

■标识机器人或装置的用户或控制者；和 / 或

■接收用户隐私约束，该操作通过禁止 / 隐私协议模块 307。

303 交易模块

[0086] 交易模块 303 用于处理金融交易以便支付由服务器 300 或相关联的、有关的第三方提供的服务。

[0087] 在一个实施例中，交易模块 303 负责发布或处理用户、所有者或客户的产品和 / 或服务订阅账户，这些账户可以在用户 / 所有者 / 客户账户数据库 321 中列出。这类订阅可以用于禁区或隐私约束（不限于覆盖或模糊）的发起或执行。

[0088] 而且，交易模块 303 可以负责发布或处理与例如（不限于）机器人、装置或车辆的不适当的、未授权的、未注册的、不正当的、非法的或违规的使用、控制、管理或拥有相关的罚款、侵权或处罚。这些罚款、侵权或处罚可以利用任务 / 活动 / 程序模块 312、占用协议模块 309 和 / 或通信模块 302 传送至相关方。

304 控制器

[0089] 在一些实施例中，列出的模块和数据库自主地进行操作。然而，在本文描述的实施例中，中央控制器 304 用于提供“监督 (supervisory)”功能。中央控制器可以自主地操作或可以由用户来控制，以便“重写 (override)”任何单个模块的自主运行。例如，如果检测到对系统的破解的危害，用户可以使用控制器来重写任何给定的许可码或给予特定机器人装置的其他许可。

305 建议的和活跃的任务 / 功能和行进计划和跟踪模块

[0090] 建议的和活跃的任务 / 功能和行进计划和跟踪模块 305 负责多种过程或任务，包括接收、分析、存储和（如有必要）输出最终用户建议的机器人装置命令。

[0091] 建议的和活跃的任务 / 功能和行进计划和跟踪模块 305 使用用户 / 所有者 / 客户账户数据库 321 或无资格数据库 322 中存储的数据或信息来确认建议的任务或功能是允许的，即可以得到授权。

[0092] 建议的和活跃的任务 / 功能和行进计划和跟踪模块 305 还使用注册机器人数据库 323 中存储的数据和信息来确定具体类别、型号或类型的机器人装置是否具有硬件、软件或

能力（包括功能性的或操作性的）来从事并成功地完成建议的任务、操作或功能。

[0093] 建议的和活跃的任务 / 功能和行进计划和跟踪模块 305 还根据机器人 'App' / 功能数据库 325 中的信息和 / 或操作空间数据库 326 中的信息来确认建议的或活跃的任务、操作或功能是可允许的或得到授权的，这些信息包含批准的、'受限的' 或不允许的任务、操作或功能。

[0094] 建议的和活跃的任务 / 功能和行进计划和跟踪模块 305 可以协商、检查和 / 或确认服务器 300 的数据库或模块中的一个或多个中包含或存储的信息和数据，以便运行任何必要的测试，例如那些可由诊断测试数据库 327 进行的测试。

306 许可码模块

[0095] 许可码模块 306 允许生成适合的授权码，目的是允许或批准用户机器人、装置或车辆从事或成功地完成任务、操作或功能。

[0096] 在一些实例中，许可码模块 306 可致使机器人、装置或车辆执行用户可能未建议或发起的另一类任务、操作或功能。

[0097] 在执行任务之前需要进行诊断测试的情况下，成功通过诊断测试之后，任务 / 活动 / 程序模块 312 可指令许可码模块。

307 禁止 / 隐私协议模块

[0098] 禁止 / 隐私协议模块 307 可以是服务器 300 的组件，该组件负责处理处理所有隐私相关的事项，例如但不限于禁区、覆盖和模糊，它们在其他方面可能被认为是隐私约束。

[0099] 在一个实施例中，禁止 / 隐私协议模块 307 包括基于 web 的接口，该接口允许用户访问可用的服务器工具或特征或与其交互，这些服务器工具或特征创建、建立、修改、移除和 / 或支付隐私约束和 / 或订阅或相关联用户账户。这类账户可以在用户 / 所有者 / 客户账户数据库 321 中列出或由其存储。当有必要允许例如用户创建、建立、修改或移除账户时，禁止 / 隐私协议模块 307 可以与用户 / 所有者 / 客户账户数据库 321 进行通信，该账户可以仅为实施隐私约束（可以传达给其他人的机器人、装置或车辆以便于执行或实施）而存在。通信模块 302 可以促进用户的（位于远程位置上的）装置和禁止 / 隐私协议模块 307 之间的连接，该装置用于连接至服务器 300。通信模块 302 还可以促进隐私约束发布至其他服务器和 / 或用户机器人、装置或车辆。

[0100] 禁止 / 隐私协议模块 307 还可以例如通过变更或修改机器人 app 或功能来改变机器人 'App' / 功能数据库 325，方式不限于在执行具体任务、操作或功能时允许机器人进入特定空间或在其中行进。

[0101] 在这种情况中，可以更改操作空间数据库 326 以便将变化反映到行进空间中。

[0102] 在另一个实例中，禁止 / 隐私协议模块 307 可以与诊断测试数据库 327 进行通信，其目的不限于以下内容：变更、修改、分析、审核和 / 或确认诊断测试数据库 327 将恰当地且精确地指令或命令机器人、装置或车辆，以便在任务、操作或功能之前、期间或之后针对禁止 / 隐私协议模块 307 中列出的或存储的任何现有的隐私约束或对其新近的改变执行所有必要的测试。

[0103] 例如，用户可以形成或创建新的隐私约束，该新隐私约束可能带来机器人、装置或车辆事先未处理过的特定挑战或一组不同参数。因此，在诊断测试数据库 327 上对相关或可应用的诊断测试进行修改和 / 或添加，这会使所有相关的或可应用的机器人、装置或车

辆在下一次需要时从事或成功地完成更新的诊断测试。

[0104] 禁止 / 隐私协议模块 307 可以与有效载荷数据库 328 进行通信以便形成新的授权有效载荷列表或者更改或修改现有的列表，该列表在机器人、装置或车辆之中或之上携带，或由其携带。某些隐私约束可以指定哪些机器人、装置或车辆可以携带或运输具体有效载荷。授权的有效载荷也可以由施加在用户上的任何限制来指定，该用户在用户 / 所有者 / 客户账户数据库 321 中列出。

[0105] 禁止 / 隐私协议模块 307 还可以与监视数据库 330 进行通信，以便更改或修改授权的和未授权的监视区域。针对监视数据库 330，可以进一步使用操作空间数据库 326 实现相同目的。

[0106] 禁止 / 隐私协议模块 307 还可以与简档数据库 332 进行通信，以便实现可能涉及简档的任何隐私约束。例如，用户可以在通信模块 302 的协助下利用他们的机器人、装置或车辆将新的或更新的简档上传至服务器 300 的简档数据库 332，对主简档的任何更新涉及与禁止 / 隐私协议模块 307 进行通信的隐私约束，然后该简档被发布到任何相关的或可应用的机器人、装置或车辆上。

308 约定（传感器 / 扫描器）协议模块

[0107] 约定（传感器 / 扫描器）协议模块 308 是负责处理所有约定协议（不限于‘感测 / 扫描’操作的示例）的服务器 300 的组件。这些协议可以涉及将机器人、装置或车辆重新定位至指定的位置。约定协议可以由注册方、用户、主管部门或其他利益相关者或第三方从服务器 300 的一个或多个数据库或模块（不限于约定（传感器 / 扫描器）协议模块 308）来形成、建立、修改或移除。

[0108] 以‘感测 / 扫描’约定协议为示例场景，这类协议使用在专用或共享硬件或其他外围设备上执行的软件应用，在一个示例中，这些硬件或其他外围设备使机器人、装置和车辆执行预定义的操作。进一步地，约定（例如传感器 / 扫描器）协议模块 308 可以与一个或多个数据库进行通信，例如用户 / 所有者 / 客户账户数据库 321 或注册机器人数据库 323，以确定哪些用户、所有者或客户要求他们的机器人、装置或车辆由示例传感器或扫描器进行测试或检查。

[0109] 约定（例如传感器 / 扫描器）协议模块 308 还可以与建议的和活跃的任务 / 功能和行进计划和跟踪模块 305 进行通信，以便计划、编程、计算、预计或期望哪些机器人、装置或车辆在何时或何地可能‘被号召’（适合的情况下）履行约定协议。例如，机器人可以位于感测 / 扫描站附近，因此在恰当的时刻激活或发起相关的约定协议。

[0110] 在另一个示例中，利用隐藏（最终的）约定位置或地点的办法作为示例场景，当激活机器人、装置或车辆以进行感测或扫描时，约定（传感器 / 扫描器）协议模块 308 可以利用通信模块 302 与机器人、装置或车辆进行通信，以便控制它的监视或跟踪能力，尤其是根据未授权方可以查看或存储的数据。

[0111] 操作空间数据库 326 或监视数据库 330 可以提供可能需要遵守的（最新的）隐私约束，以便例如保护传感器 / 扫描器站点位置或地点的机密性。操作空间数据库 326 还可以不时地更新站点位置或地点。

[0112] 某些许可码由许可码模块 306 生成，或从许可码数据库 331 获得或针对许可码数据库进行确认。发送的许可码可以是数据信号，该数据信号使机器人、装置或车辆发起或执

行特定的任务、操作或功能，或者为了本实例或者为了另一个实例的目的。

[0113] 在另一个示例中，约定（传感器 / 扫描器）协议模块 308 可以生成机器人、装置或车辆的正检测结果，然后该正检测结果致使发起另一个协议，例如占用协议模块 309 运行的‘占用协议’。占用协议重写任何一方传达至机器人、装置或车辆的任何先前的命令或指令，以便例如指令机器人、装置或车辆替代地执行由注册器或主管部门发布的新命令或指令。

[0114] 占用协议命令将机器人、装置或车辆编程为从事或成功地完成特定的任务、操作或功能。例如，该任务可以到操作空间数据库 326 中列出的指定空间（例如，拘留所）。进一步地，不同类型或型号的机器人、装置或车辆（可以在注册机器人数据库 323 中指定）可以具有不同的指定空间。

309 占用协议模块

该模块命令用户的机器人、装置或车辆重新定位至注册的指定空间。该空间可以存储在操作空间数据库 326 中。在不同的实施例中，命令可以传送或上传至机器人、装置或车辆中（利用通信模块 302）。传送的具体数据信号（例如输出文件）可以触发机器人、装置或车辆上安装的软件应用，并且该应用将执行大部分计算。在其他实施例中，服务器 300 运行可应用的软件应用（作为主机），并且位于远处的机器人、装置和车辆（客户端）仅仅是从服务器 300 接收命令的船舶。

310 订单（维护 / 维修 / 检查）模块

[0115] 模块 310 命令用户的或所有者的机器人重定位至指定空间。该空间可以在操作空间数据库 326 中列出。模块 310 还可以结合涉及维护、维修、检查或其他事项的所有必要信息、数据、任务、活动或要求。该模块 310 也可以是机器人、装置和车辆测试装置使用的主模块；因此，不仅用于唆使机器人、装置和车辆重新定位，而且通过命令、从事或实现（例如未完成的）订单，还能够在机器人到达重定位目的地后使用。

[0116] 在另一个方面，该模块 310 可以与批准的和历史的任务 / 功能和行进计划和轨迹数据库 329 进行通信（例如，可能利用通信模块 302）以便向服务器 300 通知机器人、装置或车辆相对于以上段落描述的指定空间的位置或地点。服务器和任何相关用户、所有者或客户可以在任何订单事项上保持更新。

312 任务 / 活动 / 程序模块

[0117] 该模块可用于很多应用。例如，模块可以负责操作、管理、监测和控制（在本文中，本发明，根据上下文这些术语可以称为‘运行 (running)’或‘运行 (run)’）服务器 300 的数据库或其他模块中的一个或多个。

[0118] 以下给出一些非详尽示例：

- 诊断测试数据库 327：312 模块与数据库 327 接口连接，以便在必要时利用数据库 327 中包含的数据（远程地）运行机器人诊断测试。这些测试涉及的要求可以是在发布许可码之前机器人的用户或所有者是熟手或得到批准的，以便执行任务或功能。在另一个非限制性示例中，测试可以涉及优选地正在用户或所有者的机器人上进行维护、维修、检查或其他订单的授权方。

- 机器人‘App’/ 功能数据库 325：312 模块可以与数据库 325 接口连接，以便检查机器人应用（‘app’）的适用性或批准由用户或所有者的机器人使用和 / 或机器人 app 市场上

的接受情况，这些情况可以公开地或秘密地获得。进一步地，312 模块可以与数据库 325 接口连接以进行公开或秘密的检查或评估，即在确定 app 或功能的适用性或批准过程中，系统可以允许开源的或闭源的评价、评论和 / 或反馈。

- 简档数据库 332 :312 模块可以与数据库 332 接口连接以便运行用户、所有者或客户的简档输入和输出。在一个示例中，新的或更新的简档数据可以发送至服务器并且 312 模块可以负责分配到现有的各个主简档或创建新的主简档账户。

[0119] 在另一个示例中，312 模块还负责与简档数据库 332 接口连接以便确定主简档的精确度百分比。

[0120] 换言之，模块 312 可以改变分配给具体主简档的精确度百分比。然后将此变化发布给可应用的或相关联的用户，该变化将用信号通知用户需要更新主体简档。服务器进行发布或与远程装置（例如机器人）进行通信可以由通信模块 302 来唆使。

[0121] 如果简档还应用于或例如注册用于隐私保护，例如简档禁区、简档覆盖或简档模糊，那么这些来自简档数据库 332 的那些可应用的简档可以与操作空间数据库 326 接口连接（在禁止空间的情况下）并且结合禁止 / 隐私协议模块 307 来实现这些隐私约束。进一步地，在执行上述程序时，例如模块 312 和简档数据库 332 在必要时可以与用户 / 所有者 / 客户账户数据库 321 交互。例如，简档数据库 332 中的简档可以与用户 / 所有者 / 客户账户数据库 321 中的具体账户相链接或相关联。

[0122] 在一个实施例中，任务 / 活动 / 程序模块 312 促进监控‘流氓机器人’或未注册的、未许可的、非法的、非参与的等等这样的机器人、装置和车辆。在一个方面，利用来自传感器、扫描器或其他监视捕获装置（安装在用户的机器人、装置或车辆上）和传输至服务器 300（利用通信模块 302）并由监视数据库 330 接收或存储在其中的数据和信息，任务 / 活动 / 程序模块 312 可以运行监测例如监视信息或数据的软件程序，这些信息或数据包括标识在空间中存在或正在操作的‘流氓机器人’的因素或由标识这些因素构成，而该空间并未与建议的和活跃的任务 / 功能和行进计划和跟踪模块 305（连接操作空间数据库 326）中列出的或在其中存储的任何任务、操作或功能相关联。

[0123] 换言之，监视数据库 330 接收数据 ；该数据可以是例如机器人的捕获视频图像 ；可以针对于或利用图像文件来记录在何处以及何时捕获该图像，任务 / 活动 / 程序模块 312 并且然后与包含在建议的和活跃的任务 / 功能和行进计划和跟踪模块 305、监视数据库 330、注册机器人数据库 323、制造商和机器人数据 324、机器人‘App’/ 功能数据库 325、操作空间数据库 326 和简档数据库 332 中的数据进行交叉标引。

[0124] 更为详细地 ：

■任务 / 活动 / 程序模块 312 可以操作用于执行本文描述的（即便不是全部）大部分功能，不限于以下数据库和模块列表中列出的或存储的交叉标引数据和信息 ；

■建议的和活跃的任务 / 功能和行进计划和跟踪模块 305 可以允许标识当前活跃的任务、操作和功能以及它们出现的地点和时间 ；

■监视数据库 330 可以接收并包含有待搜索的原始或未处理的机器人参考数据，不限于有待标识的机器人的数字图片 ；

■在处理监视数据之后，注册机器人数据库 323 可以提供有关任何已标识机器人的注册状态的信息 ；

■制造商和机器人数据库 324 可以提供有关机器人的具体类型或型号的数据或图形表示信息，以促进所述表示和监视数据的比较和对比；

■如果注册的机器人最近执行过或当前正在执行软件应用（该软件应用会使注册的机器人在特定的时间出现在特定的地点上），机器人‘App’/ 功能数据库 325 可以允许另一种形式的检查和确认；

■操作空间数据库 326 可用于将有关特定空间的数据或信息添加到监测数据中；以及

■简档数据库 332 可以列出或存储各种相关的机器人简档，以协助本发明的这个方面确定监视数据中捕获的（无形）有形的元素、主体或对象。

321 用户 / 所有者 / 客户账户数据库

[0125] 用户 / 所有者 / 客户账户数据库 321 包括参与本文描述的系统的所有用户的数据结构。用户 / 所有者 / 客户账户数据库 321 包含与以下内容相关的数据，但不限于：

■用户、所有者或客户的身份，并且该身份链接至简档数据库 332 上列出的或存储的一些或所有信息或数据或者与它们相关联，诸如简档图片或其他媒体文件；

■如果用户、所有者或客户链接至任何注册的机器人、装置或车辆或与其相关联，一些或所有数据就在注册机器人数据库 323 中列出；

■历史事件（日期或时间），链接至用户、所有者或客户或与其相关联，例如与用户、所有者或客户相关或可用于他们的一些或所有信息此时可以在批准的和历史的任务 / 功能和行进计划和轨迹数据库 329 中列出或存储；

■是否用户、所有者或客户当前具有或形式上具有有效的安全和 / 或保护机制或‘密钥’，不限于用于访问或登录至他们的机器人、装置或车辆的生物标识锁或简档数据，或他们的用于支付维修费用、处理隐私约束事项（创建、修改等）的注册账户等，并且与简档相关的关联或可应用的数据或信息可以从简档数据库 332 中列出或存储的数据或信息获得或利用它们来引用；

■是否用户、所有者或客户事先已经或当前正在与机器人、装置或车辆（它已经是、过去是或仍然是被‘根植的’、‘破解的’或‘非法入侵的’）相关联，或者是否就机器人、装置或车辆的硬件、软件或能力而言已经存在问题或值得注意的报告，并且这样的信息或数据可以在注册机器人数据库 323 中列出或存储。

■是否用户、所有者或客户具有链接至或相关联的机器人、装置或车辆的任何未完成订单（可以涉及维护、维修或检查请求），并且是否与订单有关的这类信息或数据可以在注册机器人数据库 323、订单（例如，维护 / 维修 / 检查）模块 310 和 / 或诊断测试数据库 327 中列出或存储；

■是否用户、所有者或客户针对他们的身份具有在他们的账户文件中列出或存储的任何特殊的豁免权、许可、授权或免除权，不限于使他们的机器人、装置或车辆运行监视应用以允许父母监视他们的孩子的行走或赶上汽车去学校 / 从学校来，或者允许他们的机器人、装置或车辆携带特定的有效载荷或从事某个‘受限的’功能，这些信息或数据可以在有效载荷数据库 328 中列出或存储。

322 无资格数据库

[0126] 无资格数据库 322 包括无资格用户、所有者或客户的列表。无资格可以是针对于各种应用、活动或请求，例如特定的用户、所有者或客户可能太年轻（例如，法定年龄以

下），不足以占有或具有向特定类型或型号的机器人、装置或车辆指令、命令或传达任务、操作或功能的权限。在一个实施例中，无资格数据库 322 由任务 / 活动 / 程序模块 312 进行操作，并从制造商和机器人数据库 324 接收协作的信息或数据，这些信息或数据规定了特定类型或型号的机器人、装置或车辆的硬件、软件和能力（即规范）。

[0127] 被认为无资格的机器人、装置或车辆可以在无资格数据库 322 中列出，并且相应的无资格等级或状态链接至或与用户 / 所有者 / 客户账户数据库 321 中可以列出的用户账户或与其相关联。

323 注册机器人数据库

[0128] 注册机器人数据库 323 包括与机器人、装置或车辆（已经由它们的用户、所有者或客户注册）相关的信息。无资格的或可能变为无资格注册的机器人、装置或车辆相反可以在无资格数据库 322 中列出或存储。

324 制造商和机器人数据库

[0129] 制造商和机器人数据库 324 包括与机器人、装置或车辆的制造商有关的数据或信息。更为详细地，制造商和机器人数据库 324 列出了服务器 300 的系统所识别的所有机器人、装置和车辆。

[0130] 进一步地，制造和机器人数据库 324 包括与‘类型批准’方法有关的数据，典型地这些数据与符合性标识 / 资格相关联。例如符合性过程的一部分可以为特定的机器人类型建立性能基线，该基线需要高于符合性批准的所需标准。

[0131] 进一步地，与符合性事项相关的数据可以存储在制造和机器人数据库 324 中。当从事诊断测试时，例如由任务 / 活动 / 程序模块 312 结合诊断测试数据库 327 来进行，可以引用制造和机器人数据库 324 以获得任何所需的数据或信息。

325 机器人‘App’/ 功能数据库

[0132] 机器人“App”/ 功能数据库 325 包括与批准的或未批准的机器人、装置或车辆软件应用相关的数据。

[0133] 更为详细地，服务器 300 使用机器人‘App’/ 功能数据库 325 列出或存储所有可用的‘app’供用户、所有者或客户下载和 / 或购买，以用于他们各自的机器人、装置或车辆。那些团体可以访问或登入到他们的注册账户、导航基于 web 的接口以便搜索、选择和购买，然后下载所需的 app。

[0134] ‘app 市场’可以与前述模块和 / 或数据库中的任何一个或多个接口连接。例如：

■通信模块 302，该模块被安排成用于促进数据传输以便：访问账户、完成任何交易活动、从服务器 300 和 / 或另一个机器人、装置或车辆下载任何相关文件；

■任务 / 活动 / 程序模块 312，用于操作基于 web 的‘app 市场’或 API 接口；

■交易模块 303 促进 e、f、s 和 / 或 m 商务活动；

■用户 / 所有者 / 客户账户数据库 321 负责指派限制、规则，列出 / 存储和 / 或宣传与具体 app 相关的任何可适用或相关的信息；

■无资格数据库 322 控制哪些团体无资格下载特定的 app；

■包括机器人、装置或车辆已经拥有的 app 列表的注册机器人数据库 323 可以是有资格的或者与特定的 app 相兼容的；

■制造商和机器人数据库 324 指定适合于使用或与特定 app 相兼容的 app，或提供指导

方针或参数以特定于不同类型的机器人、装置或车辆；

■机器人‘App’/ 功能数据库 325 包括针对于‘app 市场’中可用的所有类型的机器人、装置或车辆的批准或未批准 app 列表；

■操作空间数据库 326 公开被授权一起工作的或被批准由 app 使用的所有空间，这些空间可以通过说明具体区域的基于 web 的交互式地图进入；

■诊断测试数据库 327 确定在机器人、装置或车辆上执行具体 app 之前、在执行这些 app 期间和 / 或之后应当或必须运行哪些测试；

■有效载荷数据库 328 确定哪些有效载荷（如果存在的话）可以与特定的 app 一起使用；

■批准的和历史的任务 / 功能和行进计划和轨迹数据库 329 提供统计数据或信息，这些统计数据和信息与特定 app 已经使用的场合的数量有关；

■监视数据库 330 针对机器人、装置或车辆执行的监视活动通知‘app 市场’中哪些 app 具有施加在它们上的限制；

■简档数据库 332 确定哪些简档需要交换或传输至服务器 300 和 / 或另一个机器人、装置或车辆。

326 操作空间数据库

[0135] 提供包括批准用于机器人、装置或车辆的环境、地点、区域或空间的完整清单的操作空间数据库 326。任务 / 活动 / 程序模块 312 与该数据库接口连接以便将信息传输至机器人、装置或车辆。

[0136] 更具体地，操作空间数据库 326 管控机器人、装置或车辆的具体任务、操作或功能。例如，出于安全、保障或隐私考虑，特定的大气空间可以永远不为所有或特定的机器人、装置或车辆使用。

327 诊断测试数据库

[0137] 诊断测试数据库 327 包括用于在机器人、装置或车辆上执行的多种测试。在一个实施例中，在请求进行测试时，机器人、装置或车辆使用服务器 300 的诊断测试数据库 327，和 / 或服务器 300 可以引用它的诊断测试数据库 327 以确认机器人、装置或车辆在其自己的数据库和 / 或模块上具有正确的测试。

[0138] 服务器 300 的任务 / 活动 / 程序模块 312 和 / 或通信模块 302 分别用于：

(i) 在机器人、装置或车辆上或针对于它们远程地运行或执行测试；以及

(ii) 为了这些目的，促进到主机（例如注册服务器 300）和客户端（例如用户、所有人或客户的机器人、装置或车辆）的任何必要传输 / 从它们的传输。

329 批准的和历史的任务 / 功能和行进计划和轨迹数据库

[0139] 批准的和历史的任务 / 功能和行进计划和轨迹数据库 329 包含注册器、主管部门或其他第三方批准的机器人、装置或车辆任务、操作或功能，它包括用于机器人、装置或车辆的许可操作空间行进。

[0140] 在批准或修改任何建议的或活跃的任务、操作或功能之前，建议的和活跃的任务 / 功能和行进计划和跟踪模块 305 传达或引用在批准的和历史的任务 / 功能和行进计划和轨迹数据库 329 中包含的信息或数据。

[0141] 与批准的和历史的任务 / 功能和行进计划和轨迹数据库 329 协作之后，在建议的

和活跃的任务 / 功能和行进计划和跟踪模块 305 已经认为任务、操作或功能是可接受的或经批准的之后，使用许可码模块 306 生成任何相关的或适当的许可码。

330 监视数据库

[0142] 除了本文已经描述的一些方面之外，监视数据库 330 可用于从多个机器人、装置或车辆采集特定的监视数据或信息。

[0143] 用户可以运行特定的软件应用（可以在机器人 'App' / 功能数据库 325 中列出或存储），并且该应用携带将特定监视数据（例如与时间、数据或位置相关）转发至服务器 300 以进行分析、处理、存储等的规定。通信模块 302 可以促进服务器 300 和远程机器人、装置或车辆之间的传输。然后，任务 / 活动 / 程序模块 312 可以将相关的、适当的或有价值的数据路由至监视数据库 330（例如在过滤之后）。

331 许可码数据库

[0144] 许可码数据库 331 可以列出或存储所有发布的历史或当前活跃码以及它们各自的任务、操作或功能细节（它发布给哪个机器人、涉及的用户、时间 / 日期等），并由许可码模块 306 运行。许可码数据库 331 还可以用于确保特定代码不会再次使用，或仅在适合的隔离期之后就回收。

[0145] 图 4 至图 7 的流程图展示了在机器人可以操作（在特定时间或以特定的方式或在特定的空间中）之前发布许可码给它们的过程。本实施例利用 '公共' 空间作为示例，但更宽泛发明概念可以扩展到任何物理的或虚拟的空间。

[0146] 参考图 4，示出了与总体上在图 3 中示出的注册器（即服务器 300）和与总体上在图 2 中示出的服务器系统（即服务器集群 100a）相一致的注册器的典型过程流程。

[0147] 在步骤 402，用户通常希望为特定的功能而使用机器人。在进入步骤 406 之前，如果消费者没有机器人，在步骤 404 他可能希望购买或以其他方式获得机器人，在步骤 406 用户确定是否在公共空间中使用该机器人。

[0148] 如果消费者希望在公共空间中操作他们的机器人，过程流程继续到步骤 412，在该步骤确定消费者是否拥有有效的机器人账户。如果消费者没有账户，在步骤 414 进一步确定消费者是否有资格获得账户。如果消费者没有资格获得账户，在步骤 416 消费者可以进行注册以确定以后他们是否可以有资格获得账户。

[0149] 如果消费者有资格获得账户，在步骤 418，消费者获得有效账户。

[0150] 一旦系统确定该消费者具有有效账户，在步骤 420 就进行检查以确定该消费者的机器人是否进行了注册。如果该机器人没有注册，那么在步骤 422，确定该消费者的机器人是否有资格注册。如果该机器人对注册而言是不可注册的，在步骤 424 消费者可以获得机器人，然后该有资格的机器人可以继续通过步骤 406 的流程过程。如果消费者的机器人有资格注册，在步骤 426 该消费者注册该机器人，该过程流程可以如图 5 所示继续进行。

[0151] 现在参考图 5，一旦确定授权了消费者操作机器人并且对该机器人进行了注册和授权以执行动作，那么在步骤 428，确定是否消费者的机器人具有未完成订单。如果是，过程流程继续至步骤 430，在该步骤消费者得到通知，在步骤 430 消费者做出应答，并且满足订单，并且在步骤 434 恢复该机器人。此后，该机器人准备接收未来的订单并且在步骤 440 过程流程继续进行，在步骤消费者向机器人传达任务或功能指令。

[0152] 参考图 5a，所示的图例展示了根据本发明的软件应用的概念。

[0153] 参考图5b，描述了由机器人装置生成、处理和接收命令的方式的过程流程。在步骤A001，外部命令或请求生成器1（例如，用户和/或用户的“智能”装置或机器人附件）生成命令或请求（包括任何元数据）。

[0154] 在步骤A002，该命令或请求（包括任何附加的信息或元数据）传送8至远程服务器2（或机器人注册器）。在步骤A003，远程服务器2接收并评估该命令或请求，然后生成评估判定。

[0155] 在步骤A004和A005，如果该判定是有条件地批准该命令和请求（受限于未解决的评估要求的结果或响应的批准），远程服务器2将未解决的要求或指令（例如，评估、诊断或健康测试指令）传达9至机器人6的接收器/发送器模块10。

[0156] 因此，在一个实施例中，在原则上首先批准该命令或请求（例如，操作任务），然后在得到授权以便完成命令或请求之前需要对机器人进行审查（例如以确保它能够完成任务）（例如类似两部分程序或评估）。

[0157] 接收器/发送器模块10将要求或指令发送至机器人6的管控‘芯片’3（例如，机器人本地的机器人注册装置），该芯片可以是软件、硬件和/或固件，并且可以包括一个或多个分离地、依赖性地或独立地协同工作的装置。这些装置可以集成到机器人模块或单元中，例如中央处理单元（CPU）。

[0158] 在步骤A006和A007，管控芯片3促进和/或监督机器人测试或查询、将结果或响应传送9至远程服务器2（例如，通过机器人6的接收器/发送器模块10）。

[0159] 在步骤A008，远程服务器2接收并评估结果或响应，然后生成评估判定。（注意：步骤A004至A008可以经历很多循环或重复，例如以便在先前的查询或测试结果或响应的接收、评估和判定之后促进进一步的查询或测试）。

[0160] 在步骤A009，在接收和评估机器人6的结果或响应之后如果确定批准命令或请求，那么远程服务器2将命令或请求传送9至机器人6的接收器/发送器模块10。接收器/发送器模块10将命令或请求传输至于机器人6的管控芯片3。

[0161] 在步骤A010，管控芯片3促进将命令或请求传输至机器人6的输出5，这基本上使得命令或请求得以实现。

[0162] 参考图5c，该图是命令和控制序列的另一个示例。在步骤B001，外部命令或请求生成器1生成命令或请求。

[0163] 在另一个实施例中，内部命令或请求生成器7（例如，机器人6的自主逻辑或‘大脑’）生成命令或请求。在一个示例中，机器人检测它的环境中的情况，例如不利的或恶劣的天气，在此情况下内部逻辑评估使机器人需要生成请求，例如允许实施绕行到目的地，即避免恶劣天气。

[0164] 由于绕行将涉及新的行进路径，在允许机器人实行新路线之前，机器人首先需要它得到批准。在步骤B002，将命令或请求传送12（或传输11，根据步骤B001中的其他实施例）至机器人6的输入模块4。机器人6的输入模块4将命令或请求传输至机器人6的管控‘芯片’3。

[0165] 在步骤B003，机器人6的管控芯片3评估该命令或请求，然后生成评估判定。在步骤B004和B005，如果该判定是有条件地批准该命令或请求（受限于未解决的评估要求的结果或响应的批准），那么管控芯片3促进和/或监督机器人测试或查询以建立所述结果或响

[0177] 在步骤C007，如果确定批准命令或请求，管控芯片3促进将命令或请求传输至机器人6的输出5，这等同于命令或请求由机器人6实现。

[0178] 一旦接收了指令，在步骤445，机器人开始进行诊断测试，随后在步骤450，将机器人测试数据发送到注册器，在步骤455，确定机器人是否已经成功地完成了诊断测试。如果未完成，在步骤460终止处理，因为消费者的机器人并未发布在公共空间中执行任务和/或执行限制功能所需的许可码。如果机器人成功地完成了诊断测试，在步骤465注册器向消费者的机器人发布适当的指令或许可码，并在步骤470消费者的机器人执行任务或功能。执行任务或功能之后，在步骤475可以任选地更新注册器，并在步骤480进一步确定消费者对机器人是否有其他任务或功能指令。如果没有，在步骤485结束处理，但如果有还进一步的指令，过程返回至图4的步骤406。

简档更新

[0179] 现在参考图6，示出了描绘更新简档的方式的流程图。在步骤A505，消费者获得简档捕获产品，最终在步骤510消费者获得订阅账户并且如果使用订阅模型会因此得到发票。

[0180] 一旦消费者获得了简档捕获产品和订阅账户，在步骤A515消费者形成了他们的简档。在步骤A520一旦形成了简档，消费者登入他们的账户，并随后在步骤A525消费者可以上传他们的简档更新（或可替代地，简档可以自动地更新）。

[0181] 在一些实施例中，文件更新可以发送至主简档并如步骤A530所示添加到主简档中。随后，发布消费者更新的主简档。

[0182] 现在参考图7，示出了如何更新主简档的简短描述。在步骤419b，确定是否维护简档。如果否，在步骤419c通知用户需要更新他们的简档。在419d用户随后更新他们的简档，并且在步骤419e过程结束。如果正确地维护了简档，不需要进一步的步骤，并且在步骤419e过程结束。

条件或约束

[0183] 在前述部分中，参考图5a-5d描述了命令和控制结构的方法的不同示例。过程中的一个步骤是在机器人装置的操作上施加“条件或约束”。参考图7a，图中描述了示例性实施例，每一条路径由选择的流程图路线来定义。

[0184] 图7b可以符合以下宽泛处理步骤的类似结构：

(1) 生成；

(2) 评估（可选的）；

(3) 响应；以及

(4) 修改（可选的）。

[0185] 参考图7c和图7b，以下内容总结生成、评估和施加条件或约束的两个示例性过程。对于图7c中的场景1，在步骤D01，条件/约束生成器CC10生成条件或约束（包括任何元数据）。

[0186] 在步骤D02，该条件或约束（包括任何附加的信息或元数据）传送至远程服务器CC11（或机器人注册器）。在步骤D03，远程服务器CC11接收并评估该条件或约束，然后生成评估判定。

[0187] 步骤D04，远程服务器CC11可以批准施加该条件或约束。在步骤D05，远程服务器

应。

[0166] 在步骤B006，结合命令和请求，如果结果或响应令人满意，然后管控芯片3将这种数据信息传达9至远程服务器2（例如通过机器人6的接收器/发送器模块10）以做进一步的或最终的评估和判定。换言之，管控芯片3可以预审查该命令或请求和/或机器人的结果或响应，即在与远程服务器2通信之前。

[0167] 这样做的优点包括降低了远程服务器2接收和处理外来的、冗余的或无目的的数据信息流的几率，例如管控芯片3可以用作'第一屏障'，拒绝不符合要求的或远程服务器2确定（很可能）未批准的任何命令或请求（这可以结合机器人的结果或响应）。

[0168] 在步骤A007，远程服务器2接收并评估命令或请求和/或结果或响应，然后生成评估判定。在步骤A008，如果确定批准命令或请求，那么远程服务器2将命令或请求传送9至机器人6的接收器/发送器模块10。

[0169] 接收器/发送器模块10将命令或请求传输至于机器人6的管控芯片3。在步骤A009，管控芯片3促进将命令或请求传送至机器人6的输出5，这等同于命令或请求由机器人6实现。注意，如场景1所描述的，场景2的过程还可以包括与场景1的步骤4至7相同或相似的步骤，例如，在批准命令或请求之前，远程服务器2可以指定进一步的机器人查询或测试。

[0170] 现在参考图5d，示出了命令和控制状态的另一个示例。在步骤C001，外部命令或请求生成器1（或者是内部命令或请求生成器7）生成命令或请求。

[0171] 在步骤C002，将命令或请求传送12（或传输11）至机器人6的输入模块4。机器人6的输入模块4将命令或请求传输至机器人6的管控'芯片'3。

[0172] 在步骤B003，机器人6的管控芯片3评估该命令或请求，然后生成评估判定。在步骤C004和C005，如果该判定是有条件地批准该命令或请求（受限于未解决的评估要求的结果或响应的批准），那么管控芯片3促进和/或监督机器人测试或查询以建立所述结果或响应。

[0173] 在步骤C006，此处的过程可以不同于场景2，不同之处在于管控芯片3可以确定不与远程服务器2进行通信（例如，机器人6可以'超出范围'，处于无线信号拒绝环境中，或者并不'永久'在线），因此管控芯片3评估到它的能力和/或编程命令或请求和/或结果或响应的最佳水平（例如，它可以扮演远程服务器2执行的相同或相似的角色）。

[0174] 在一个实施例中，管控芯片3可以偶尔与远程服务器2进行通信9，例如通过机器人6的接收器/发送器模块10，并且在这样做时可以促进机器人的管控芯片服务订阅（或许可密钥）的恢复和/或相关软件、补丁或快报的更新，例如机器人6将要服从或遵守的最新订单和/或协议。

[0175] 在一个进一步的实施例中，如果机器人6的管控芯片3可以在指定的时间段内或就当前提议的命令或请求不与远程服务器进行通信，机器人6的管控芯片3可以使全部或部分命令或请求不得到批准—基本上限制或约束机器人6或防止它操作。

[0176] 限制或约束的示例包括命令或请求被'围绕[此]位置行进、拍摄监视录像'；然而，由于机器人在指定的时段内不与远程服务器通信，减少或限制了命令或请求，例如如下情况：机器人只被允许在其'大本营(home base)'（或注册地址）的指定半径范围内行进或者不允许在公共空间内行进。

CC11 将该条件或约束传送至于机器人 CC12 的一个或多个‘管控芯片’。在步骤 D06，机器人的 CC12 的管控芯片促进施加条件或约束。

[0188] 在步骤 D07，出于一个或多个原因，可以修改或撤销该条件或约束，例如条件 / 约束生成器 CC10 可以不再要求该条件或约束是活跃的，因此可以取消它。

[0189] 对于图 7c 中的场景 2，在步骤 E01，条件 / 约束生成器 CC20 生成条件或约束（包括任何元数据）。在步骤 E02，将该条件或约束传送至机器人 CC22 的一个或多个管控芯片上。在步骤 E03，机器人的 CC22 接收并促进评估该条件或约束，然后生成评估判定。在步骤 E04，管控芯片可以批准该条件或约束。在步骤 D05，管控芯片促进施加该条件或约束。在步骤 E06，可以修改或撤销该条件或约束。

隐私问题和模糊

[0190] 图 8 至图 11 展示了服务器 300 所使用的技术的一些示例，这些技术用于防止用户由于未经注册或者用户未经许可在特定空间内或附近操作或运行以从任何装置、机器或机器人捕获、查看或记录监视数据。然而，例如机器人仍然可以能够使用照相机或其他监视功能进行导航或用于其他目的，但它们的用户将不被批准或不能访问、查看或记录这些镜头或数据。

[0191] 隐私约束可以采用软件代码下载到机器人上的形式，然后机器人可以自我管理它的导航移动。在一个实施例中，机器人的导航系统可以在其‘内部’地图上具有‘封锁’或‘禁行’区域。可以不时地添加、删减或修改这些禁行区域。兼容的导航软件代码可以使用或多维（地理）坐标系统 / 技术或以此为特色。例如，通知机器人的系统避免或不要在某些区域内行进。

[0192] 例如，未注册的机器人通常不会接收到许可码，但它们可以接收隐私约束。尽管没有注册，但能够接收这些约束，这可能是由于机器人制造商支持‘隐私协议标准’，因而，默认地设计机器人自动接收这些相关信息—不论采用什么形式，都可以将它们转发至机器人（从注册器或另一方）—不论用户是否知道这些接收内容。

[0193] 在替代示例中，注册的机器人可以接收许可码；但是不接收任何隐私约束。这样做的一个原因可能是因为消费者所指令的任务或功能不会或将来也不会使机器人在禁区（可以与注册或另一方一起注册的区域）之中、之上或附近冒险。

[0194] 更详细地，促进禁区的步骤（例如，调整行进路径或计划）：

(1) 接收条件或约束位置数据信息（例如，由机器人或由远程服务器）；

(2) 在意图执行或批准之前，查询机器人的行进计划或路径，以避免与接收到的条件或约束位置数据信息冲突；

(3) 如果存在冲突，调整计划或路径以避免与条件或约束位置数据信息定义的空间（或该空间内的主体）（的冲突）。

[0195] 促进覆盖或模糊的宽泛步骤（例如，修改监视数据和管控公开）有：

(1) 接收条件或约束位置数据信息（例如，由机器人或由远程服务器）；

(2) 在意图执行或批准之前（包括传输监视数据以便在非缓冲 / 易失性存储器中查看和 / 或存储；或数据信息的公开，例如主体‘加标签’），查询机器人传感器的捕获领域以避免与接收到的条件或约束位置数据信息冲突；

(3) 如果存在冲突，对机器人传感器的捕获领域施加条件或进行约束（例如，扩大），例

如通过阻挡传感器数据馈送或通过模糊、删除、涂黑或遮白与接收到的条件或约束数据信息相一致的捕获领域。在一个实施例中，类似于在增强现实环境中创建 3D 模型，这种覆盖机制可被促进，即当识别场景中的简档时，实际上用‘空白’形状替代该简档，从而遮挡该简档。

[0196] 条件或约束位置数据信息由机器人和 / 或远程服务器以如下方式接收：

■参考图 7c 所示的场景 1（或 2），对于预先定义的位置数据信息（例如，固定的坐标 + 海拔），远程服务器（或机器人的管控芯片）通常提前接收所生成的条件或约束，例如 D03（或 E03）。

■对于实时的位置数据信息（例如，并置的定位模块），机器人可以接收广播装置的传输。

■对于实时的简档识别：机器人可以捕获简档，在本地识别它（例如，通过管控芯片），然后确定是否对该简档施加了条件或约束。在另一个实施例中，机器人捕获简档，然后将捕获的数据信息传送至远程服务器以进行处理（即，识别或查询）；如果该简档被施加了条件或受到约束，那么可以发布经管控的响应或不响应。

[0197] 可以促进禁区的系统、方法、计算机程序、数据信号和设备包括为机载防撞系统配置的那些技术。示例（非限制性），包括：

(1) 交通警告和防撞系统 (TCAS)

；

(2) 便携式防撞系统 (PCAS)

；

(3)FLARM；

(4) 地形感知和告警系统 (TAWS)

；

(5) 障碍物防撞系统 (OCAS)

简档识别

[0198] 通过简档而不是并置的定位模块或固定的坐标 + 海拔来促进禁区的主要不同之处包括以简档识别技术替代位置发布传输装置和信号并在该识别的简档周围生成规定的禁区来，这可以在机器人的地理信息系统 (GIS)、导航和路径规划系统得到促进。

[0199] 现在返回到图 8，示出了展示很多客户端、用户装置和机器人的图。客户端 111 选择隐私约束，该隐私约束通过通信网络 60 并经由服务器 100a 传送至多个机器人 210a、210b 和 210n。系统对该隐私约束进行过滤，这样使得只有是网络中的参与者的机器人接收该隐私约束。如图可见，未参与的机器人 210c 无法接收施加的隐私约束。

[0200] 类似地，是非参与者的用户装置 110b 无法接收施加的隐私约束。然而，用户装置 110a 和 110n 的确可以接收隐私约束。

[0201] 现在参考图 9，示出了在实际中禁止、覆盖或模糊如何操作的示例。注册器可以利用它的资源禁止机器人行进（或穿过）的空间，基本上是通过例如规定机器人服从的‘禁行’或‘禁飞’区。另外，通过不允许在这些禁区内或附近无妨碍地操作，还可以管控其他装置或机器。可以关闭或减少这些装置或机器的功能。

[0202] 在一个实施例中，注册器的服务器实现禁区，并且所有机器人必须相应地调整它

们的后续行进计划和轨迹。

[0203] 这可由用于机器人的软件应用实现，该软件应用防止任何（机载）设备（例如照相机）在面对或遇到覆盖区域时监视操作，以保护例如公众隐私。

[0204] 更为详细的，在解释图 9 的过程流程之前，将要理解的是，当参与的机器人或装置捕获了注册的简档（不限于有形对象，例如人）时，在处理时所捕获的数据将提示它是注册的隐私，然后该主体立即被覆盖（例如，模糊化）。简档可以在参与的机器人或装置上本地存储和处理（减少滞后或延迟时间），或在例如注册器的云服务器上远程地存储和处理。在非注册装置或机器人上不存储这类数据将是首选的，以便安全地维护（客户端的）敏感的简档数据。

[0205] 在另一个实施例中，选择的简档数据在用户的装置或机器人上本地存储（并处理）。例如，注册器可以将出现在这些参与机器人和装置附近的注册客户（订阅者）的简档数据传输至参与的机器人和装置。所以，如果他们将遇到彼此（即进入到捕获视野中），那么这些隐私措施可以生效。然后，一旦参与的机器人或装置离开注册的客户端，就将该客户端的简档数据从那些的机器人和装置中移除。此实施例通过本地存储和处理将帮助缓解潜在的问题，并稍微解决本地存储和处理其他敏感的简档数据而不是由注册器的服务器进行的问题。

[0206] 简档数据以任何数量的方式存储、处理和过滤（结合数据库查询）。例如，最终用户的装置或机器人可以在本地存储所有数据库简档的备份（并接收相关的更新）；并且装置或机器人还可以随后处理并过滤这些查询。

[0207] 在本发明的一个实施例中，可以向商业呈现地图（至少是一维的），然而优选的是三维映射计算机程序，就像以下产品中的一个或多个：Bing 3D Maps；Placebase；Google Tour Guide或Maps GL、3D Maps Mobile；亚马逊的UpNext应用；Whereis 3D City Model；Uniden TRAX 5000；Aviation Mapper；Nokia 3D Maps（例如 Ovi）等。

[0208] 商业将得到在地图区域或空间上进行选择的机会（通过指引鼠标光标或相同功能的可操作指示器），可能通过在屏幕上拖拽光标或指示器或不时地使用姿态控制、语音命令或可能是或成为可应用方法的其他有效动作。

[0209] 覆盖的一个示例是居民希望覆盖他们的公寓窗户和阳台以免机器人监视（可能是空中机器人装置），他会访问系统、定位他们财产的窗户和阳台、在这些区域或空间上拖拽光标以便覆盖（它们可以在屏幕上以尺寸变化的长方形或矩形柱体来图示）、确认选择、输入并接受支付条款、确认交易、在规定的时间帧使覆盖有效。

[0210] 只有可应用的或可允许的区域可供商业的选择。例如，团体可能没有可用于选择他们并未控制、并不拥有或在土地契约上并未指定的空间的选择权。如果一方选择禁区（即为了防止其他机器人在该空间内或在该区域上行进）并且该区域不是与该方合法关联的空间，例如由于其他失去联系方施加的禁止阻止与同该空间合法关联的一方相关联的机器人，那么可以批准这些机器人来重写这些施加。[需要解释下对抗方，即取消关联方，他可以试图防止其他方的机器人在特定空间中坦然地访问或行进。]

[0211] 现在参考图 9，在步骤 1，具有监视的增强现实装置或机器人捕获数据，在步骤 2 该数据可以是图像或语音数据。在步骤 3，捕获的数据通过通信网络 60a 传输至远程服务器以进行处理。在步骤 5，捕获的数据由至少一个服务器接收，例如服务器 300a，并且存储数据

并与隐私约束相比较。在步骤6，通过通信网络上传数据。在步骤7，处理的数据传输至机器人或装置，从而使得在步骤8机器人或装置可以采取适当的动作。

[0212] 现在参考图9a，图中描述了如何创建禁区的示例（例如，城镇中的特定区域或街区如何被指定为机器人的非操作区域）。

[0213] 远程服务器（机器人注册器）负责确保更新和维护所有的禁区数据。该数据来自不同的数据源，例如公共航空部门、国防部、LEO组织、公司和个人。禁区（例如'禁飞区'）由包含以下内容的各种元数据组成：

■地理位置数据，该数据定义了映射到地表的三维体积；

■条件或约束就位的时间；

■条件或约束就位的日期；

■禁区应用的规范。例如，机器人超出某个尺寸/速度能力；

■条件或约束的解释；以及

■请求条件或约束的本体/个人。

[0214] 远程服务器允许数据通过安全web形式或通过自动应用程序设计接口提交，在远程服务器web形式接口中，个人可以利用若干方式输入数据。数据以一系列GPS位置的形式输入，以创建闭合环路，或者可以显示地图，以允许个人在地图上绘制该闭合环路。一旦提交，远程服务器就验证地理数据并批准它，以便提交至禁区数据库。附加的屏幕允许如远程服务器工作人员要求的那样对这种数据进行编辑和配置。可替代地，一旦提交，远程服务器的自动评估程序可以确定适合性以进行批准。

[0215] 为了创建精确的三维体积，所有的数据都是基于GPS的，包括海拔数据。默认的高度可以应用于该区域。

[0216] 用户可以使用任何工具创建形成环路的一组有效GPS坐标，或者可替代地他们可以使用远程服务器（机器人注册器）提供的在线映射接口。

[0217] 在线映射接口的一个示例是谷歌地图开发者API。可以在此找到与性能有关的具体信息。

[0218] 用户或服务提供商向远程服务器发送意图请求，该意图请求包含目标着陆点的GPS定位。这种数据以兼容JSON格式呈现并满足远程服务器API要求或被拒绝。典型的请求类似如下：

{

```
"recipient": "Mr Craig Smith"
"address": [
    {"address1": "1 Joth st"}
    {"address2": "Craig's farmt"}
    ],
"geo":{
    "lat": "-32.118056"
    "long": "141.923447"
},
"payload":{
    "lot": "of date"
}
}
```


[0219] 远程服务器处理该请求以标识它是否存在于该远程服务器自身的已知禁区数据库中。

[0220] 如果目的地位于禁区内，发送拒绝并提供替代方案（例如最近的可能安全点或选项）以便放弃该请求。如果批准了目的地，那么发送确认以批准该请求。

[0221] 进一步参考图 10 描述该过程。图 10 展示了过程流程，其中在步骤 505 客户希望申请禁区、覆盖或模糊服务。在步骤 510，如果不存在，客户创建注册账户，并在步骤 515 该客户登录他们的账户。在步骤 520，为客户提供该选项或建议的禁区、覆盖和 / 或模糊选项，可以通过在地图上选择客户希望的区域来促进这个处理，以便覆盖客户希望的设置为禁区的区域。

[0222] 在步骤 525，客户确认他们的选择和任何必要的支付。在步骤 530 注册器接收客户的申请，在步骤 535 注册器审核该申请并与第三方协商（如果相关的话）。

[0223] 在步骤 540，注册器可以对客户的申请进行批准、拒绝或提出修改，在步骤 545 一旦所有相关方接受了该申请，就为客户开出发票并结束申请。

[0224] 在步骤 550，当收到支付时，注册器采取必要的动作来更新数据库以排除、覆盖或模糊该区域、装置、机器或机器人。

[0225] 装置、机器或机器人得到通知并开始遵守更新的隐私约束。

[0226] 在非常具有选择性的情况中，可以获得豁免权以允许机器人和参与的装置不受‘隐私协议”的约束。在一个实施例中，对已批准的父母（运行批准的专用 app），可以免除‘禁区’、‘覆盖（固定的）’和‘简档覆盖（移动的）’，这样父母可以监控他们的孩子，例如：

(i) 父母向注册器申请豁免权；

(ii) 可选的：父母向注册器提供他们孩子的简档；

(iii) 父母被授予的豁免权。

[0227] 本发明的另一个方面是最终限制不受妨碍的操作或功能（例如监视）机会。

[0228] 将要理解的是，可以为用户提供时间有限的照相机查看（可能是在特定类别的禁区中行进时）。在允许的时间到期之后，例如允许用户获得另一个定时查看之前可以申请延期。

[0229] 转到图 11，更为详细地描述隐私约束的过程流程。在步骤 565，用户登录到他们的账户，并且在步骤 570 用户向装置、机器或机器人发起任务或功能指令。在步骤 575，装置、机器或机器人指令转发给注册器并因此在步骤 580 注册器可以处理和管控任何指令。

[0230] 在步骤 585，注册器可以向装置、机器或机器人转发许可码和相关的隐私约束（如果有的话），并且在步骤 590，用户的装置、机器或机器人执行任务或功能并遵守任何隐私约束。

[0231] 将要理解的是，在其他实施例中，如箭头 2、3 和 4 总体上所指示的，过程流程上的变化是可能的。例如，根据过程流程 2，当用户发起任务或功能指令时，在步骤 570 相关的隐私约束可以直接转发至用户的装置、机器或机器人，在步骤 584 机器人随后执行该任务或功能，并在步骤 590 遵守任何隐私约束。

[0232] 替代实施例也是可以设想的，在这些实施例中不需要用户登录到他们的账户或发起任务或功能。总体上如过程流程 3 和 4 所示，隐私约束可以转发至用户的装置、机器或机器人。然后这些隐私约束可以用于执行步骤 590 所示的功能或可以简单地添加到机器人的信息门，以备后用。总体上由过程流程 3 和 4 所示的过程流程可用在指令直接发布给机器人且不通过注册器发送的实施例中。

[0233] 参考图 11a 至图 11k，披露了若干计算机实现的过程，通过这些过程，可以运行监管过程。图 11a 描述了用于监管的宽泛过程。以下简要描述过程步骤。

宽泛过程步骤（监管）

1. 生成

生成监管倡议

首先，通过使用 'rotometrics' 生成模板（即，在机器人进行认证时进行数据采集）。优选地进行测试以检测非法物资或对象（例如，化学的、分子的或有形的签名）的存在，例如武器或危险装置。此后，生成'冰雹'信号（例如标识请求）。第三，生成'场景屏幕'（例如，搜索或标识非参与者或'流氓'机器人）。该步骤在图 14、图 15 和图 16 中更为详细地解释。

2. 评估（可选的）

测试登记的模板以查看它是否匹配最新捕获的样本。例如，如果针对非法或未批准的物资或对象或反常的或不可接受的机器人测度，一个样本匹配了登记的模板，那么这会生成强制执行触发事件。

在另一个示例中，如果一个样本匹配了一个登记的正常或可接受机器人测度，那么这不会生成强制执行触发事件。

在又一个示例中，如果一个样本不匹配一个登记的正常或可接受机器人测度，即超出

容限或超出阈值，那么这会生成强制执行触发事件。

其次，是否接收到满意的回复响应？如果没有满意的回复，强制执行触发事件发生。触发事件可以包括机器人未注册、机器人具有未批准的操作、或操作上毫无价值（例如，错误）的事实。

第三，是否外来的机器人位于场景中？例如，没有外来的信号导致强制执行触发事件。

3. 响应

利用强制执行和 / 或通知做出的响应

被动强制执行策略可以包括：

■逮捕机器人（例如，生成性能 / 功能 / 能力条件 / 约束，例如不进一步操作、保留在约定的位置 / 地点）；或

■启动监控机器人，追踪 / 跟踪 / 跟随（例如，以促进定位并逮捕用户）。

主动强制执行策略可以包括：

■启动监控机器人，与主体机器人约定或在其附近，抓获（例如捕获或捕捉）；或

■启动监控机器人，与主体机器人约定或在其附近，使其失去能力 / 消除其伤害能力（例如，干扰机、诈骗机、EMP 或射弹）；以及

■通知相关的利益相关方。

4. 修改（可选的）

修改或撤销强制执行可以包括取消强制执行追赶（例如，‘放弃追逐’）、召集强制执行（例如，更多的监控机器人来协助）和 / 或恢复为强制执行（例如，触发事件）。

宽泛处理步骤（条件）

1. 生成

生成条件 / 约束可以包括生成性能 / 功能 / 能力约束（例如，管理规程可以规定由于许可类别、不足的支撑基础设施、网络或系统、紧急供应触发事件生成的约束和 / 或强制执行触发事件生成约束）。

生成的禁区条件可以包括：

■并置的定位模块或传输（固定的或移动的）（实时的或‘空间教学’）；

■简档捕获（固定的或移动的）（上传模板或 PA/eL 简档）；

■坐标 + 海拔（固定的）；和 / 或

■‘禁飞区域’或不操作区域（全部或部分）；

生成的覆盖条件可以包括：

■‘不关注’或不监视；

■并置的定位模块或传输（固定的或移动的）（实时的或‘空间教学’）；

■简档捕获（固定的或移动的）（上传模板或 PA/eL 简档）；和 / 或

■自动地识别窗户；类似于在 Google 街景上使脸部模糊。

生成的模糊条件可以包括：

■‘没有 ID’或没有屏上的或 HUD ‘加标签’；

■并置的定位模块或传输（固定的或移动的）（实时的或‘空间教学’）；

■简档捕获（固定的或移动的）（上传模板或 PA/eL 简档）；和 / 或

■坐标 + 海拔（固定的）；

生成的条件 / 约束免除权或豁免权可以包括：

■注册到该地址 / 位置 / 地点的注册方；

■父母希望监督他们的孩子；

■特殊许可（研究目的、政府等）

■利益相关者提供操作批准（例如为了提取 / 递送、农业监测等）；和 / 或

■‘条件’和‘约束’通常可以交换地使用。

2. 评估（可选的）

评估生成的条件 / 约束可以包括检测：

■约束是否与其他约束一致？

■禁区是否适合？

■覆盖是否适合？

■模糊是否适合？

■免除权或豁免权是否适合？

3. 响应

通过施加条件 / 约束生成响应可以包括确定：

■约束的性能 / 功能 / 能力；

■施加的禁区参数；

■施加的覆盖条件；

■施加的模糊条件；和 / 或

■施加的免除权或豁免权。

[0234] 参考图 12 和图 13，可以提供允许机器人通过感测 / 扫描协议进行初始检测并随后利用占用协议来占用的机制。

[0235] 现在参考图 12，示出了如果发起了感测 / 扫描协议该过程发生的过程流程。感测 / 扫描协议可以作为机器人执行功能的结果而发起，该功能例如通常图 11 所示的功能过程流程，或在步骤 605 感测 / 扫描协议可以独立于任何用户对机器人的指示而发起。

[0236] 在步骤 608 或 610，用户的机器人意识到需要感测 / 扫描操作的情况。

[0237] 如果实现正结果，在步骤 615 可以发起占用协议。如果在步骤 617 发起了占用协议，那么在步骤 630 结束感测 / 扫描的过程。如果没有发起占用协议，那么在步骤 620 用户的机器人正常行进，并且在步骤 630 结束该过程之前，在步骤 625 用户的机器人可以完成用户的任务或功能，或可替代地在步骤 623 用户的机器人可以返回到感测 / 扫描协议发起前的位置。

[0238] 现在参考图 13，示出了占用协议的过程流程，例如图 12 中提及的占用协议。在步骤 555 或 705，占用协议的发起是由于独立的请求或由于图 12 所示的感测 / 扫描操作。在步骤 708 这可以导致用户机器人行进至指定的占用位置或在步骤 710 用户的机器人偏离行进计划以执行占用协议。一旦已经执行了占用，在步骤 715 该过程结束。

[0239] 一种允许注册器监控机器人的环境的系统，这些机器人可能是未注册的、非法的、对公众危险的、入侵人们隐私的或不当操作的，甚至可能偷窃。因此，这些机器人将被称为‘流氓机器人’。

[0240] 注册器的系统利用它的监测、控制和管理能力（不限于它可能监视大量各种不同

的机器人的行进路径和轨迹的事实)—在一个实施例中,可能赋予它特定的能力或机会来针对流氓机器人监控环境。

[0241] 在另一个实施例中,通过利用在特定空间中或附近操作的非注册机器人(例如,消费者的机器人),注册器可以'发现'流氓机器人。优选地,消费者的机器人可以将环境数据反馈到注册器或在本地处理环境,然后将结果发送至注册器。在任一方法中,注册器可以使用消费者机器人的机载传感器和扫描器,可能通过消费者的机器人的'防碰撞和避障'检测器或模块来专门针对流氓机器人(即不应当遇到的机器人)监控它们的行进环境。

[0242] 这种利用消费者机器人帮助的主动性还允许跟踪最初检测的流氓机器人。在一个实施例中,由于每个消费者机器人都检测特定流氓机器人的存在或签名,检测流氓机器人的每个对应的消费者机器人的当前位置和/或每个消费者机器人所检测的流氓机器人的位置可以允许轨迹描绘(并且这种轨迹描绘可以是多维的)。

[0243] 然而,优选地还可以将模糊用于有形物体上,该有形物体通过其他手段识别,也就是说不通过简档识别方法。例如,如果有形物体位于已禁止的区域内(有可能通过客户在3D地图上选择它)或如果它与定位模块装置(例如具有地理位置特征的智能手机)相关联(例如,并置),可以不标识或标记该有形物体。

[0244] 换言之,在第一实例中,注册器的系统可以"认出"或标识特定环境中的所有机器人,然后从其电子视野中将注册的或已知的发布许可码后正在操作的所有机器人清除(即,移除不是流氓的机器人)。因此,如果在这种清除过程后仍有一些剩余的机器人,可以认为剩余的机器人是"另类的(off the grid)"或流氓操作者。

[0245] 另外,注册器可以利用各种方法进行这种调查。在一个方法中,注册器配置它自己的至少一个机器人来跟踪流氓机器人到它的目的地(有希望到达用户所在的位置),或者可能利用很多方法(例如,一个理想的实施例可以是重写或"欺骗"它的通信系统以破坏注册器的"占用协议")(安全地)使流氓机器人解除激活。

[0246] 随时间推移,注册器为各种机器人建立了签名(不限于声音)库或清单,这些签名可以分配给特定的机器人类型。

[0247] 参考图14,示出了二维环境的示例,所有检测到的机器人由注册器的系统形象地标识。

[0248] 参考图15,示出了二维环境的示例,所有注册的或非流氓机器人都从视野中清除了(选择性地移除),以便显示任何剩余的(流氓)机器人。

[0249] 机器人735和740仍保留在视野中。这些机器人被认为是未注册的。进一步地,已经列出具有无法识别的签名(以它的唯一符号表示)的流氓机器人740。而735被检测为具有熟悉的签名,根据注册器的数据库分析,它被列为'同心圆'类型的机器人。

[0250] 参考图16,示出了示例情况,该情况是街景,出现了各种参与者803、805、807、809、811、813、817、819、821、823和825以及非参与者801和815。

[0251] 参与者可以充当检测器节点和/或(移动的)中继站—分别促进检测非参与者和协助转发任何警告通知或其他相关数据至其他参与者。动作的机制可以类似于(信号)传播。[图中,'R'可以等同于'注册的'状态。]

[0252] 在第一实例中,803捕获大于非参与装置、机器或机器人801的部分匹配。该匹配百分比值被认为十分重要,足以保证(间接)直接传输警告至于附近的参与者805和807,

这两个参与者都位于警告半径范围内。

[0253] 在另一个示例中，多个参与者 809、811 和 813 只捕获非参与装置、机器或机器人 815 的部分匹配。个别地，这些匹配可能不足以引起警告的发布，然而考虑到是多重的，这些匹配协同组成一个百分比值，该百分比值被认为十分重要，足以保证（间接）直接发送警告至于附近的参与者 819 和 817，这两个参与者都位于警告半径范围内；进一步地，类似地会警告原始的检测器 809、811 和 813，通知它们的部分匹配的确是相关的。

[0254] 同时，由于位于任何警告半径之外或远离任何非参与者，参与者 821、823 和 825 并未涉及以上示例的任何一个。

优点

[0255] 本文描述的示例和较宽泛发明的优点之一是本发明在任何给定时间为消费者（即机器人的所有者）卸除了从事机器人动作的所有职责的负担或控制。只要通过中央服务器系统对命令进行过滤或处理，则极大地降低了自主装置和机器人装置的非法的、邪恶的或意外的使用。

[0256] 或意外的使用。如果机器人在它们的活动（操作或功能）中不受限制，能够冒险进入特定的无障碍空间（利用或不利用来自用户的显示指令或控制），那么这会导致或引起争议问题—这些问题中的一些包括隐私、安全、保障、负债、技术和伦理问题。因此，系统提供了一种机制和框架，通过该机制和框架要求机器人和 / 或它们的控制者在允许操作之前获得相关许可，尤其是如果该操作将在公共空间中出现。

[0257] 而且，由于要求消费者注册并标识他们自己，在涉及他们的机器人使用的范围内，系统提供监测、控制或管理消费者的动作或活动的能力。这反映了社会在要求人们获得执照开车、驾驶飞机或拥有并使用枪支方面的一般兴趣。

[0258] 也就是说，在防止用户允许他们的机器人被未经批准的用户使用或防止让他们的机器人由未经批准的用户不知不觉地使用方面，存在公共利益。这样的机器人可能具有能力和功能来执行受限的（例如危险的）功能。首先且最重要的是，这些事件会带来安全问题，例如机器人（由父母拥有）由未成年的儿童使用，而该儿童并未被列为或批准为注册用户。

[0259] 因此，机器人和负责促进至关重要的机器人更新的自主系统提供商的责任很少。相反，不论机器人的原产地、国家或操作空间如何，所有更新都由本文描述的系统处理并从其发布。这减轻了机器人和自主系统提供商的法律责任。

[0260] 本文描述的实施例的优点是实施例由与机器人分离的装置或由远程服务器来实现：

(1) 机器人有可能与外部管理服务器更频繁的通信（例如，提供更加有保证的或跟高安全级别的第三方管理或监督）；

(2) 远程服务器有可能处理或促进远程诊断服务；以及

(3) 机器人更频繁地从远程服务器接收软件、更新和 / 或快报。

[0261] 用户和 / 或用户的‘智能’装置或机器人附件例如通过远程服务器间接或根本不与机器人通信的进一步的优点是不包括‘迷失东京 (lost in translation)’事件，因为远程服务器（机器人注册器）直接从数据源（即用户或用户的装置）接收建议的命令或操作请求。换言之，远程服务器充当用户（或他们的装置）和机器人之间的媒介。

免责声明

[0262] 在本说明书和以下权利要求书中，除非上下文另外要求，否则词语“包括(comprise)”和诸如“包括(comprises)”或“包括(comprising)”的变体将被理解为暗示包括一个规定的整数或步骤或一组整数或步骤，但不排除任何其他整数或步骤或其他组整数或步骤。

[0263] 本领域技术人员将认识到的是，除那些专门描述的变化和修改以外，可对本文描述的发明做出变化和修改。本发明包括所有这些变化和修改。本发明还包括单独地或全体地在说明书中提及或指明的所有的步骤、特征、公式和化合物以及任何和所有组合或者这些步骤或特征中任何两个或多个的。

[0264] 本文使用的所选术语的其他定义可以在本发明的详细描述中找到并全文使用。除非另外定义，否则本文所使用的所有其他科技和技术术语具有本发明所属领域的技术人员通常所理解的相同含义。

[0265] 尽管并未要求，但参考该方法、计算机程序、数据信号和该系统的一些方面描述的实施例可以通过供开发者使用以创建软件应用的应用程序接口(API)、应用开发包(ADK)或一系列程序库来实现，这些软件应用将在任何一个或多个计算平台或装置上使用，例如终端或个人计算机操作系统，或在便携式计算装置上使用，例如智能电话或平板计算系统操作系统，或在更大的服务器结构中使用，例如‘数据群’，或在更大的交易处理系统中使用。

[0266] 通常，因为程序模块包括执行或促进实现具体功能的性能的例程、程序、对象、组件和数据文件，将要理解的是软件应用的功能可以分布在很多例程、程序、对象或组件上以实现与实施例和本文要求保护的宽泛发明相同的功能。这些变化和修改在本领域技术人员的权限范围内。

[0267] 还将认识到，当本发明的方法和系统和/或实施例由计算系统实现或由计算系统部分实现时，则可以使用任何适当的计算系统架构。这包括独立计算机、网络计算机和专用计算装置(例如现场可编程门阵列)。

[0268] 当在说明书中使用术语“计算机”、“计算系统”和“计算装置”时，这些术语旨在涵盖用于实现本发明概念和/或本文描述的实施例的任何适当的计算机硬件设置。

[0269] 当在说明书中使用术语“机器人装置”、“自主装置”和“智能装置”时，但这些术语旨在涵盖任何适当的装置，该装置能够接收命令并使用该命令执行功能，该功能可以是“物理的”功能(即移动)或“虚拟的”功能(例如，通过电子命令与另一个装置交互)。

[0270] 当引用通信标准、方法和/或系统时，机器人或装置可以通过各种形式传输和接收数据：3G、4G(CDMA/GSM)、Wi-Fi、蓝牙、其他射频、光、声音、磁、GPS/GPRS、或任何其他形式或方法的通信，它们有时变得可以利用。

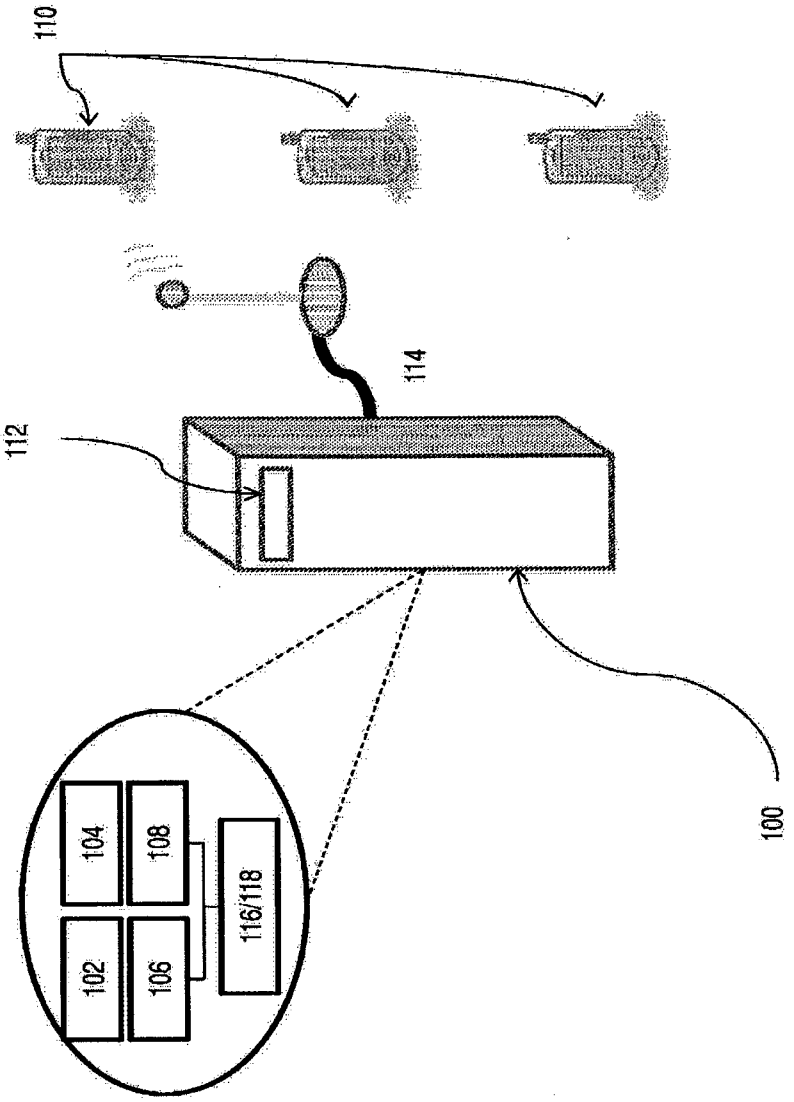


图 1

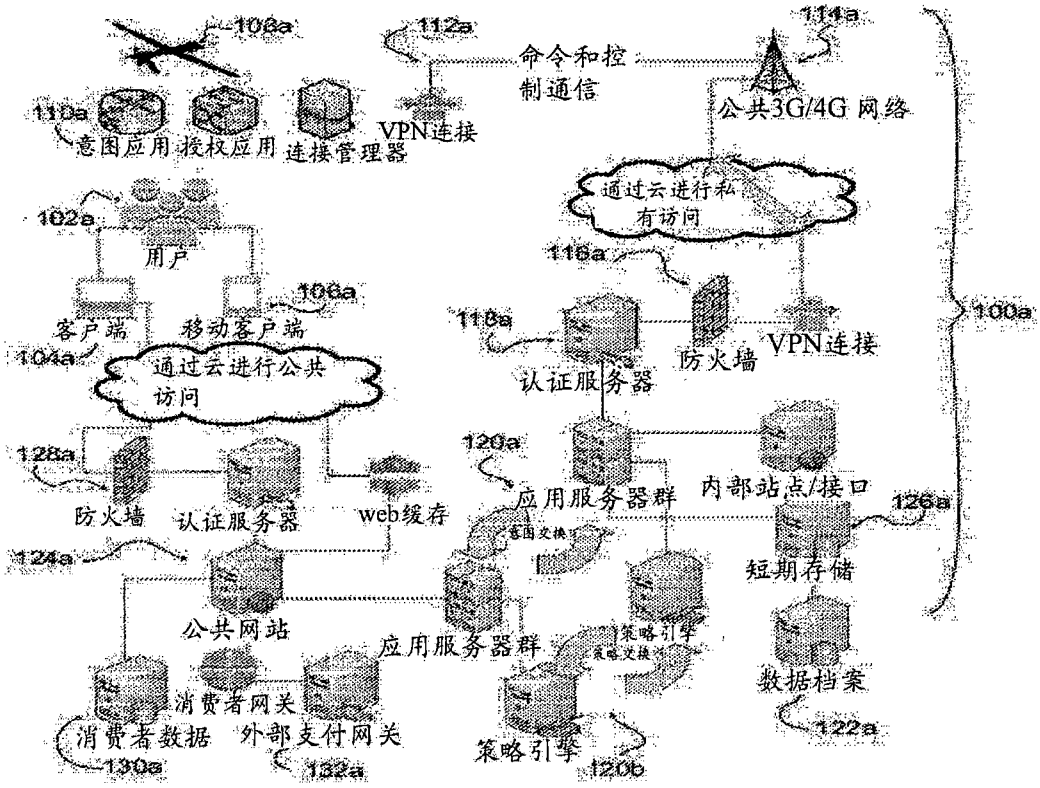

108a
112a
命令和控制通信
114a
公共3G/4G 网络
110a
意图应用
授权应用
连接管理器
VPN连接
通过云进行私有访问
102a
用户
116a
客户端
移动客户端
106a
100a
118a
104a
通过云进行公共访问
防火墙
VPN连接
认证服务器
128a
120a
应用服务器群
内部站点/接口
126a
防火墙
认证服务器
web缓存
负载均衡
124a
短期存储
公共网站
应用服务器群
策略引擎
策略实施
数据档案
消费者网关
外部支付网关
消费者数据
122a
130a
132a
策略引擎
120b

图 2

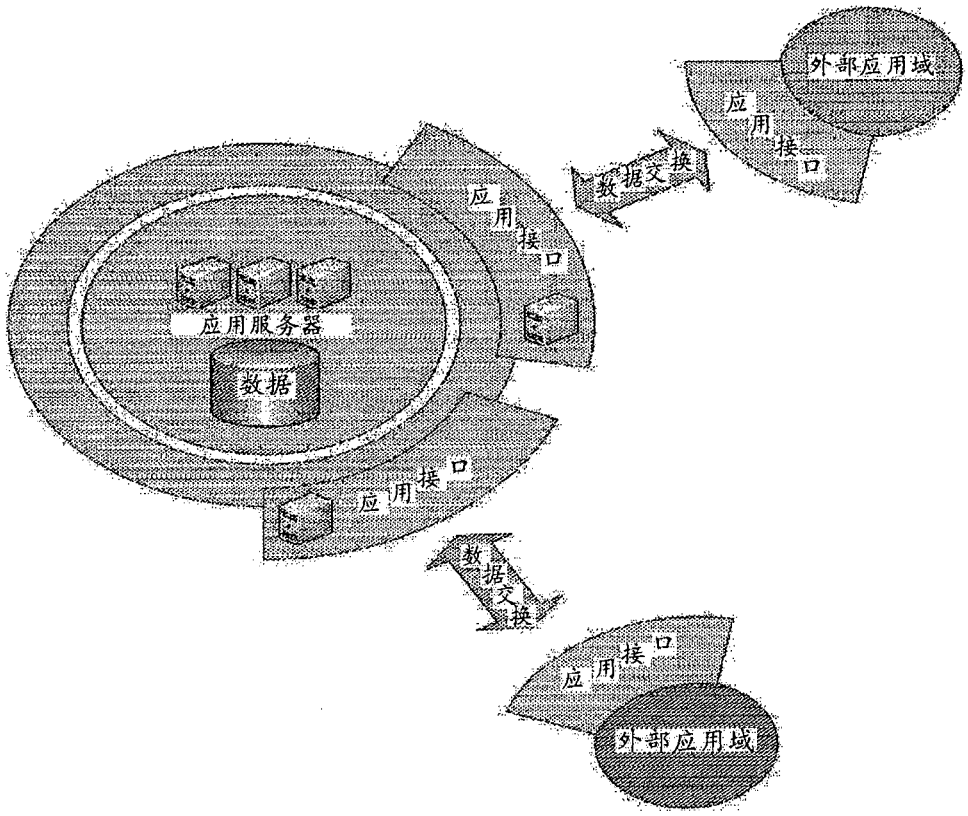


图 2a

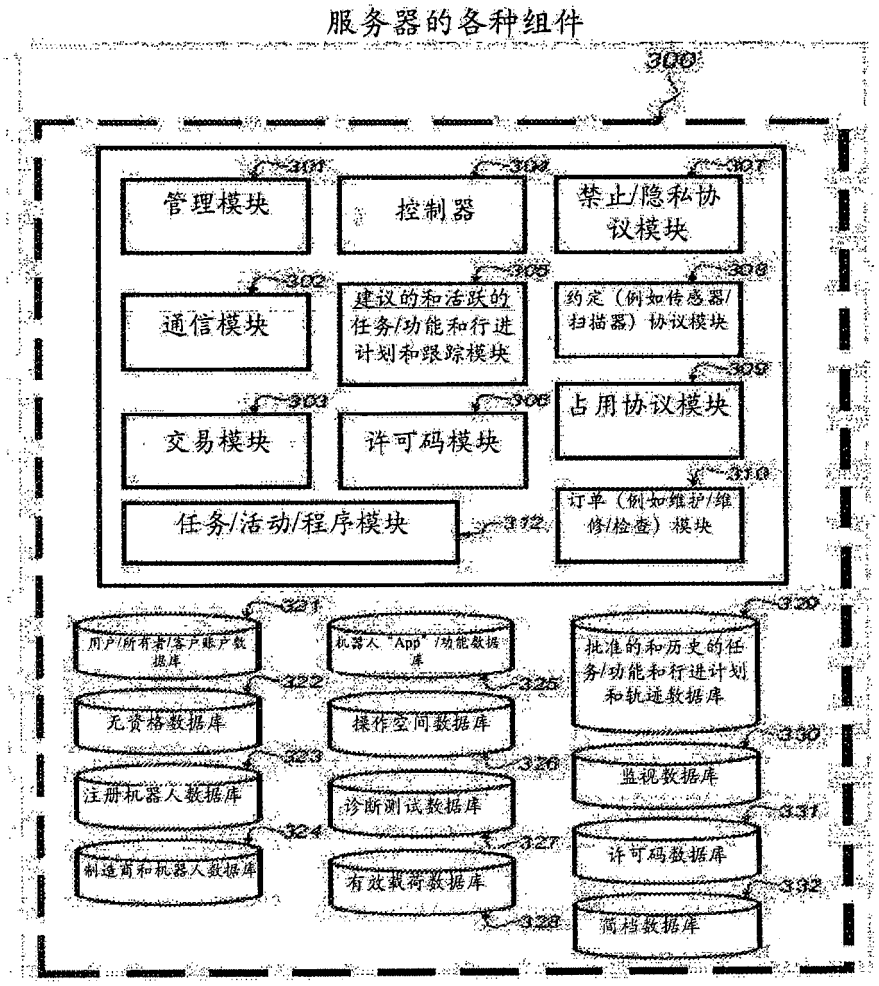

服务器的各种组件
300
301
管理模块
304
控制器
307
禁止/隐私协议模块
302
通信模块
308
建议的和活跃的任务/功能和行进计划和跟踪模块
306
约定（例如传感器/扫描器）协议模块
309
占用协议模块
303
交易模块
305
许可码模块
310
订单（例如维护/维修/检查）模块
312
任务/活动/程序模块
321
用户/所有者/客户账户数据库
322
无资格数据库
323
注册机器人数据库
324
制造商和机器人数据库
325
机器人"App"/功能数据库
326
操作空间数据库
327
诊断测试数据库
328
有效载荷数据库
329
批准的和历史的任务/功能和行进计划和轨迹数据库
330
监视数据库
331
许可码数据库
332
简档数据库

图 3

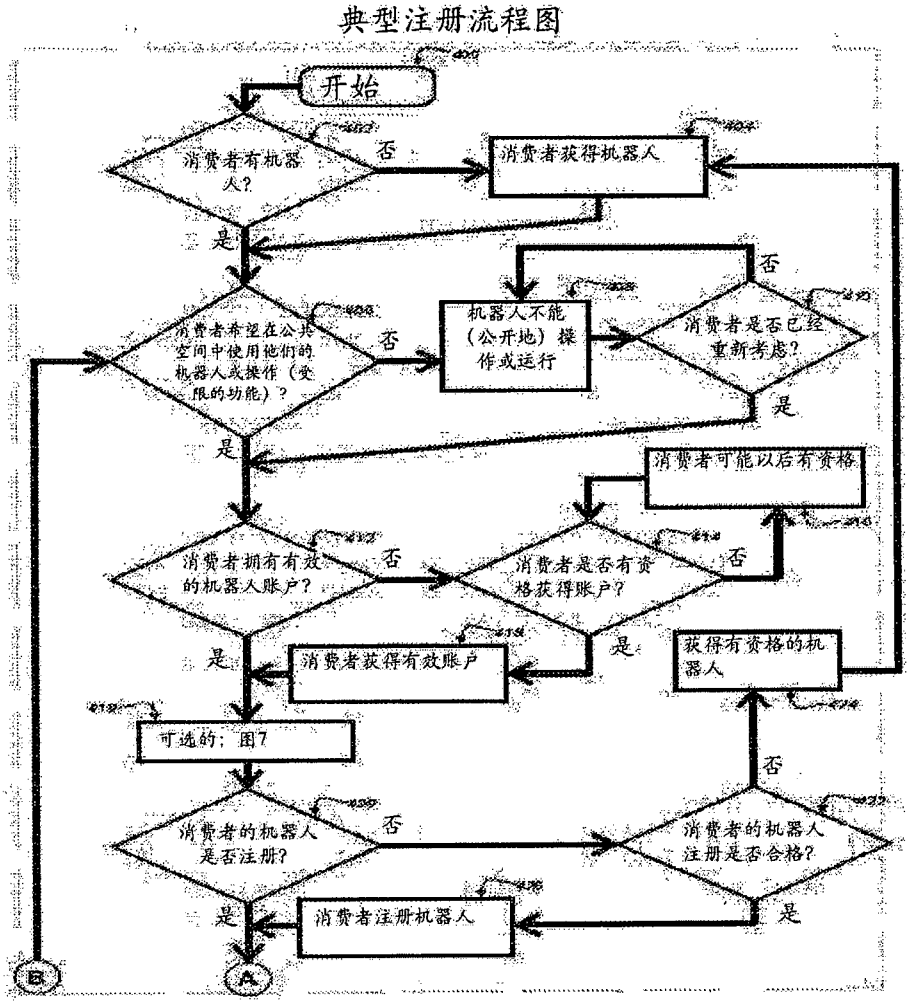

典型注册流程图
开始
消费者有机器人?
否
消费者获得机器人
是
消费者希望在公共空间中使用他们的机器人或操作(受限的功能)?
否
机器人不能(公开地)操作或运行
消费者是否已经重新考虑?
否
是
是
消费者可能以后有资格
消费者拥有有效的机器人账户?
否
消费者是否有资格获得账户?
否
是
是
消费者获得有效账户
获得有资格的机器人
可选的:图7
否
消费者的机器人是否注册?
否
消费者的机器人注册是否合格?
是
是
消费者注册机器人
B
A

图 4

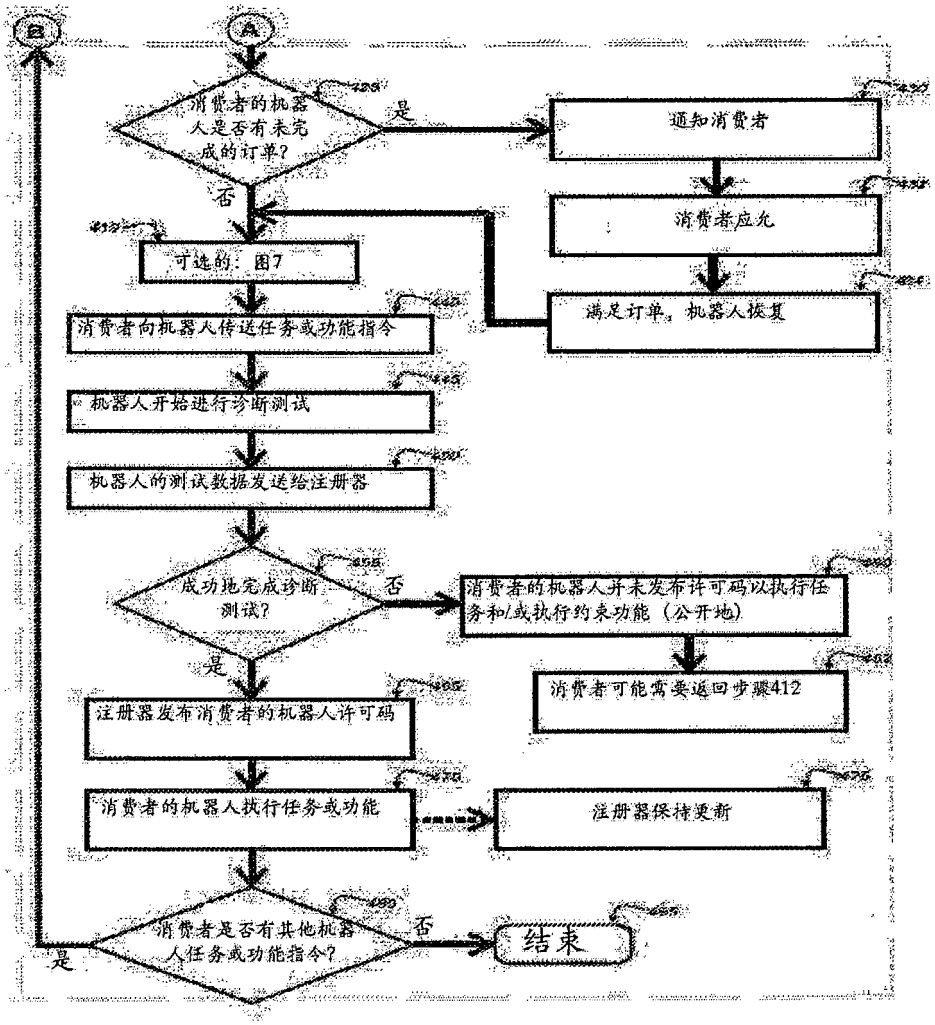


图 5

促进机器人命令或请求的场景

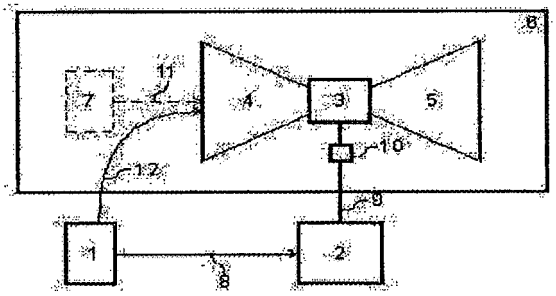


图 5a

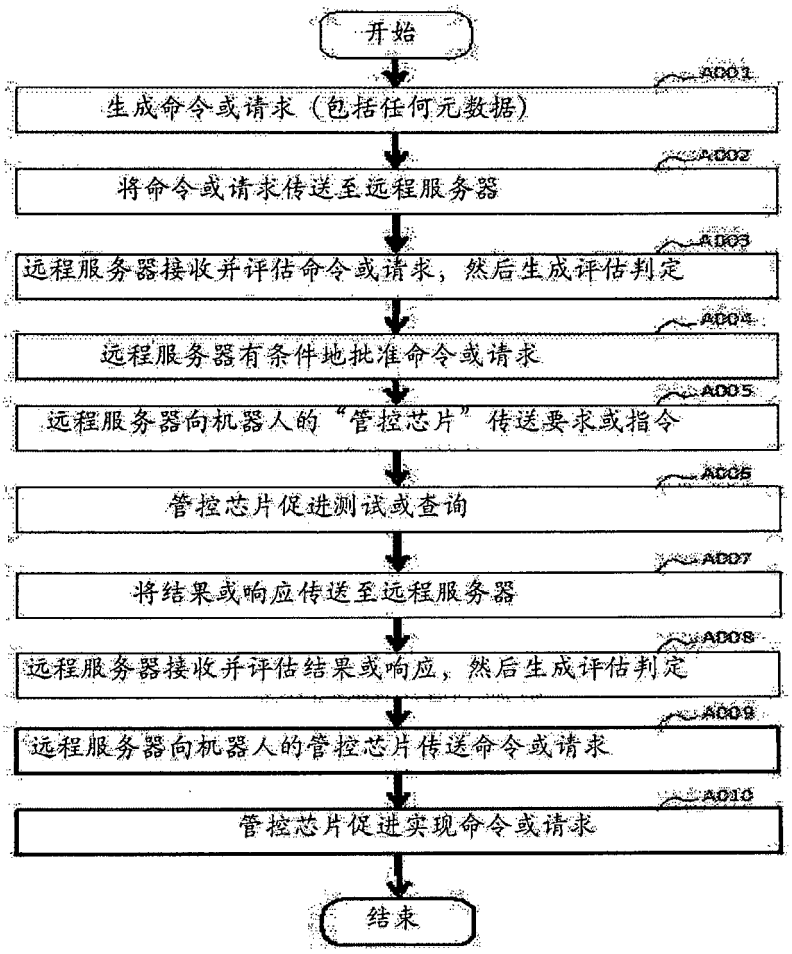

开始
A001
生成命令或请求（包括任何元数据）
A002
将命令或请求传送至远程服务器
A003
远程服务器接收并评估命令或请求，然后生成评估判定
A004
远程服务器有条件地批准命令或请求
A005
远程服务器向机器人的“管控芯片”传送要求或指令
A006
管控芯片促进测试或查询
A007
将结果或响应传送至远程服务器
A008
远程服务器接收并评估结果或响应，然后生成评估判定
A009
远程服务器向机器人的管控芯片传送命令或请求
A010
管控芯片促进实现命令或请求
结束

图 5b

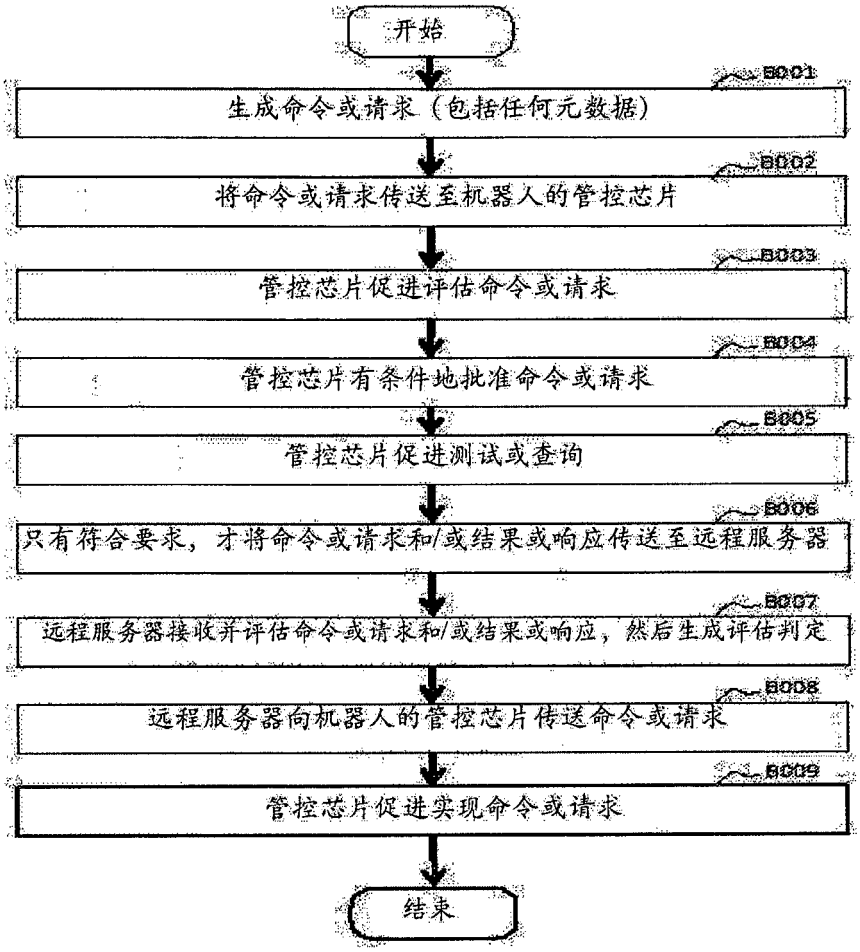

开始
S001
生成命令或请求（包括任何元数据）
S002
将命令或请求传送至机器人的管控芯片
S003
管控芯片促进评估命令或请求
S004
管控芯片有条件地批准命令或请求
S005
管控芯片促进测试或查询
S006
只有符合要求，才将命令或请求和/或结果或响应传送至远程服务器
S007
远程服务器接收并评估命令或请求和/或结果或响应，然后生成评估判定
S008
远程服务器向机器人的管控芯片传送命令或请求
S009
管控芯片促进实现命令或请求
结束

图 5c

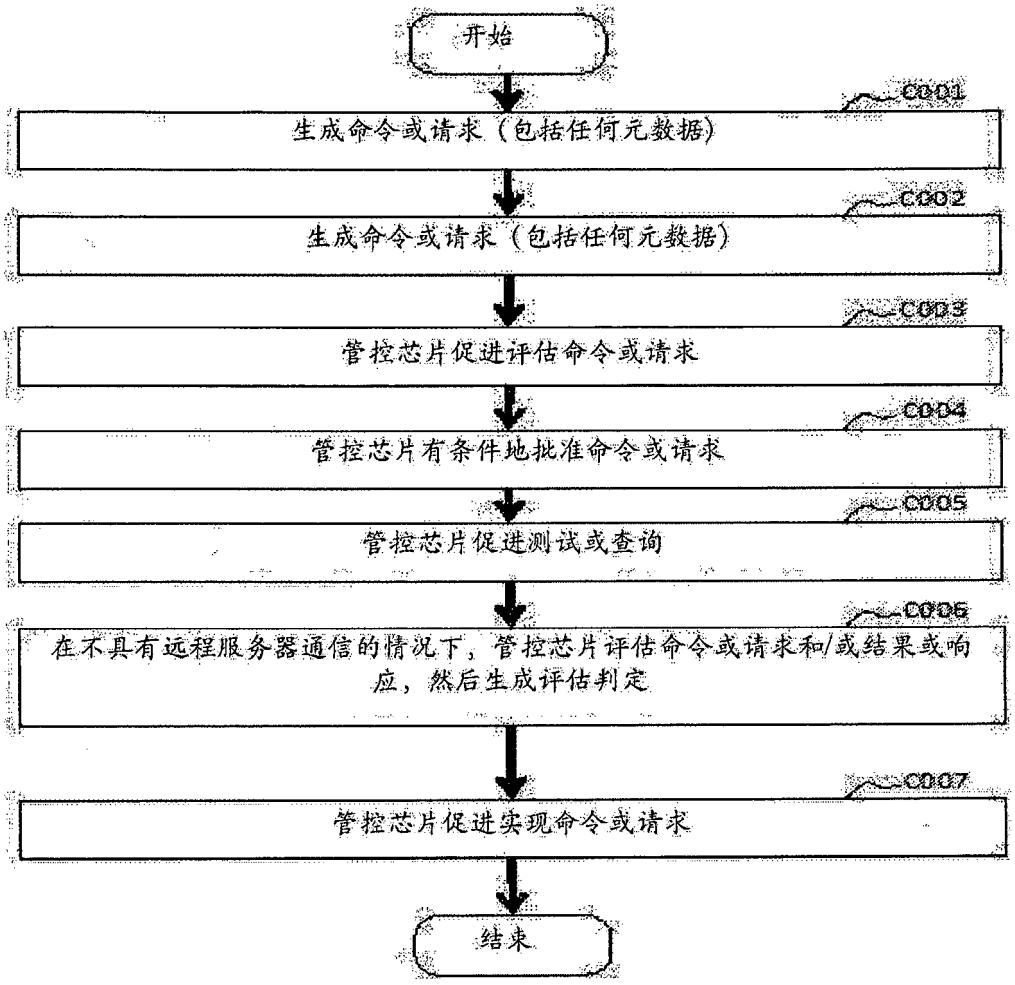

开始
C001
生成命令或请求（包括任何元数据）
C002
生成命令或请求（包括任何元数据）
C003
管控芯片促进评估命令或请求
C004
管控芯片有条件地批准命令或请求
C005
管控芯片促进测试或查询
C006
在不具有远程服务器通信的情况下，管控芯片评估命令或请求和/或结果或响应，然后生成评估判定
C007
管控芯片促进实现命令或请求
结束

图 5d

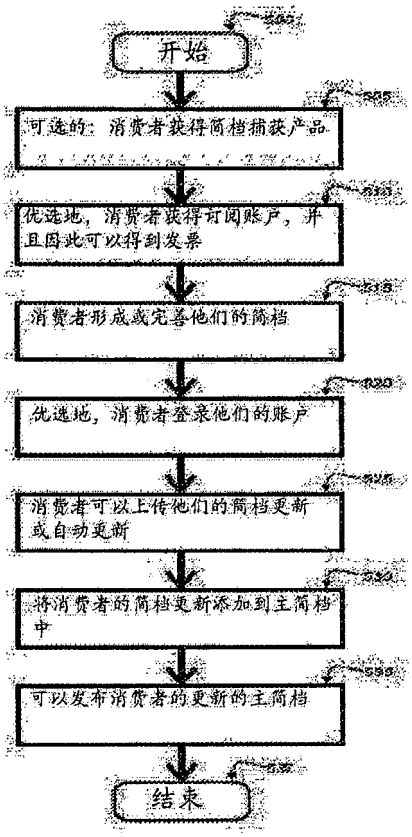

开始
可选的：消费者获得简档捕获产品
优选地，消费者获得可阅账户，并且因此可以得到发票
消费者形成或完善他们的简档
优选地，消费者登录他们的账户
消费者可以上传他们的简档更新或自动更新
将消费者的简档更新添加到主简档中
可以发布消费者的更新的主简档
结束

图 6

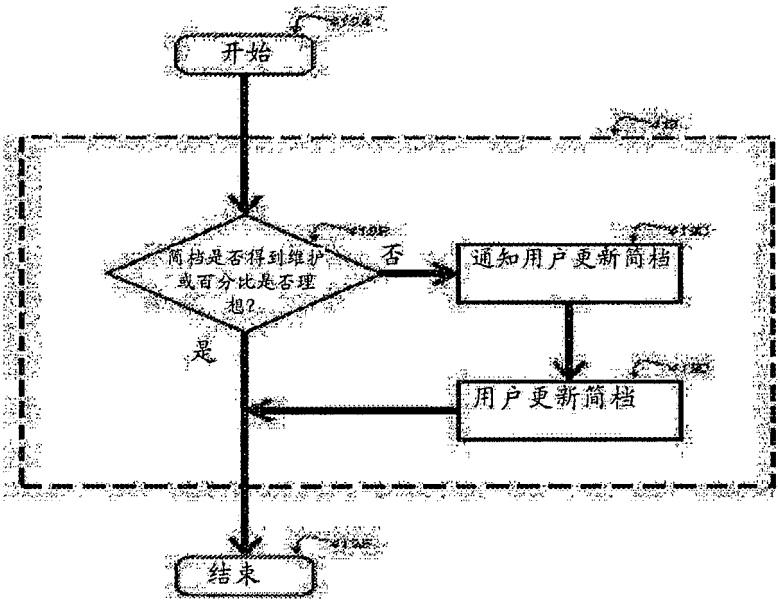


图 7

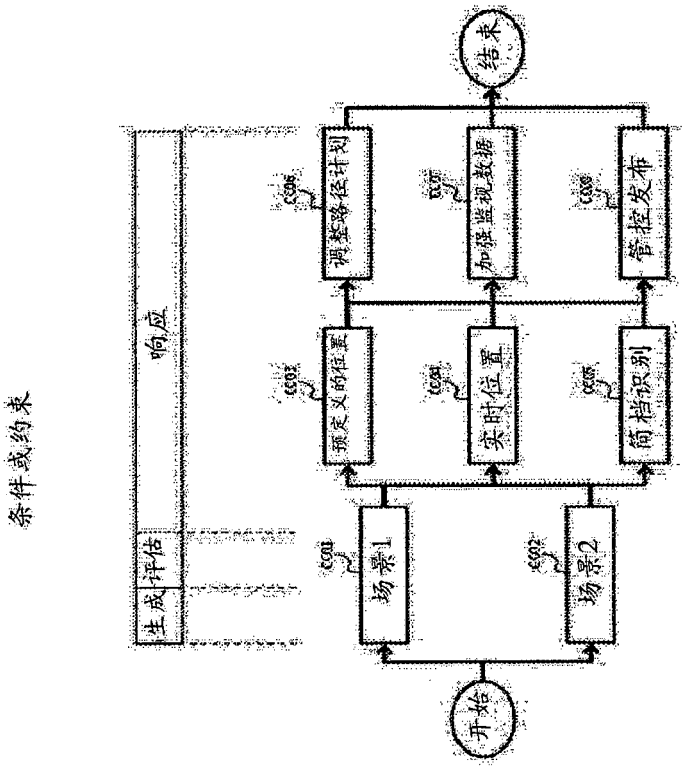

开始
结束
场景1
场景2
预定义的位置
实时位置
简档识别
调整路径计划
加强监视数据
管控发布
响应
评估
生成
条件或约束

图 7a

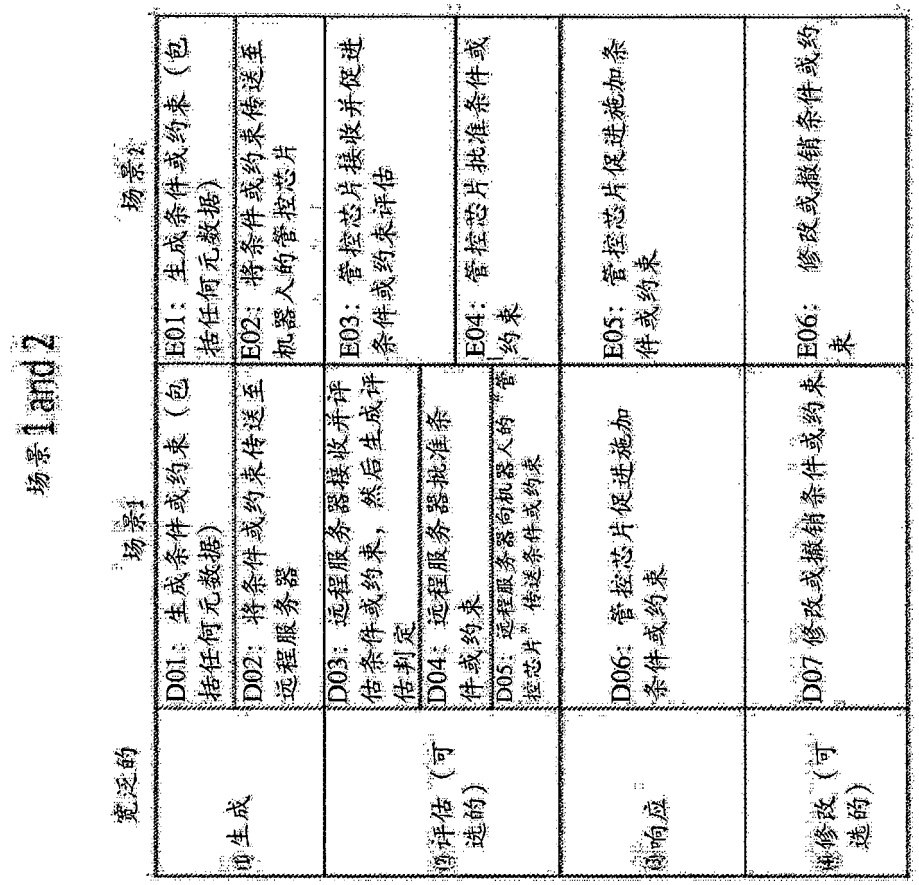

场景1 and 2
宽泛的
场景1
场景2
生成
D01：生成条件或约束（包括任何元数据）
E01：生成条件或约束（包括任何元数据）
D02：将条件或约束传送至远程服务器
E02：将条件或约束传送至机器人的管控芯片
评估（可选的）
D03：远程服务器接收并评估条件或约束，然后生成评估判定
E03：管控芯片接收并促进条件或约束评估
D04：远程服务器批准条件或约束
E04：管控芯片批准条件或约束
D05：远程服务器向机器人的"管控芯片"传送条件或约束
响应
D06：管控芯片促进施加条件或约束
E05：管控芯片促进施加条件或约束
修改（可选的）
D07 修改或撤销条件或约束
E06：修改或撤销条件或约束

图 7b

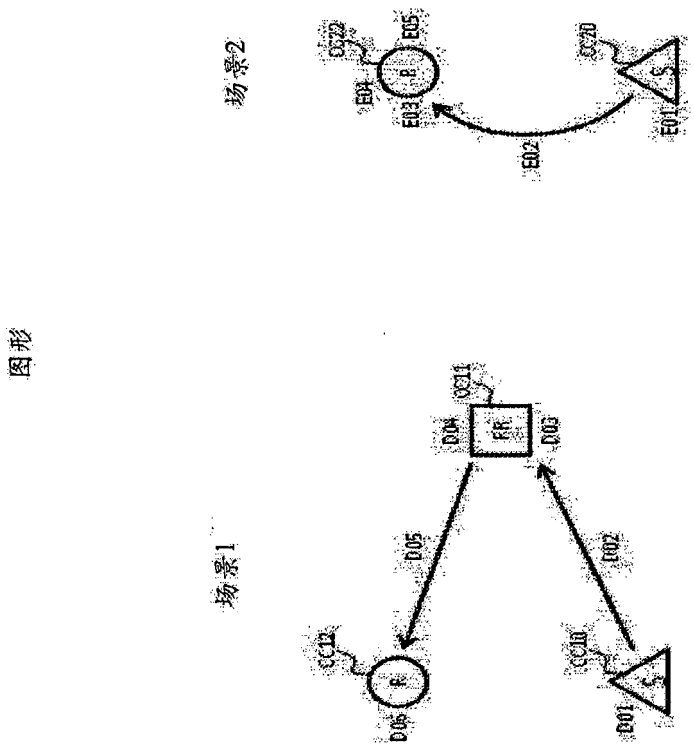

场景2
CC22
E05
E04
B
E03
CC20
S
E01
E02
图形
场景1
CC11
D04
R
D03
D05
D02
CC12
E
CC10
C
D01
D06

图 7c

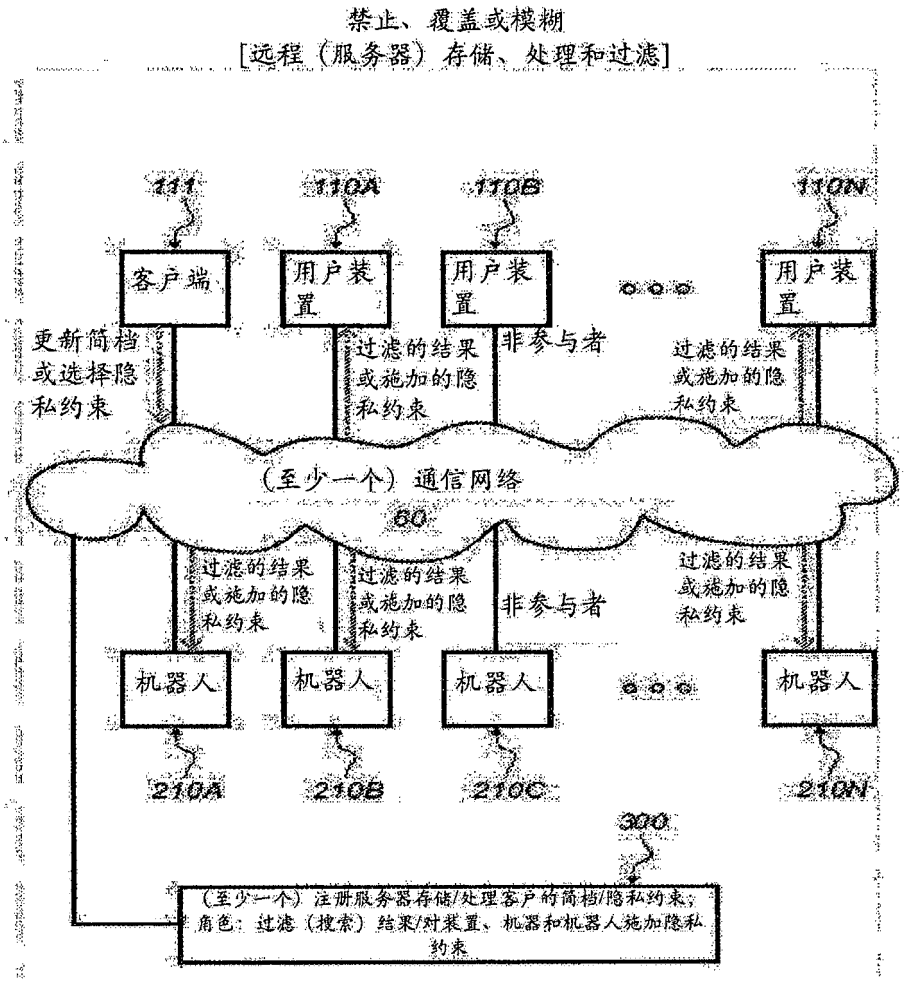

禁止、覆盖或模糊
[远程（服务器）存储、处理和过滤]
111
110A
110B
110N
客户端
用户装置
用户装置
用户装置
更新简档或选择隐私约束
过滤的结果或施加的隐私约束
非参与者
过滤的结果或施加的隐私约束
（至少一个）通信网络
60
过滤的结果或施加的隐私约束
过滤的结果或施加的隐私约束
非参与者
过滤的结果或施加的隐私约束
机器人
机器人
机器人
机器人
210A
210B
210C
210N
300
（至少一个）注册服务器存储/处理客户的简档/隐私约束；角色：过滤（搜索）结果/对装置、机器和机器人施加隐私约束

图 8

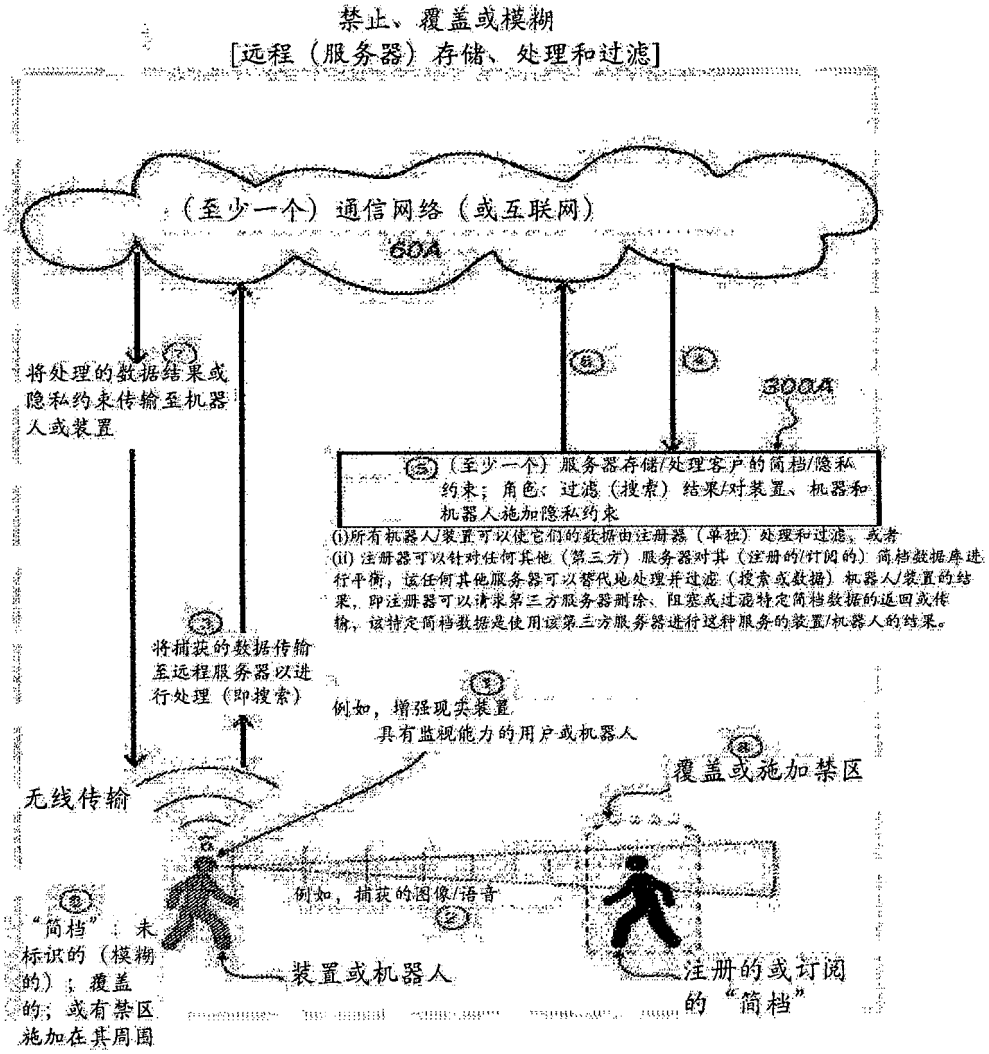

禁止、覆盖或模糊
[远程（服务器）存储、处理和过滤]
（至少一个）通信网络（或互联网）
604
将处理的数据结果或隐私约束传输至机器人或装置
300A
（至少一个）服务器存储/处理客户的简档/隐私约束；角色：过滤（搜索）结果/对装置、机器和机器人施加隐私约束
(i)所有机器人/装置可以使它们的数据由注册器（单独）处理和过滤，或者
(ii)注册器可以针对任何其他（第三方）服务器对其（注册的/订阅的）简档数据库进行平衡，该任何其他服务器可以替代地处理并过滤（搜索或数据）机器人/装置的结果，即注册器可以请求第三方服务器删除、阻塞或过滤特定简档数据的返回或传输，该特定简档数据是使用该第三方服务器进行这种服务的装置/机器人的结果。
将捕获的数据传输至远程服务器以进行处理（即搜索）
例如，增强现实装置
具有监视能力的用户或机器人
覆盖或施加禁区
无线传输
例如，捕获的图像/语音
“简档”：未标识的（模糊的）；覆盖的；或有禁区施加在其周围
装置或机器人
注册的或订阅的“简档”

图 9

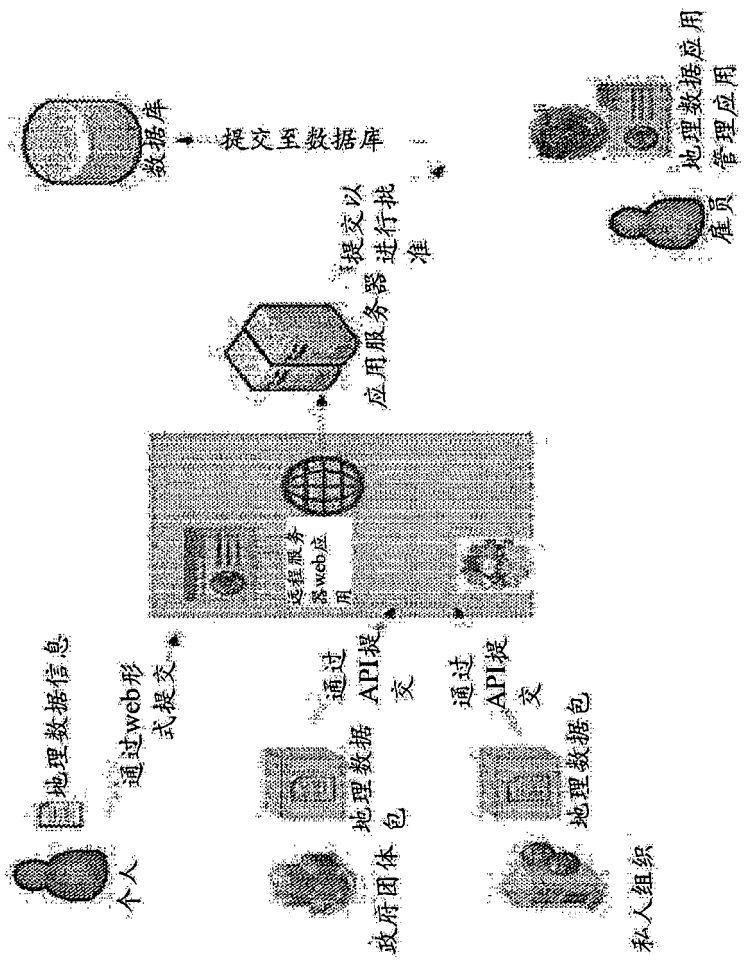

数据库
提交至数据库
地理数据应用管理应用
管理员
提交以进行批准
应用服务器
远程服务器web应用
地理数据信息
通过web形式提交
个人
通过API提交
地理数据包
政府团体
通过API提交
地理数据包
私人组织

图 9a

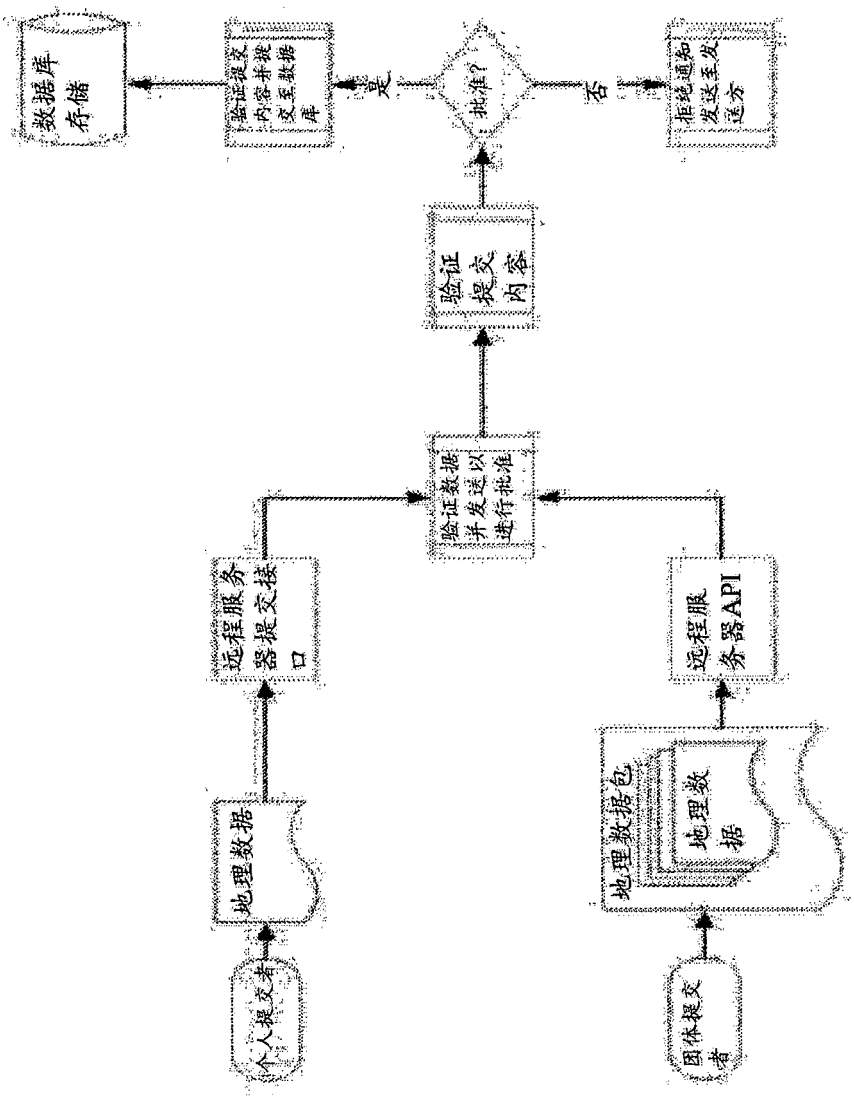

数据库存储
验证提交内容并提交至数据库
是
批准?
否
拒绝通知发送至发送方
验证提交内容
验证数据并发送以进行批准
远程服务器提交接口
远程服务器API
地理数据
地理数据包
地理数据
个人提交者
团体提交者

图 9b

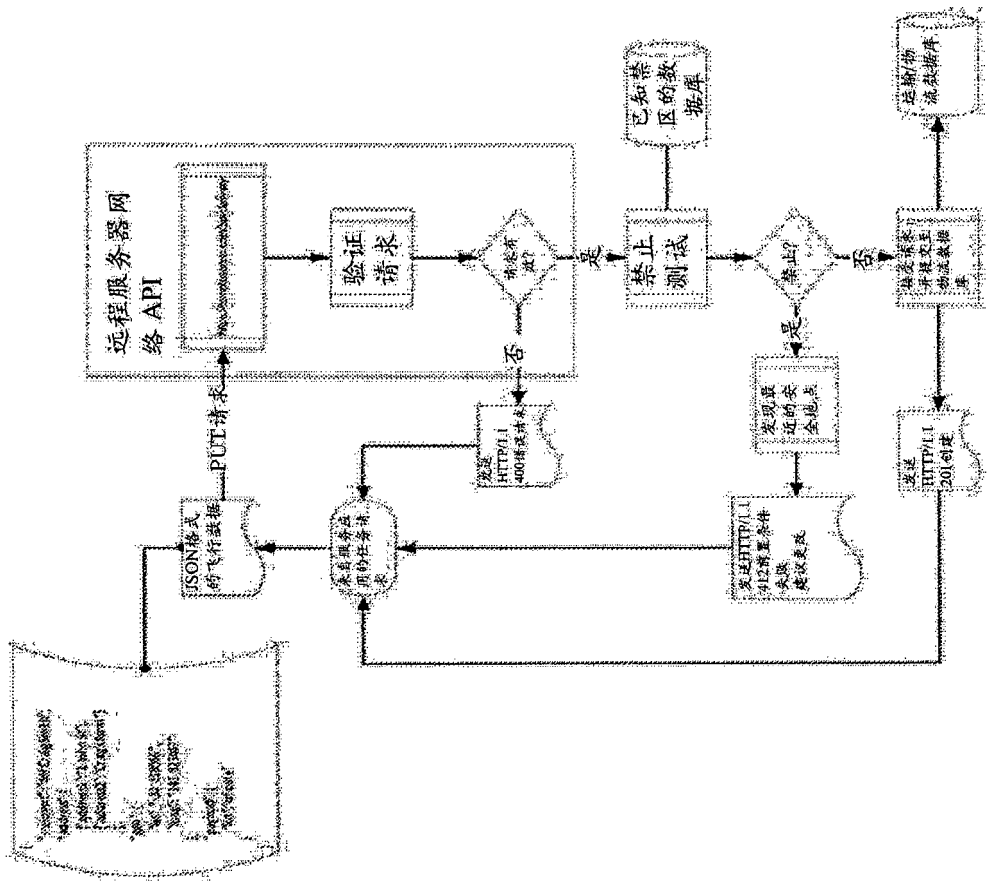

远程服务器网络 API
验证请求
是
否
禁止测试
已知禁区的数据库
禁止?
是
否
PUT请求
JSON格式的飞行数据
发送HTTP/1.1 400错误消息
发现最近的全地点
发送HTTP/1.1 201创建
发送HTTP/1.1 412前置条件失败 建议更改

图 9c

禁止、覆盖或模糊

[客户申请隐私：地图选择；位置跟踪器；简档保护]

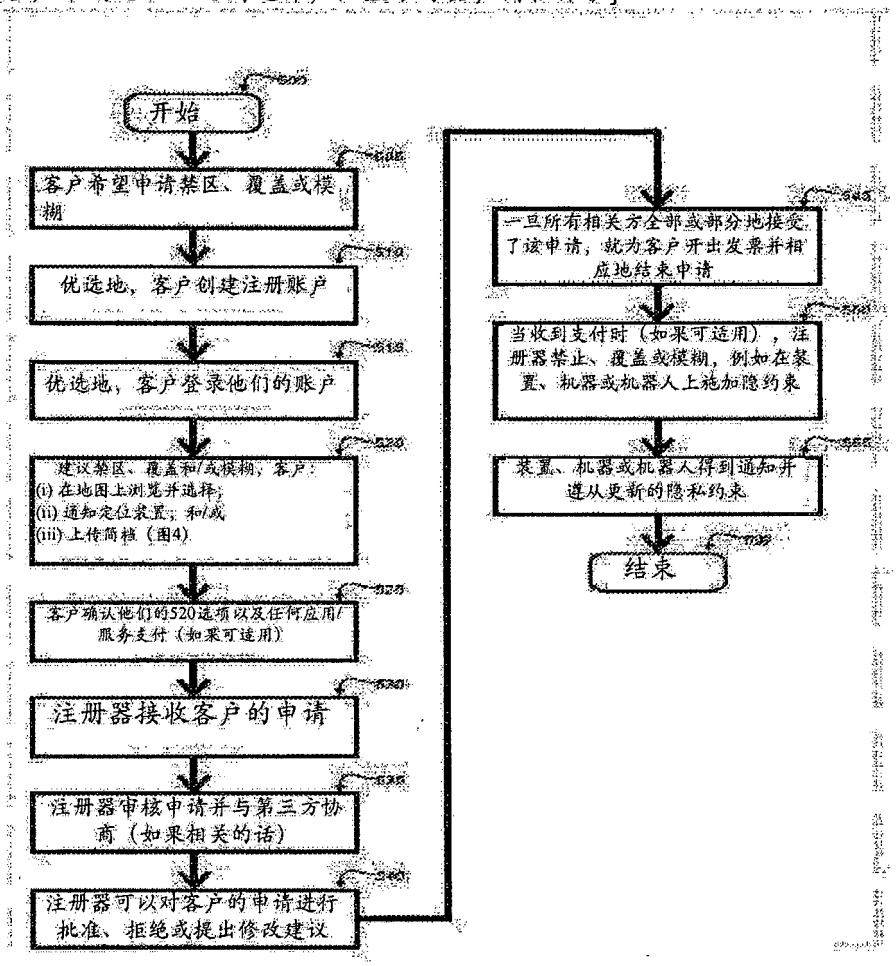


图 10

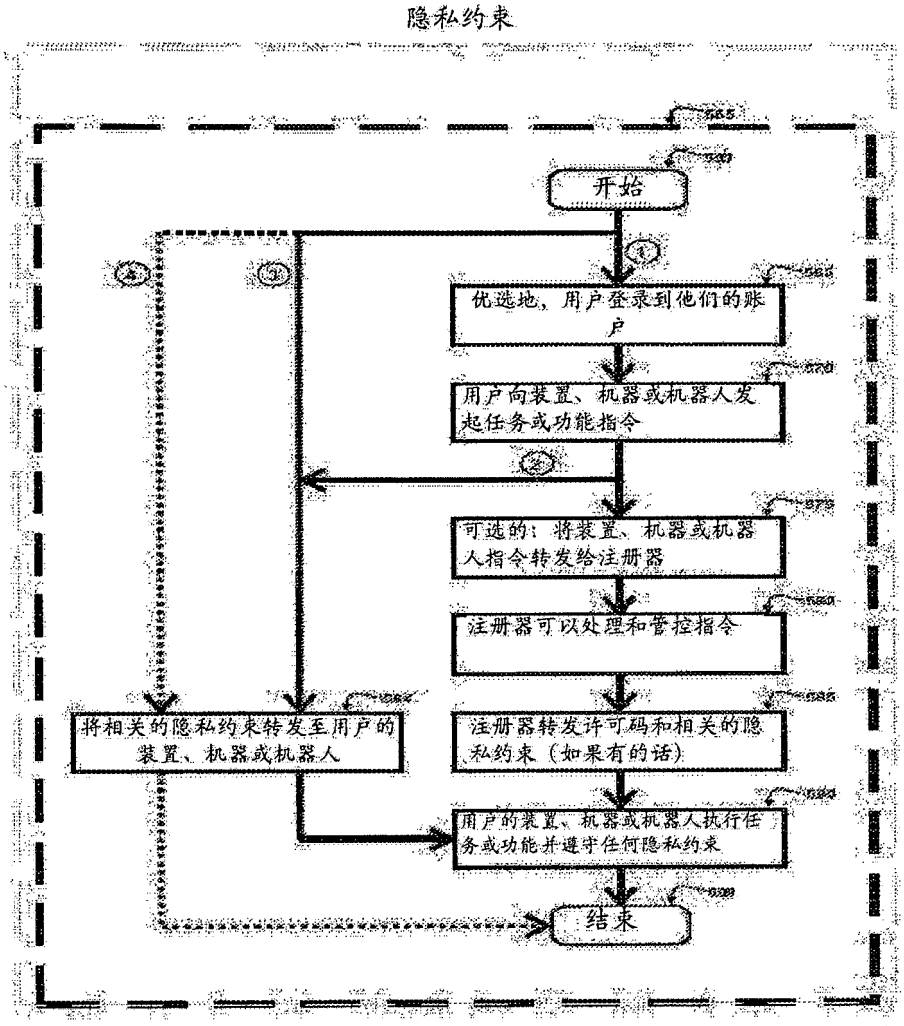

隐私约束
开始
优选地，用户登录到他们的账户
用户向装置、机器或机器人发起任务或功能指令
可选的：将装置、机器或机器人指令转发给注册器
注册器可以处理和管控指令
注册器转发许可码和相关的隐私约束（如果有的话）
用户的装置、机器或机器人执行任务或功能并遵守任何隐私约束
结束
将相关的隐私约束转发至用户的装置、机器或机器人

图 11

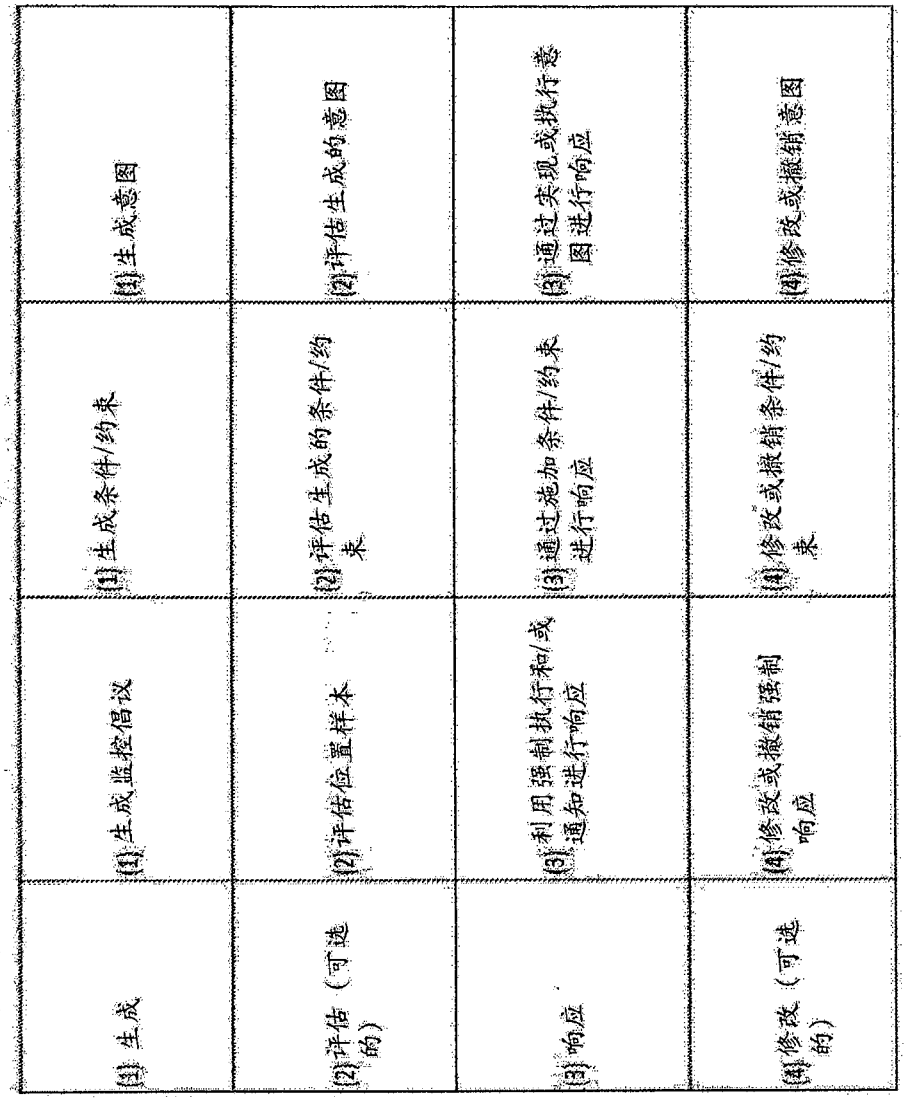
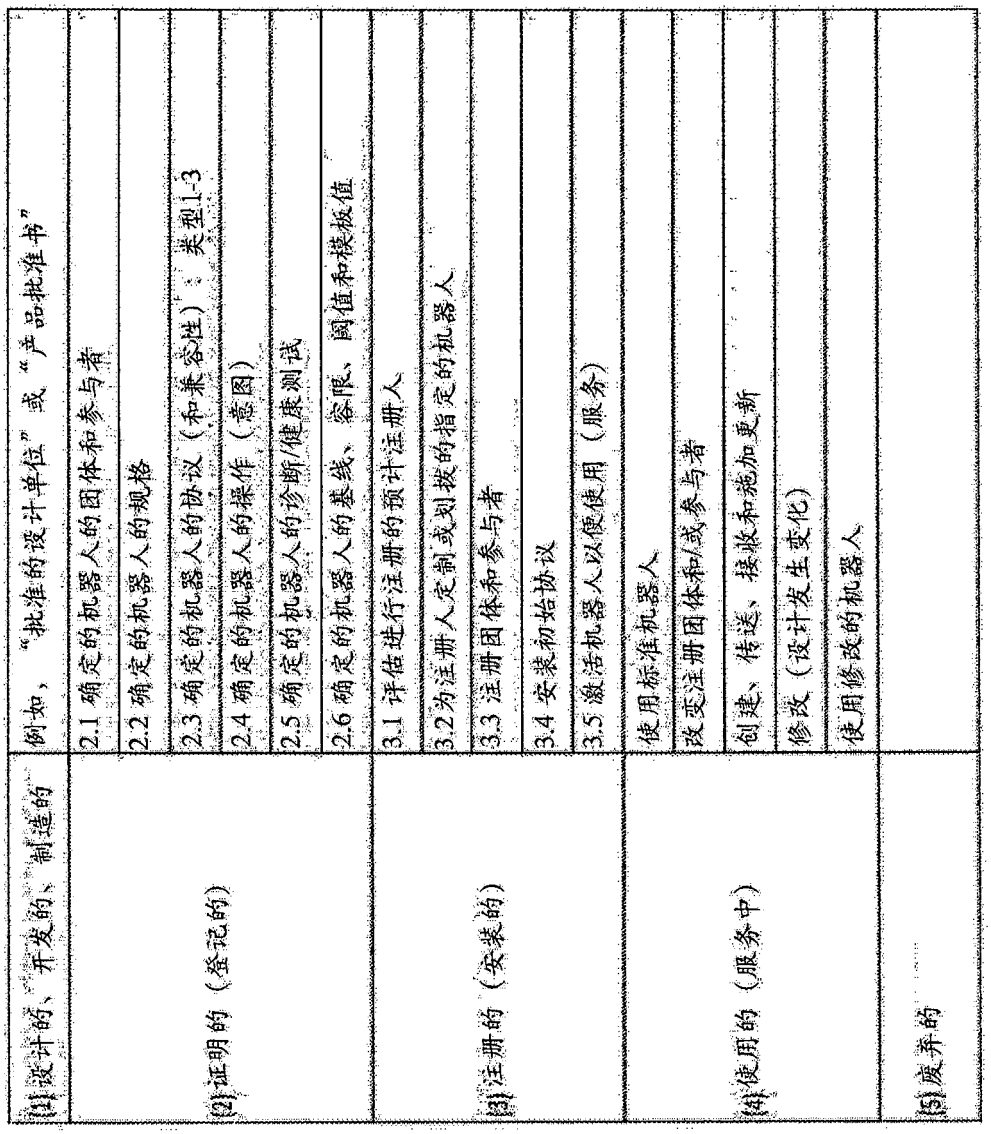

宽泛的
监控
条件
意图
(1)生成
(1)生成监控倡议
(1)生成条件/约束
(1)生成意图
(2)评估（可选的）
(2)评估位置样本
(2)评估生成的条件/约束
(2)评估生成的意图
(3)响应
(3)利用强制执行和/或通知进行响应
(3)通过施加条件/约束进行响应
(3)通过实现或执行意图进行响应
(4)修改（可选的）
(4)修改或撤销强制响应
(4)修改或撤销条件/约束
(4)修改或撤销意图

图 11a



(1)设计的、开发的、制造的	例如，“批准的设计单位”或“产品批准书”	
(2)证明的（签名的）	2.1 确定的机器人的团体和参与者	
	2.2 确定的机器人的规格	
	2.3 确定的机器人的协议（和兼容性）：类型1-3	
	2.4 确定的机器人的操作（意图）	
	2.5 确定的机器人的诊断/健康测试	
	2.6 确定的机器人的基线、容限、阈值和模板值	
(3)注册的（安装的）	3.1 评估进行注册的预计注册人	
	3.2 为注册人定制或划拨的指定的机器人	
	3.3 注册团体和参与者	
	3.4 安装初始协议	
	3.5 激活机器人以便使用（服务）	
(4)使用的（服务中）	使用标准机器人	
	改变注册团体和/或参与者	
	创建、传送、接收和施加更新	
	修改（设计发生变化）	
	使用修改的机器人	
(5)废弃的		

图 11b

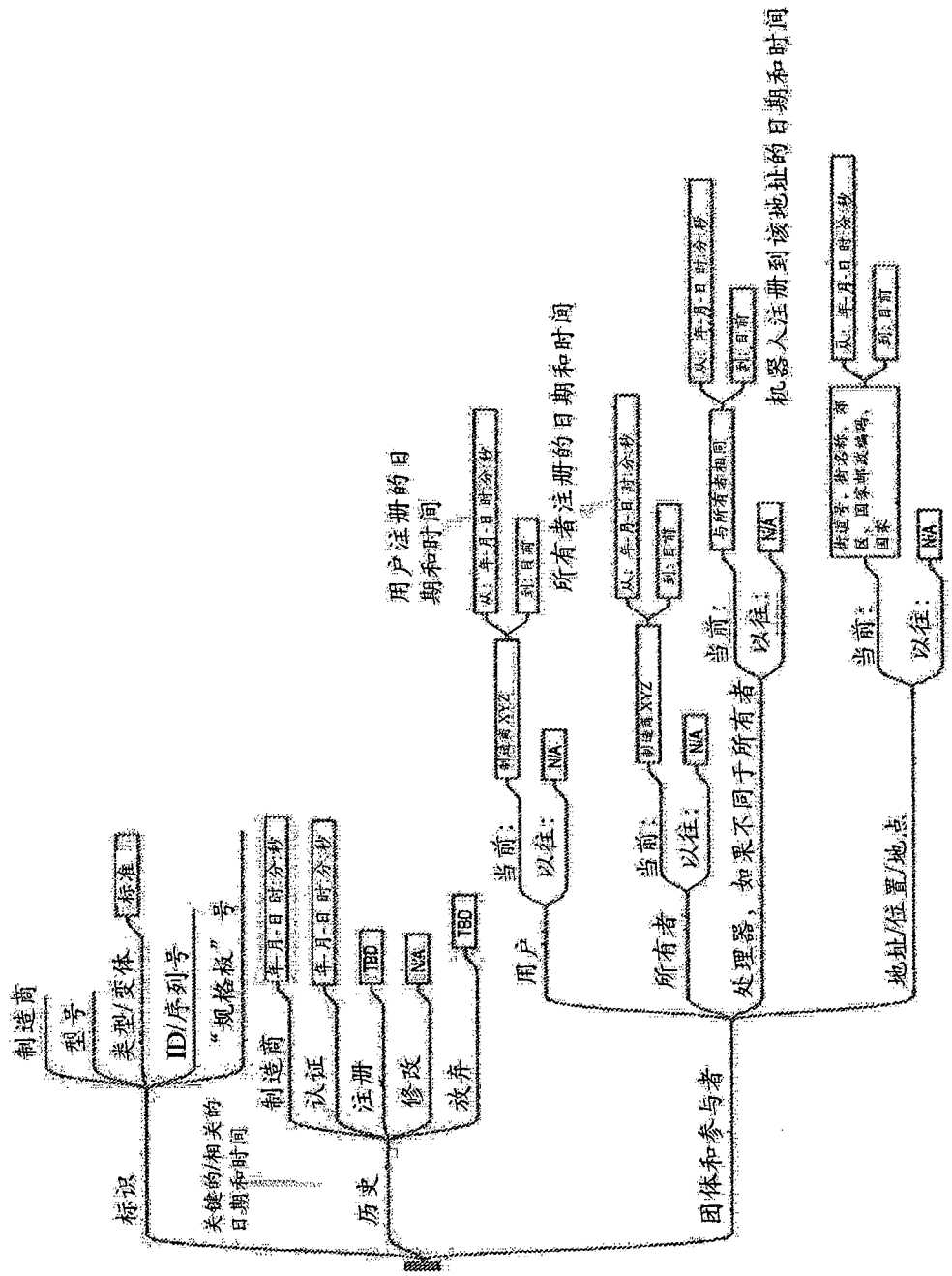

制造商
型号
类型/变体
标准
ID/序列号
"规格板"号
关键的/相关的日期和时间
制造商
年-月-日 时:分:秒
认证
年-月-日 时:分:秒
注册
TBD
修改
NA
放弃
TBD
标识
历史
用户
当前:
制造商XYZ
以往:
NA
用户注册的日期和时间
从: 年-月-日 时:分:秒
到: 目前
所有者
当前:
制造商XYZ
以往:
NA
所有者注册的日期和时间
从: 年-月-日 时:分:秒
到: 目前
处理器,如果不同于所有者
当前:
与所有者相同
以往:
NA
机器入注册到该地址的日期和时间
从: 年-月-日 时:分:秒
到: 目前
地址/位置/地点
当前:
街道号,街名称,城镇,州/县,国家/地区,邮政编码
以往:
NA
从: 年-月-日 时:分:秒
到: 目前
团体和参与者

图 11c

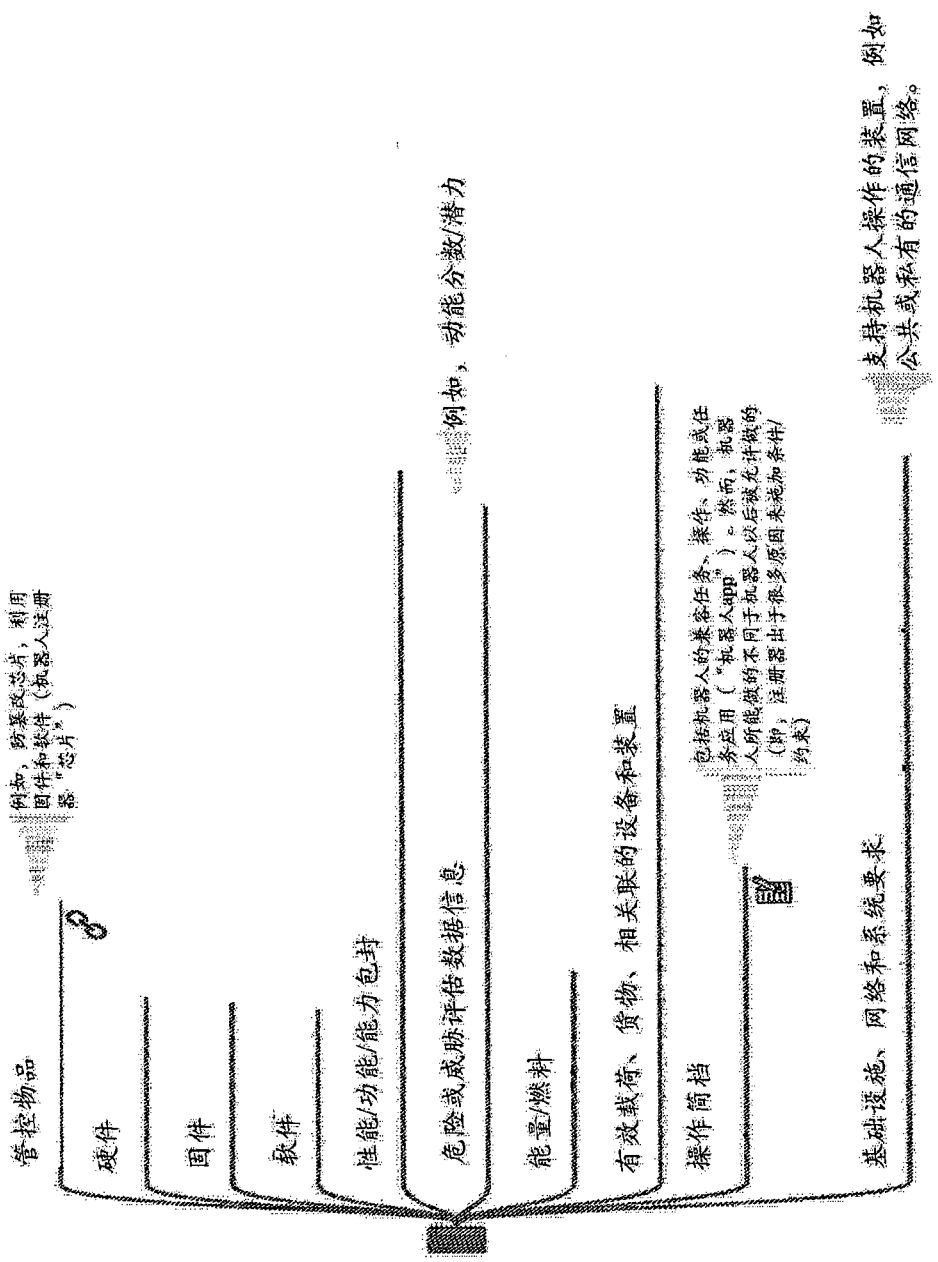

管控物品
例如，防篡改芯片，利用固件和软件（机器人注册器"芯片"）
硬件
固件
软件
性能/功能/能力包封
危险或威胁评估数据信息
例如，功能分数/潜力
能量/燃料
有效载荷、货物、相关联的设备和装置
操作简档
包括机器人的兼容任务、操作、功能或任务应用（"机器人app"）。然而，机器人所能做的不同于机器人以后被允许做的（例，注册器出于很多原因未施加条件/约束）
基础设施、网络和系统要求
支持机器人操作的装置，例如公共或私有的通信网络。

图 11d

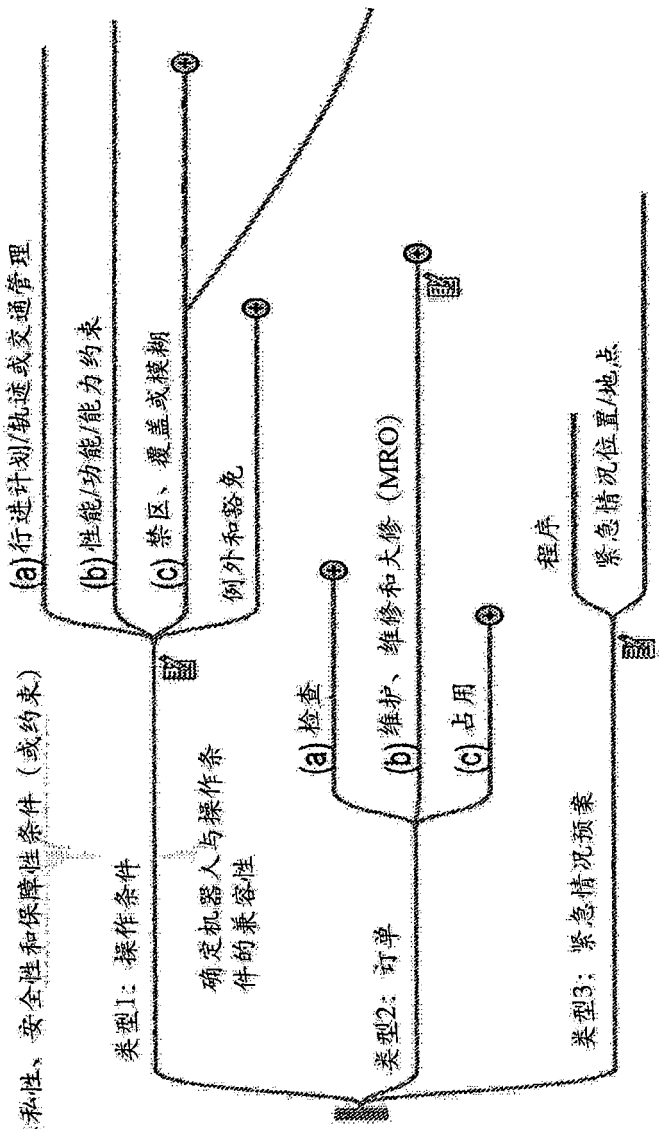

隐私性、安全性和保障性条件（或约束）
类型1：操作条件
确定机器人与操作条件的兼容性
(a)行进计划/轨迹或交通管理
(b)性能/功能/能力约束
(c)禁区、覆盖或模糊
例外和豁免
类型2：订单
(a)检查
(b)维护、维修和大修（MRO）
(c)占用
类型3：紧急情况预案
程序
紧急情况位置/地点

图 11e

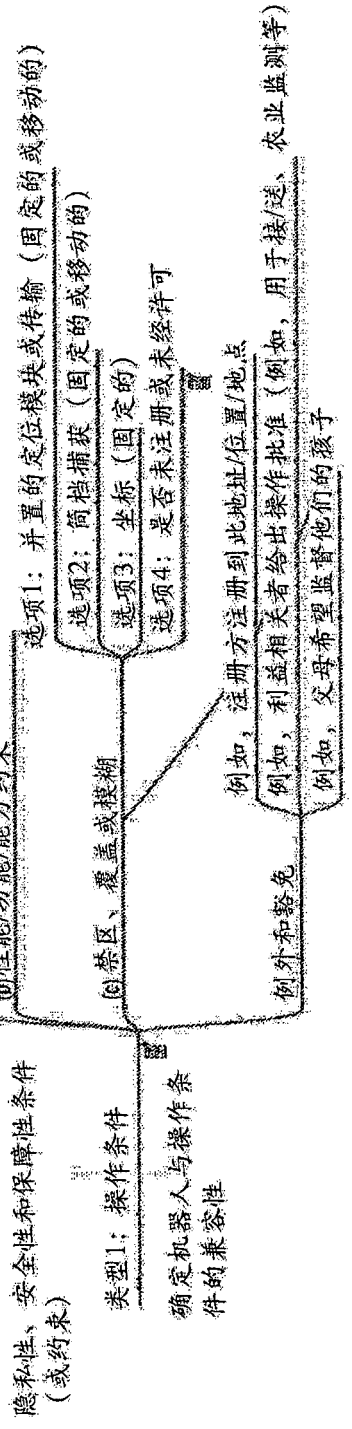

隐私性、安全性和保障性条件（或约束）
类型1：操作条件
确定机器人与操作条件的兼容性
(a)行进计划/轨迹或交通管理
(b)性能/功能/能力约束
(c)禁区、覆盖或模糊
例外和豁免
选项1：并置的定位模块或传输（固定的或移动的）
选项2：简档捕获（固定的或移动的）
选项3：坐标（固定的）
选项4：是否未注册或未经许可
例如，注册方注册到此地址/位置/地点
例如，利益相关者给出操作批准（例如，用于接/送、农业监测等）
例如，父母希望监督他们的孩子

图 11f

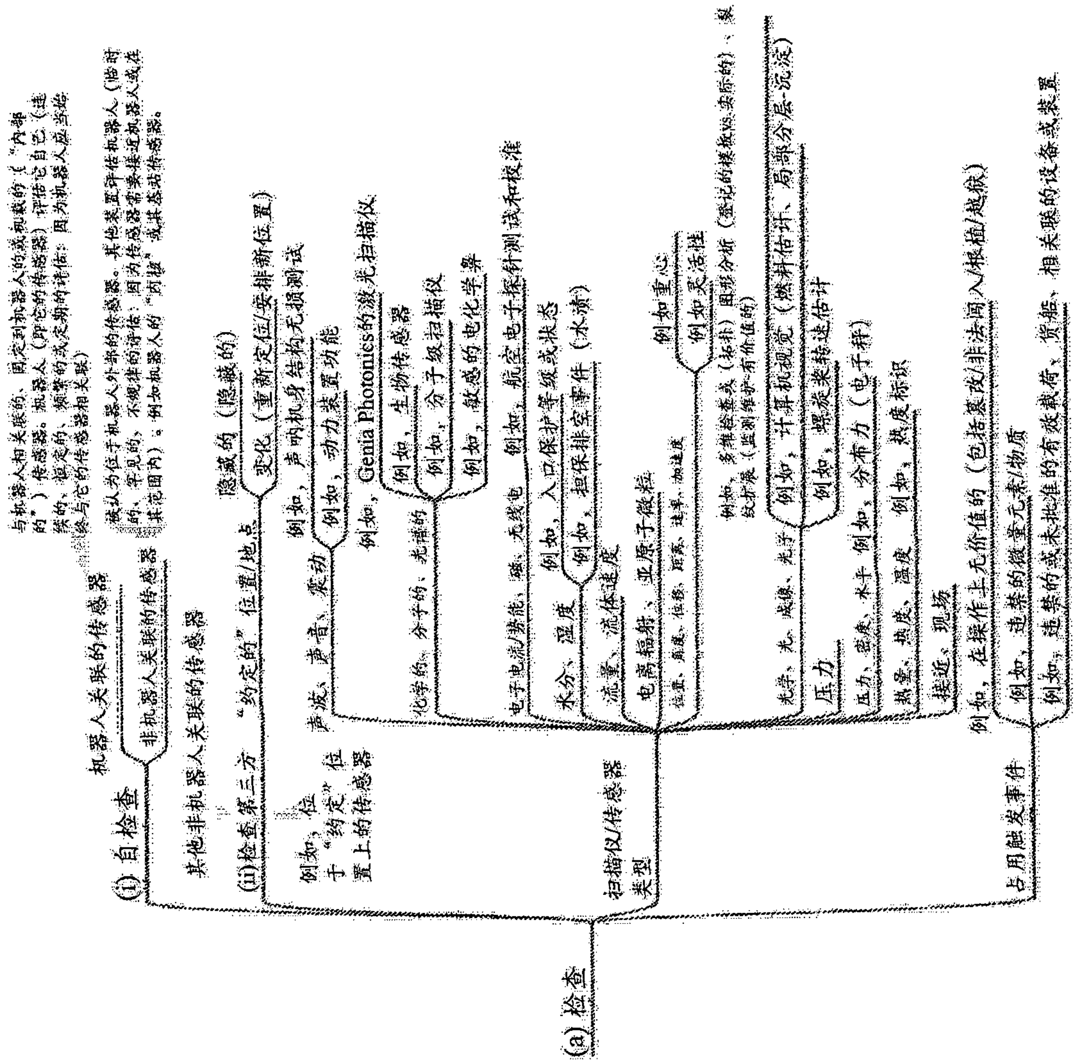

(a) 检查
(i) 自检查
机器人关联的传感器
与机器人相关联的、固定到机器人的或承载的（"内部的"）传感器。机器人（即它的传感器）评估它自己（连续的、指定的、频繁的或定期的评估；因为机器人应当总是与它的传感器相关联）
非机器人关联的传感器
被认为位于机器人外部的传感器。其他装置评估机器人（临时的、罕见的、不规律的评估；因为传感器需要接近机器人或在其范围内）。例如机器人的"内脏"或其表现传感器。
其他非机器人关联的传感器
(ii)检查第三方
"约定的"位置/地点
例如，位于"约定"位置上的传感器
隐藏的（隐藏的）
变化（重新定位/安排新位置）
例如，声呐机身结构无损测试
声波、声音、震动
例如，动力装置功能
化学的、分子的、光谱的
例如，Genia Photonics的激光扫描仪
例如，生物传感器
例如，分子级扫描仪
例如，敏感的电化学鼻
电子电流/势能、磁、无线电
例如，航空电子探针测试和校准
水分、湿度
例如，入口保护等级或状态
例如，担保排空事件（水渍）
流量、流体速度
电离辐射、亚原子微粒
位置、角度、位移、距离、速度、加速度
例如重心
例如灵活性
例如，多维检查点（标针）图形分析（登记的模板vs.实际的），复杂扩展（监测维护-有价值的）
光学、光、成像、光子
例如，计算机视觉（燃料估计、局部分层-沉淀）
例如，螺旋桨转速估计
压力、应力、水平
例如，分布力（电子秤）
热量、热度、温度
例如，热度标识
接近、现场
扫描仪/传感器类型
占用触发事件
例如，在操作上无价值的（包括暴皮/非法闯入/根植/越狱）
例如，违禁的微量元素/物质
例如，违禁的或未批准的有效载荷、货船、相关联的设备或装置

图 11g

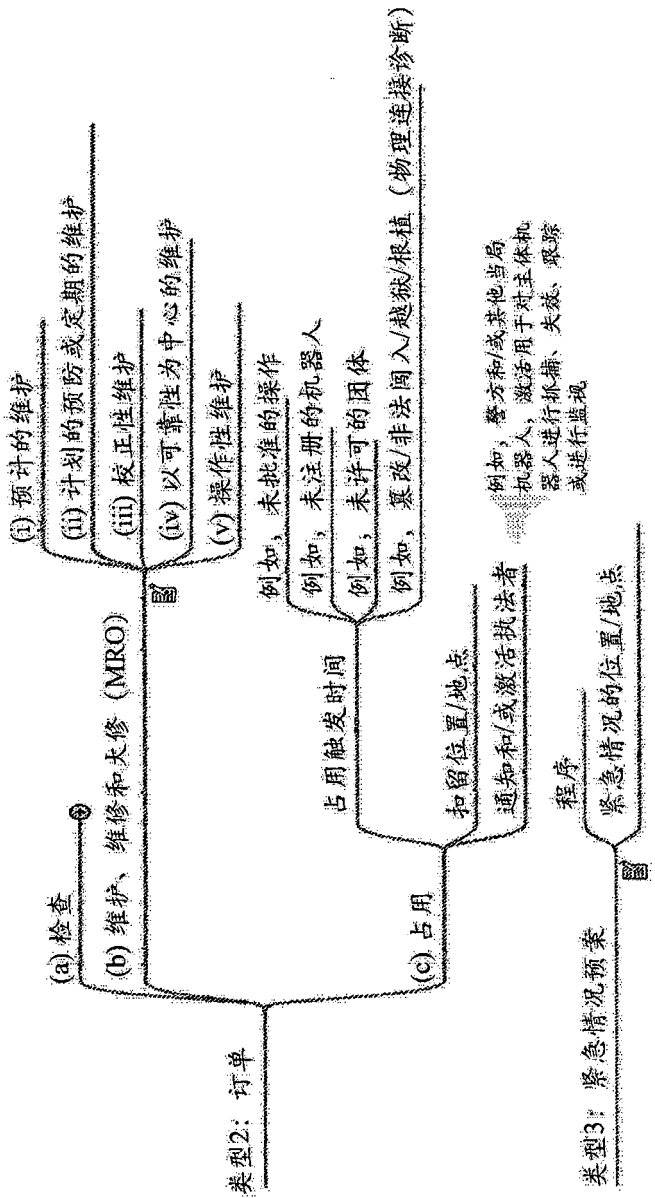

类型2：订单
(a) 检查
(b) 维护、维修和大修（MRO）
(i) 预计的维护
(ii) 计划的预防或定期的维护
(iii) 校正性维护
(iv) 以可靠性为中心的维护
(v) 操作性维护
(c) 占用
占用触发时间
例如，未批准的操作
例如，未注册的机器人
例如，未许可的团体
例如，塞茨/非法闯入/越狱/根植（物理连接诊断）
扣留位置/地点
通知和/或激活执法者
例如，警方和/或其他当局机器人，激活用于对主体机器人进行扣押、失效、跟踪或进行监视
程序
类型3：紧急情况预案
紧急情况的位置/地点

图 11h

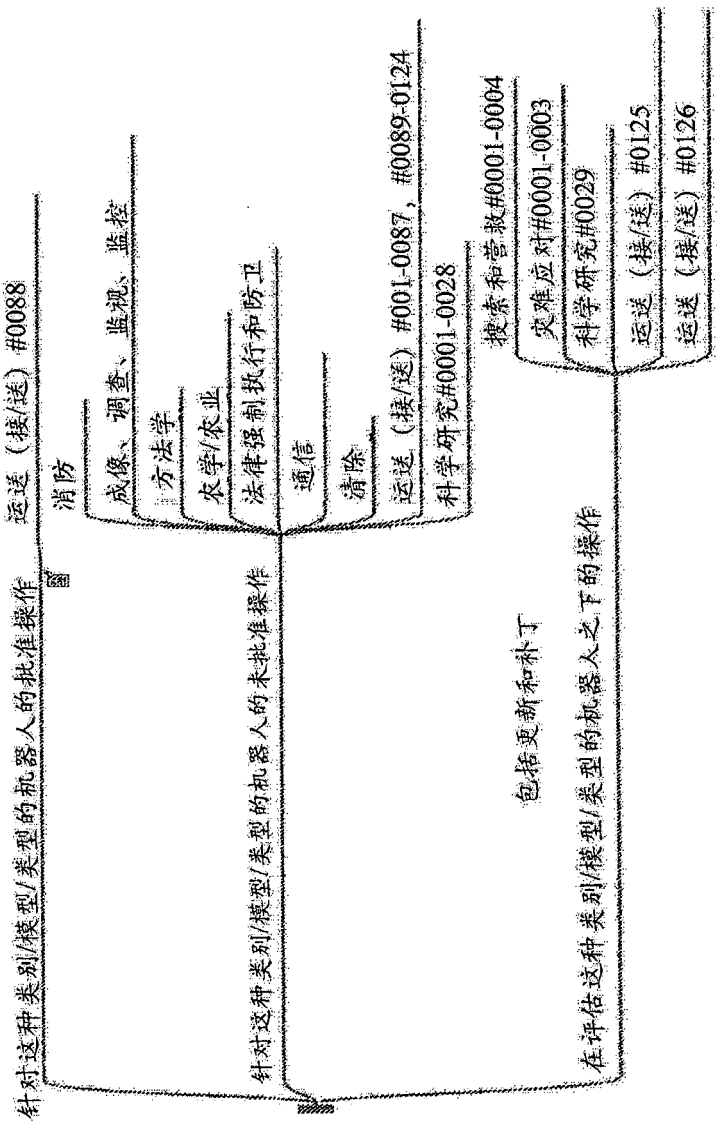

针对这种类别/模型/类型的机器人的批准操作
运送（接/送）#0088
针对这种类别/模型/类型的机器人的未批准操作
消防
成像、调查、监视、监控
方法学
农学/农业
法律强制执行和防卫
通信
清除
运送（接/送）#0001-0087，#0089-0124
科学研究#0001-0028
搜索和营救#0001-0004
灾难应对#0001-0003
科学研究#0029
运送（接/送）#0125
运送（接/送）#0126
包括更新和补丁
在评估这种类别/模型/类型的机器人之下的操作

图 11i

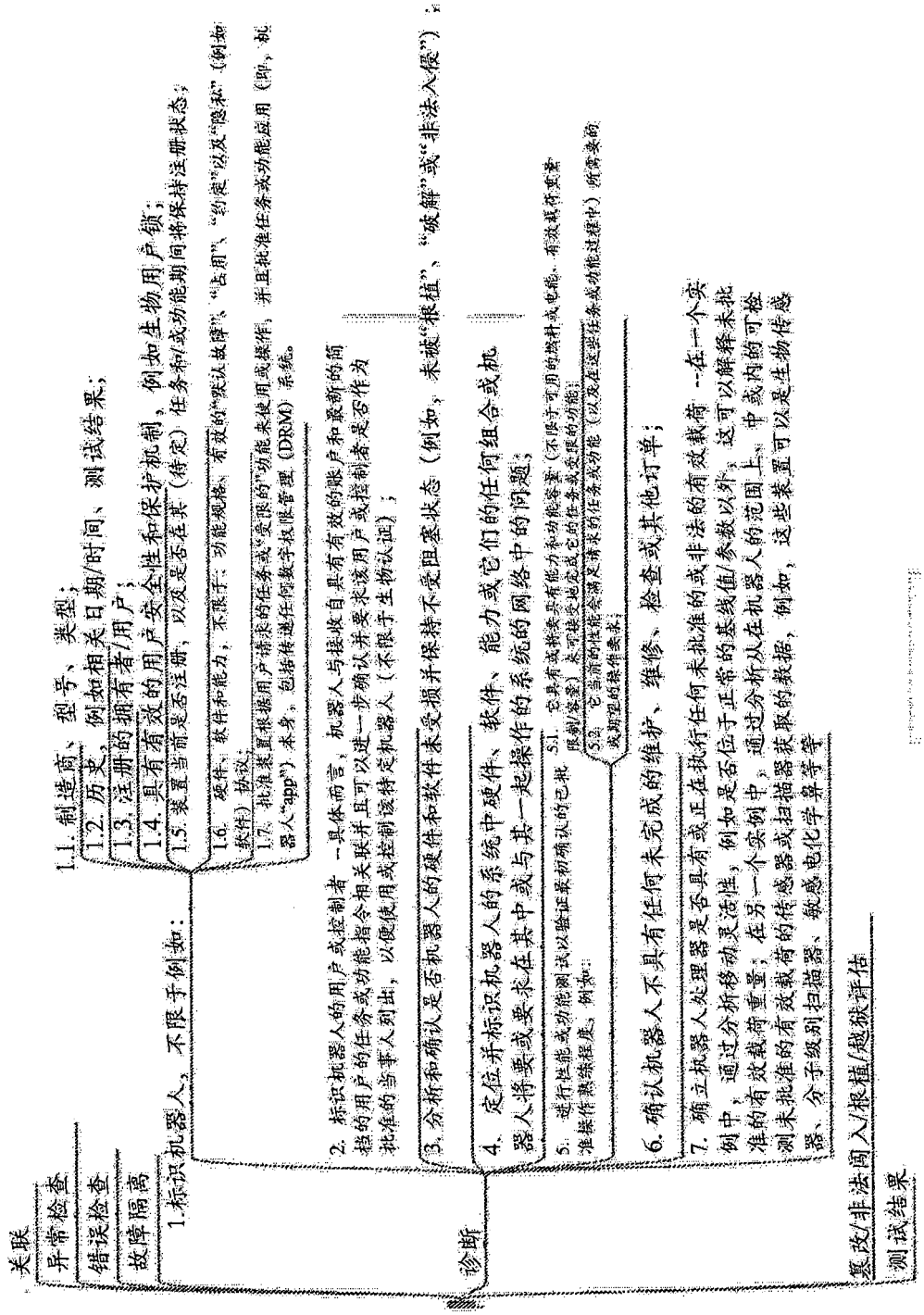

关联
异常检查
错误检查
故障隔离
诊断
1.标识机器人，不限于例如：
1.1. 制造商、型号、类型；
1.2. 历史，例如相关日期/时间、测试结果；
1.3. 注册的拥有者/用户；
1.4. 具有有效的用户安全性和保护机制，例如生物用户锁；
1.5. 装置当前是否注册，以及是否在某（特定）任务和/或功能期间将保持注册状态；
1.6. 硬件、软件和能力，不限于：功能规格、有效的"默认故障"、"出厂"、"约定"以及"隐私"（例如软件）协议；
1.7. 批准某些被用户请求的任务或"受限的"功能来使用或操作，并且批准任务或功能应用（即，机器人"app"）本身，包括传送任何数字权限管理（DRM）系统。
2. 标识机器人的用户或授权者 -具体而言，机器人与接收自具有有效的账户和最新的简档的用户的任务或功能指令相关联并且可以进一步确认并要求该用户或控制者是否作为批准的当事人列出，以便使用或控制该特定机器人（不限于生物认证）；
3. 分析和确认是否机器人的硬件和软件未受损并保持不受阻塞状态（例如，未被"根植"、"破解"或"非法入侵"）；
4. 定位并标识机器人的系统中硬件、软件、能力或它们的任何组合或机器人将要或要求在其中或与其一起操作的系统的网络中的问题；
5. 进行性能或功能测试以验证最初确认的已批准操作熟练程度，例如：
5.1. 它具有或将要具有能力和功能容量（不限于可用的燃料或电能、有效载荷容量）是可接受地完成它的任务或受限的功能；
5.2. 它当前的性能会满足需求的任务或功能（以及在这些任务或功能过程中）所需要的载荷的操作要求；
6. 确认机器人不具有任何未完成的维护、维修、检查或其他订单；
7. 确立机器人处理器是否具有或正在执行任何未批准的或非法的有效载荷 --在一个实例中，通过分析移动灵活性，例如是否位于正常的基线值/参数以外，这可以解释未批准的有效载荷重量；在另一个实例中，通过分析从在机器人的范围上、中或内的可检测未批准的有效载荷的传感器或扫描器获取的数据，例如，这些装置可以是生物传感器、分子级别扫描器、敏感电化学鼻等等
篡改/非法闯入/根植/越狱评估
测试结果

图 11j

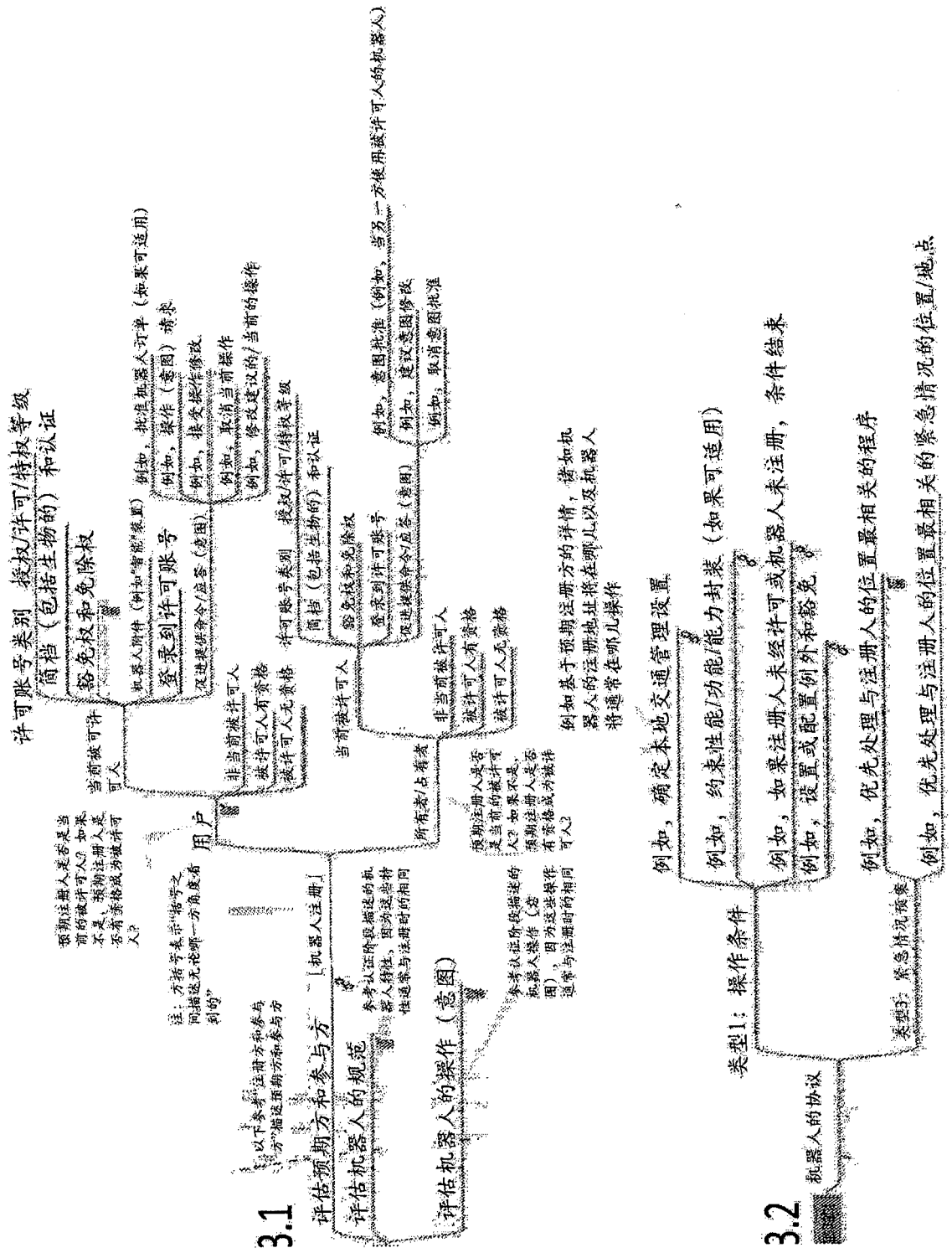

3.1
3.2
用户
[机器人注册]
评估预期方和参与方
评估机器人的规范
评估机器人的操作（意图）
许可账号类别 接权/许可/特权等级
简档（包括生物的）和认证
豁免权和免除权
登录到许可账号
当前被许可人
非当前被许可人
被许可人有资格
被许可人无资格
所有者/占有者
机器人协议
类型1：操作条件
类型3：紧急情况预案
例如，确定本地交通管理设置
例如，约束性能/功能/能力封装（如果可适用）
例如，如果注册人未经许可或机器人未注册，条件结束
例如，设置或配置例外和豁免
例如，优先处理与注册人的位置最相关的程序
例如，优先处理与注册人的位置最相关的紧急情况的位置/地点

图 11k

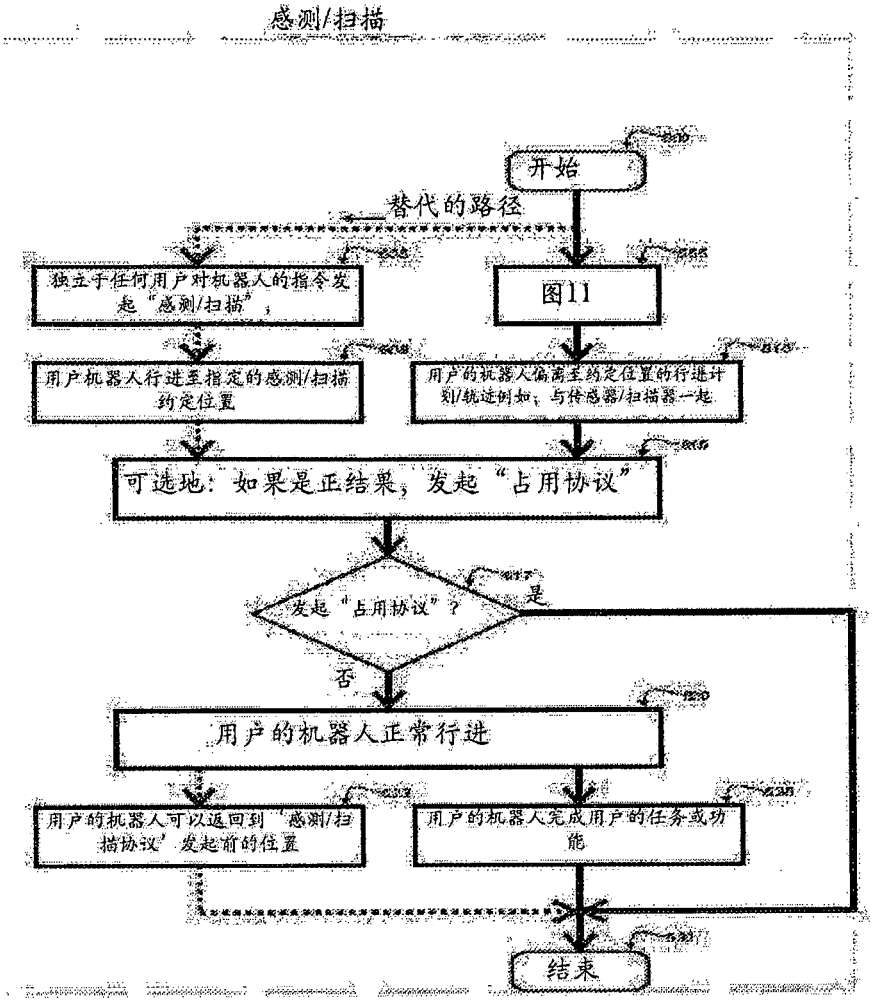

感测/扫描
开始
替代的路径
独立于任何用户对机器人的指令发起“感测/扫描”；
图11
用户机器人行进至指定的感测/扫描约定位置
用户的机器人偏离至约定位置的行进计划/轨迹例如，与传感器/扫描器一起
可选地：如果是正结果，发起“占用协议”
发起“占用协议”？
是
否
用户的机器人正常行进
用户的机器人可以返回到“感测/扫描协议”发起前的位置
用户的机器人完成用户的任务或功能
结束

图 12

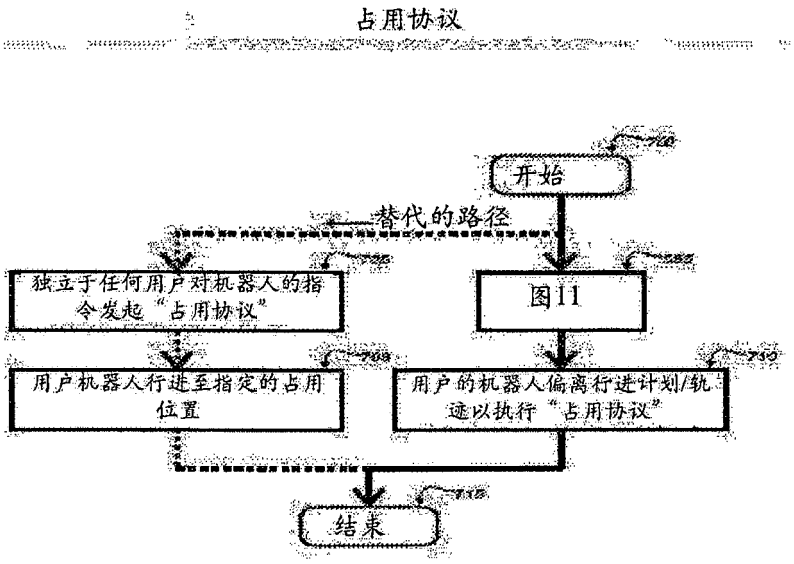

占用协议
开始
替代的路径
独立于任何用户对机器人的指令发起“占用协议”
图11
用户机器人行进至指定的占用位置
用户的机器人偏离行进计划/轨迹以执行“占用协议”
结束

图 13

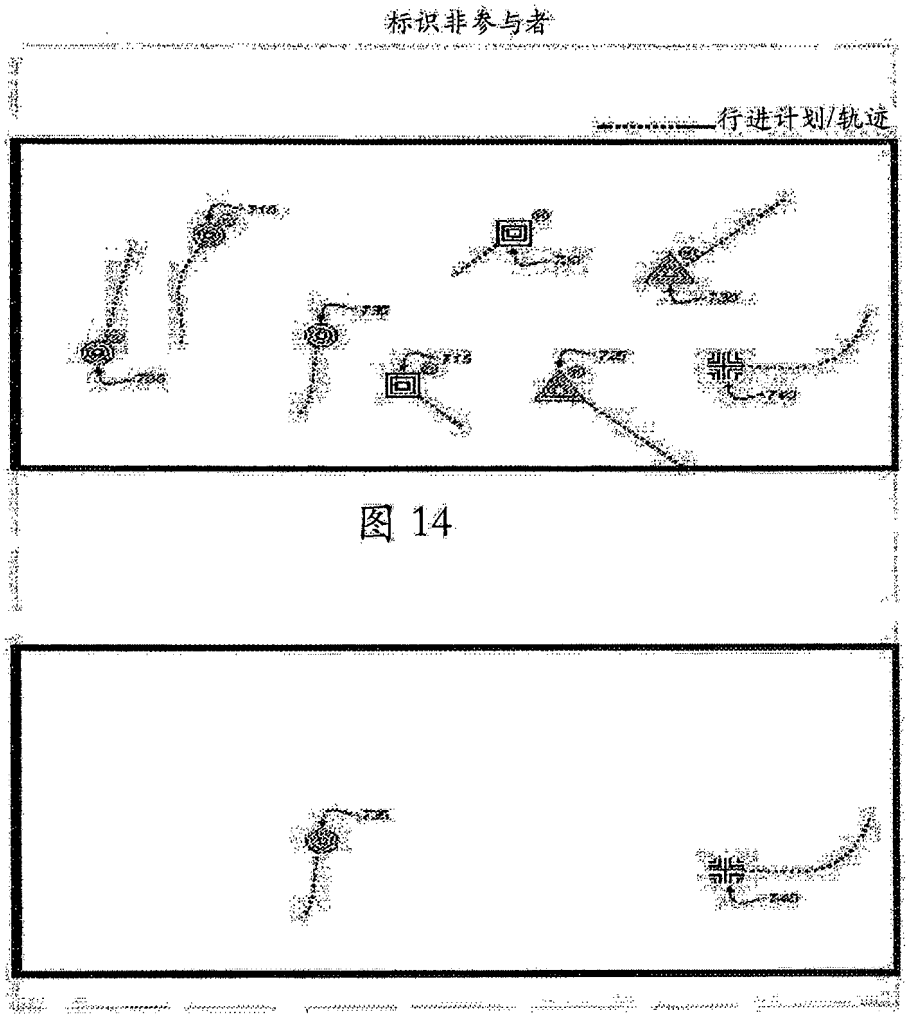


图 14

图 15

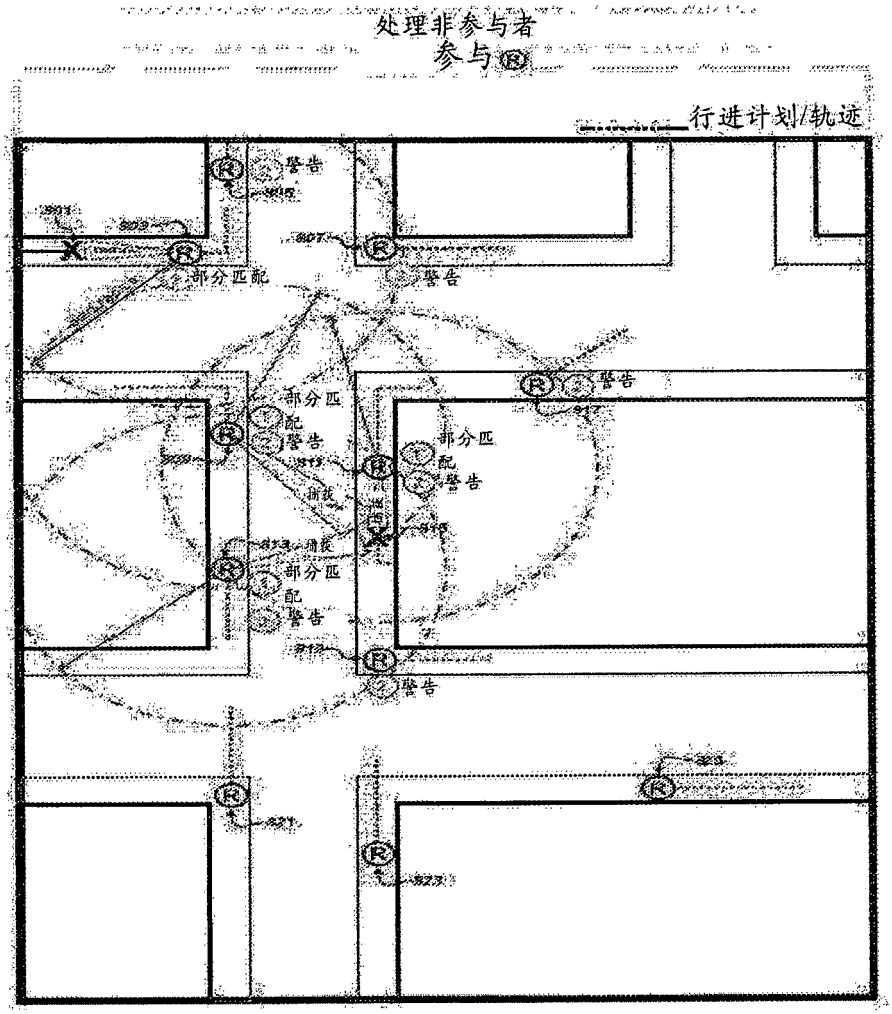


图 16