(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 4 239 601 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
06.09.2023 Bulletin 2023/36

(21) Application number: **23160018.0**

(22) Date of filing: **03.03.2023**

(51) International Patent Classification (IPC):
G07C 9/00 $^{(2020.01)}$ ***B65F 5/00*** $^{(2006.01)}$

(52) Cooperative Patent Classification (CPC):
G07C 9/00174; B65F 5/005; G07C 9/00896;
G07C 2009/0065; G07C 2009/00769

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC ME MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA
Designated Validation States:
KH MA MD TN

(30) Priority: **04.03.2022 IT 202200004133**

(71) Applicant: **Hyperion S.r.l.**
52100 Arezzo (IT)

(72) Inventors:
- **BARTOLINI, Sandro**
  52100 Arezzo (IT)
- **ZOPPETTI, Claudia**
  52100 Arezzo (IT)
- **ROSADINI, Simone**
  52100 Arezzo (IT)
- **MECOCCI, Alessandro**
  52100 Arezzo (IT)
- **RACIOPPI, Vittorio**
  52100 Arezzo (IT)
- **BAGHINI, Andrea**
  52100 Arezzo (IT)
- **FRANCI, Lorenzo**
  52100 Arezzo (IT)
- **PARRINO, Stefano**
  52100 Arezzo (IT)
- **POZZEBON, Alessandro**
  52100 Arezzo (IT)

(74) Representative: **Penza, Giancarlo et al**
Bugnion S.p.A.
Viale Lancetti, 17
20158 Milano (IT)

(54) ELECTRONIC SYSTEM TO CONTROL ACCESS TO A WASTE CONTAINER AND WASTE CONTAINER THEREOF

(57) It is disclosed an electronic system (1) to control the access of a user to a waste container. The system comprises a Central Processing Unit (2), a volatile central memory (3), a non-volatile memory (4), a short-distance wireless signal transceiver (20, 5, 6, 7), a power supply battery, a circuit to manage electrical energy flows and a photovoltaic panel. The central memory is configured to store the object code of the running operating system and the object code of the running software program and data of the software program. The Central Processing Unit is configured to receive a signal indicative of the value of a user identifier or indicative of an authenticated command or of an invalidity command, to verify whether the user is authorized to deliver waste in the waste container, by means of a verification of the validity of at least part of said user identifier or by means of the verification of reception of said authenticated command or of said invalidity command, and to generate, as a function of the outcome of said verification, a driving signal (S_drv) to lock or unlock the electro-mechanical lock of the waste container.

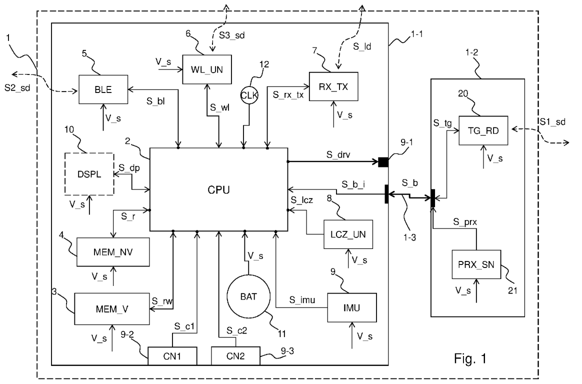

Fig. 1

Processed by Luminess, 75001 PARIS (FR)

Description

TECHNICAL FIELD OF THE INVENTION

[0001] The present invention generally relates to the field of waste delivery.

[0002] More particularly, the present invention concerns an electronic system to control the access of a user to a waste container and waste container thereof.

PRIOR ART

[0003] It is known to use microcontroller electronic boards to control the access to a waste container, by means of electronic keys (for example, RFID or NFC tags) adapted to unlock the opening of a lock of the container.

[0004] The Applicant has observed that the use of a microcontroller-based architecture has the following disadvantages:

- It is not very flexible when adding a new functionality associated with the control of the access of users to the waste container (such as for example adding a new user for the controlled access through authentication to open the lid of the waste container) or when modifying an already existing functionality (such as modifying the access rights of an already registered user);
- It is not very flexible when adding a new user interface (such as for example a new type of tag reader) or when modifying an already existing interface;
- It is not very flexible when adding a new hardware peripheral for connection to a new external device, both in the case of a short-distance radio connection and in the case of a medium-long-distance connection;
- It is not very flexible with regards to software development.

SUMMARY OF THE INVENTION

[0005] The present invention concerns an electronic system to control the access to a waste container as defined in the appended claim 1 and by its preferred embodiments described in the dependent claims 2 to 10.

[0006] The Applicant has perceived that the electronic system according to the present invention has the following advantages:

- it allows to easily add a new functionality associated with the control of the access of users to the waste container (such as for example adding a user for the authenticated access to open the lid of the waste container) or easily modify an already existing functionality (such as modifying the access rights of an already registered user), as an update of the software program implementing the addition or modification of the functionality of interest is sufficient;
- it allows to easily add a new user interface (such as for example a new type of tag reader) or modify an already existing interface, by using a new driver of the operating system and/or of a software library provided by the manufacturer of the user interface and compatible with the operating system itself;
- it allows to easily add a new hardware peripheral for connection with a new external short/medium/long-distance device, by using a new driver of the operating system and/or by using a software library provided by the manufacturer of the device itself and compatible with the operating system itself;
- it allows to increase the stability over time of the high-level application software;
- it has a sufficiently low electrical power consumption such that it can operate supplied by a battery for an extended period of time, possibly without requiring the battery to be replaced for the entire life of the waste container;
- it implements a strategy to exploit a photovoltaic panel, also compatible with diffused/indirect light through a suitable electrical interfacing;
- it allows switching from a stand-by operating state to an active operating state with a sufficiently low switching time, such that it is not perceived by the user;
- the number of maintenance operations necessary to replace the power supply battery that has discharged is reduced (at most reduced to zero).

[0007] It is also an object of the present invention a waste container, wherein the waste container is defined in the appended claim 11 and in the preferred embodiment described in the dependent claim 12.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Additional features and advantages of the invention will become more apparent from the description which follows of a preferred embodiment and the variants thereof, provided by way of example with reference to the appended drawings, in which:

- Figure 1 shows a block diagram of an electronic system to control the access to a waste container according to the invention;
- Figure 2 shows a diagram of a layered architecture implementing the electronic system of the invention;
- Figure 3 shows a waste container according to the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0009] It should be observed that, in the following description, identical or analogous blocks, components or modules are indicated in the figures with the same numerical references, even if they are shown in different embodiments of the invention.

[0010] With reference to Figure 1, it shows an electronic system 1 to control the access to a waste container according to the invention.

[0011] The electronic system 1 is positioned at least partly inside the waste container, in particular in a suitable housing inside the waste container.

[0012] The electronic system 1 has the function of exposing methods of different types for interfacing with a user, such as for example allowing the delivery of the waste within the volume of the container 1 by a citizen.

[0013] Preferably, the electronic system 1 has the function of communicating autonomously with a remote monitoring system, so as to guarantee remote diagnostics/control and at the same time convey the data collected on site and use them to provide other types of functionalities that can optimize the waste collection cycle itself, also communicating directly with the information system of the waste management company.

[0014] The electronic system 1 makes it possible to make the municipal waste collection process more efficient, safe and efficient, from the individual delivery of the citizen up to the management of data acquired on site, as well as the management of the fleet of waste containers provided with the electronic system 1.

[0015] The electronic system 1 comprises a Central Processing Unit 2, a generator 12 of a clock signal S_clk, a non-volatile memory 4, a volatile-type central memory 3, one or more electrical connectors 9-1, 9-2, 9-3 and a power supply battery 11.

[0016] The clock signal generator 12, the non-volatile memory 4, the volatile-type central memory 3, the electrical connectors 9-1, 9-2, 9-3 and the power supply battery 11 are electrically connected to the Central Processing Unit 2 by means of respective wired electrical connections.

[0017] The electronic system 1 can be powered, alternatively:

- only by the power supply battery 11;
- only by a power supply network;
- only by a photovoltaic panel;
- both by the power supply battery 11 and by the photovoltaic panel;
- by the power supply battery 11 recharged by the photovoltaic panel;
- both by the power supply network and by the power supply battery (in the case in which the power supply network is not available).

[0018] The power supply battery 11 has the function of powering the electrical and electronic components of the electronic system 1, in particular the Central Processing Unit 2, the clock signal generator 12, the non-volatile memory 4 and the central memory 3.

[0019] The central memory 3, the non-volatile memory 4 and the clock signal generator 12 are electrically connected to the Central Processing Unit 2, by means of wired connections (for example, suitable metal tracks of a printed circuit board).

[0020] The central memory 3 is a random access memory (e.g., of the SDRAM type).

[0021] The central memory 3 has the function of storing the object code of the operating system and of a software program when it is executed by means of the Central Processing Unit 2.

[0022] In addition, the central memory 3 has the function of storing the data of the operating system and of the software programs used and being run.

[0023] The software program comprises a plurality of code portions, each of which performs a particular functionality associated with the delivery of the waste in the container, such as for example:

- authentication of the user to verify whether he is authorized to deliver waste into the waste container, in order to unlock (or keep locked) an electro-mechanical lock that allows the opening (or prevents the opening) of a lid of the waste container;
- control of a user's rights to access the container by means of a comparison with a whitelist (or blacklist) of users, in order to unlock (or keep locked) the electro-mechanical lock;
- control of a user's rights to access the container by evaluating other parameters associated with the user, such as for example based on the municipality or the area of residence and on the positioning of the container, in order to unlock (or keep locked) the electro-mechanical lock.

[0024] In addition, the central memory 3 has the function of storing the object code of an operating system when it is executed by means of the Central Processing Unit 2, as will be explained in more detail later.

[0025] The non-volatile memory 4 has the function of storing the object code of the operating system.

[0026] The Central Processing Unit 2 has the function of executing the operating system and a software program that executes one or more functionalities associated with the delivery of waste in the waste container in which the electronic system 1 is mounted.

[0027] The Central Processing Unit 2 is implemented with a processor or a microprocessor, for example NXP of the i.MX 8M family.

[0028] The term "operating system" means a software program that has at least the following functions:

- to enable the execution of a software program that executes one or more functionalities associated with the delivery of the waste;
- for the execution-enabled software program, to provide a communication interface with a short-distance wireless signal transceiver and provide a further communication interface with the electro-mechanical lock of the waste container;
- for the execution-enabled software program, to pro-

vide a communication interface with other units of the electronic system 1 and/or with peripherals external to it;

- to manage the allocation of space in the central memory 3 to store the object code containing the instructions for the execution of the software program and to store the data of the program during its execution.

[0029] In addition, the operating system has the function of managing the hardware peripherals, ensuring a homogeneity of interaction.

[0030] The operating system is for example Linux and similar (Debian, Fedora, RedHat, CentOS) or Windows Embedded Compact.

[0031] The use of a general operating system running on a Central Processing Unit has the advantage of allowing greater flexibility than an architecture using a microcontroller, because it is possible to develop and add a new functionality to the electronic system 1 (or modify an already existing functionality) by means of an update of the software program authenticating the user: this is achieved easily and quickly, since the software code is written using standard programming languages (for example, C or C++), which are supported by many compilers and can be executred on different operating systems without requiring substantial changes to the code.

[0032] In addition, a general operating system can use a multitude of application libraries available for the different functionalities and can use a wide availability of standard drivers already included in the kernel of the operating system or add non-standard drivers if compatible with the operating system in question, in order to interface the operating system with new hardware peripherals.

[0033] In fact, device manufacturers (for example, a tag reader or communication device) are encouraged to make available software libraries that facilitate the interfacing and the use of their devices by user applications and this is all the more true the more the library can be provided to work within a widespread operating system (eg: Linux, Android) which, de facto, makes the interaction with a variety of systems (processors, memories, peripherals, different) uniform.

[0034] Conversely, in a microcontroller architecture each microcontroller family has its own specific development environment and a limited number of libraries and also in some cases it is necessary to develop new drivers when a new peripheral is added; in some cases it is necessary to use an architecture with a plurality of microcontrollers in which each peripheral is managed by a respective microcontroller, thus increasing the complexity, times and cost of the overall architecture.

[0035] In general, a device manufacturer has much more difficulty in making software libraries available for interfacing them to microcontroller-based systems because of the enormous variability and incompatibility of the characteristics of the microcontrollers. In fact, in microcontroller-based systems there is typically no operating system that decouples the mode of interfacing with the environment in which the programs run (computational, storage resources and peripherals), from the specific characteristics of the same (type of processor, memory and peripherals). Some embedded operating systems consist of software modules (e.g. libraries) integrated within the single running application program and provide some functionalities that are typical of real operating systems (e.g. event management from interrupt peripherals): however, these are not real operating systems, which for example run independently of the execution of one or more application programs and, consequently to the limits of the microcontroller architectures (e.g. lack of memory virtualization mechanisms), they are not able to realize memory protection mechanisms between several application programs in a consolidated way.

[0036] Advantageously, the electronic system 1 is such to operate according to two operating modes:

- an active mode, in which the Central Processing Unit 2 is such to operate in order to execute the software program associated with the control of user access to the waste container;
- a stand-by mode ("deep sleep"), in which the Central Processing Unit 2 is such to deactivate the operation of at least a part of the combinational and sequential logic circuits implementing the Central Processing Unit 2, for example by suitably interrupting the power supply and/or by disabling the clock signal of the sequential circuits.

[0037] The stand-by mode is activated when the user does not interact with the waste container (and thus with the electronic system 1), whereas the electronic system 1 switches from the stand-by mode to the active mode when the user interacts with the waste container (and thus with the electronic system 1), for example for the delivery of waste in the container.

[0038] Therefore in the stand-by mode the electrical power consumption of the electronic system 1 is minimized, thus increasing the life of the battery 11 powering the electronic components of the electronic system 1.

[0039] The electronic system 1 is such to switch between the stand-by mode and the active mode, in the case where the electronic system 1 is such to receive an activation signal from a unit, sensor or hardware peripheral connected to the Central Processing Unit 2: in this case, for example, a hardware interrupt signal is generated by the unit, sensor or hardware peripheral, then the interrupt signal is received by the Central Processing Unit 2 which switches from the stand-by mode to the active mode, in order to execute the software program that takes as input the signal generated by the unit, sensor or hardware peripheral that has awakened the Central Processing Unit 2.

[0040] Using a processor or microprocessor allows to have a switching time between the stand-by mode and the active mode that is low enough that it is not perceived by the user.

[0041] For example, the switching time of the electronic system 1 between the stand-by mode and the active mode is equal to about 1 second.

[0042] More generally, the reaction time of the electronic system 1 towards the user is of the same order of magnitude as the one that one would have using a microcontroller architecture.

[0043] For example, the Central Processing Unit 2 switches from the stand-by mode to the active mode in case one or more of the following events takes place:

- coupling of an electronic key (e.g. NFC type) or of a mobile electronic device (e.g. with NFC interface) with an NFC type identification reader unit 20;
- pressing a button of the electronic system 1 by the user;
- detection of the presence of a person in proximity to the waste container, by means of a proximity sensor 21, as will be illustrated in more detail below;
- coupling of a user's mobile electronic device with a first short-distance wireless signal transceiver 5 (e.g. Bluetooth Low Energy type) or with a second short-distance wireless signal transceiver 6 (e.g. Wi-Fi or LoRa type);
- detection of a displacement of the waste container, by means of an inertial sensor 9, as will be illustrated in more detail below.

[0044] The use of a microprocessor architecture and operating system is more flexible from the point of view of programming and ease of implementation of new functionalities; on the other hand, a microprocessor architecture and operating system increases electrical energy consumption due to the size of the memory used and of the frequency of the microprocessor which cannot be too low.

[0045] Therefore the use of a microprocessor architecture and operating system in a waste container presents problems due to the high consumption of electrical energy.

[0046] The most important aspect to manage is the robustness and the efficiency of the energy department, whether batteries for the power supply of the system or other power supply sources are used.

[0047] In fact, if batteries are used to supply a microprocessor-based system, the duration of the latter is greatly reduced compared to those of a microcontroller architecture (it ranges from a duration of a few months for microcontroller devices, to a duration of 1-2 weeks for microprocessor architectures): energy management is thus an extremely critical element.

[0048] In order to be able to use architectures of this type operationally, it is thus necessary to implement a part of the system dedicated to energy balance.

[0049] In particular, at least two solutions are possible:

1) to use microprocessors that can operate by alternating the stand-by modes to the active modes: in this way the average consumption is significantly reduced. It is useful to note that, since there is a need to have a rapid interaction with the user (for example on the occasion of the delivery of waste), the electronic system 1 cannot be completely switched off and then restarted (as can be done with a microcontroller): only the use of the stand-by modes are compatible with the awakening times of the application, clearly in the face of higher consumption than those in the (completely) switched off state. In any case, with the application and the integration of the energy management policies in the main software, 1-2 months are reached without having to replace the battery;

2) to use an additional energy storage module (for example, one or more photovoltaic panels) in order to recharge the rechargeable power supply battery.

[0050] Advantageously, the operating system executed by the Central Processing Unit 2 has the further function of managing a virtual memory simulating (by means of a combination of hardware and software) a central memory space 3 by making sure that the memory available for the execution of a software program is greater than the memory physically available in the central memory 3.

[0051] For this purpose, the operating system executed on the Central Processing Unit 2 comprises portions of software code managing the mapping between a virtual memory space and the physical memory space actually assigned to the software program in question, so that the central memory 3 appears to the running software program as a contiguous address space. Furthermore, the use of the virtual memory allows to guarantee the protection (i.e. the separation) of the memory space allocated for a program with respect to other programs and the protection of the memory space allocated for the operating system, and also to guarantee that the memory part allocated for the object code of a software program is not also used to store the data on which the same program operates.

[0052] In particular, the memory space allocated in the volatile memory 3 for the object code and data of the user authentication program is separated from the memory space allocated for the object code and the data of the operating system, thus preventing a malfunction of the authentication program from being able to compromise the operation of the operating system, protecting the operating system in case of an instability thereof or in case of a cyber attack.

[0053] In particular, in the case in which the space of the central memory 3 is not sufficient for the execution of the software programs, the operating system manages the virtual memory in the following way:

- portions of the object code and data of the software program (for example, the authentication program) are temporarily saved in the non-volatile memory 4 and space in the central memory 3 is freed;

- when it is necessary to execute such portions of code or access such data, they are restored to volatile memory 3.

[0054] For example, the following events trigger the recovery of the portions of the object code of the authentication program from the non-volatile memory 4 to the central memory 3:

- coupling of an electronic key (e.g. NFC type) or of a mobile electronic device (e.g. with NFC interface) with the NFC type identification reader unit 20;
- pressing a button of the electronic system 1 by the user;
- detection of the presence of a person in proximity to the waste container, by means of the proximity sensor 21;
- coupling of a user's mobile electronic device with the first short-distance wireless signal transceiver 5 (e.g. of Bluetooth Low Energy type) or with the second short-distance wireless signal transceiver 6 (e.g. of Wi-Fi type).

[0055] The use of the virtual memory is possible because a complete operating system is used that can be executed by means of a microprocessor (i.e. the Central Processing Unit 2); otherwise, in the solutions according to the prior art a micro-controller programmed directly (bare metal) or running an Operating System, for example in Real time (Real-time OS), which does not have the virtual memory management function is used.

[0056] Preferably, the non-volatile memory 4 has the further function of storing alarms generated by the electronic system 1, such as for example an alarm message indicative of the overturning of the waste container, an alarm indicative of the presence of smoke and/or fire inside the waste container, an alert message indicative of reaching a waste filling level greater than a defined threshold value (for example, comprised between 80 and 90%), an alarm message caused by the door that has not been shut after the delivery (e.g.: jammed), a message indicating that the lock of the lid has not moved despite receiving an open/close command.

[0057] In particular, the Central Processing Unit 2 comprises a Arithmetic Logic Unit, a Control Unit connected with the Arithmetic Logic Unit and a plurality of internal registers connected with the Arithmetic Logic Unit and with the Control Unit.

[0058] The Arithmetic Logic Unit comprises a plurality of logic ports receiving as input the data stored in at least part of the plurality of registers and receive as input at least one control signal generated by the Control Unit, then said plurality of logic ports executes suitable logic and arithmetic operations in order to execute the object code of the operating system and the object code of the software programs, then generate as output processed data that are temporarily stored in at least part of the plurality of internal registers or are stored in the central memory 3.

[0059] The electrical connectors 9-1, 9-2, 9-3 have the function of connecting three devices external to the electronic system 1 which can be of the electronic or electromechanical type, as it will be explained in more detail below.

[0060] The electronic system 1 is such to implement a user authentication functionality by means of a software program, which consists of carrying out an authentication of a user (for example, a citizen) to verify whether he is authorized to deliver waste into the waste container, in order to allow the unlocking or locking of an electro-mechanical lock controlling the closing and opening of a lid of the waste container.

[0061] The electronic system 1 further comprises a short-distance wireless signal transceiver, which can be realized with an identifier reading unit 20 or with a short-distance wireless signal transceiver 5, 6 or 7, which will be illustrated in more detail below.

[0062] Therefore according to a first embodiment, the electronic system 1 further comprises the identifier reading unit 20 and the connector 9-1 is electrically connected to an input terminal of an electro-mechanical lock mounted inside the waste container; moreover the central memory 3 is configured to store the object code of the running authentication software program performing the authentication of the user and verifies whether he is authorized to deliver the waste in general and/or to deliver the waste in a particular container.

[0063] The identifier reading unit 20 is electrically connected to the Central Processing Unit 2 by means of wired connections and is powered by the battery 11, by the power supply network, by a photovoltaic panel or by a combination thereof.

[0064] The identifier reading unit 20 is configured to receive a first short-distance wireless signal S1_sd carrying a user identifier comprising information uniquely identifying a user of the waste delivery service.

[0065] Further, the identifier reading unit 20 is configured to generate a reading signal S_tg carrying the value of the user identifier.

[0066] The user identifier comprises for example an alphanumeric string uniquely associated with a user (i.e. it is a unique code or identifier), which is therefore different among several users.

[0067] The first short-distance wireless signal S1_sd is generated by a mobile electronic device external to the electronic system 1, such as for example a smartphone, a tablet or a laptop computer, which are provided with a suitable interface adapted to communicate with the identifier reading unit 20.

[0068] The identifier reading unit 20 transmits the reading signal S_tg towards the Central Processing Unit 2 by means of a communication interface provided by the operating system executed on the Central Processing Unit 2.

[0069] Preferably, the user identifier comprises a first field containing the user's unique identifier and comprises a second field containing information associated with the user himself, such as for example his municipality of residence or his Region of residence.

[0070] The user identifier is for example contained in an electronic tag associated with the user, which can for example be stored inside an RFID or NFC tag, which contains a memory having a portion that can be written only once by the manufacturer to configure the value of a unique code or identifier of the user: in this case the identifier reading unit 20 is an NFC or RFID type tag reader that is received by means of an external electronic device that the user places in proximity to the identifier reading unit 20.

[0071] Furthermore, according to said first embodiment, the Central Processing Unit 2 is configured to execute, by means of the Arithmetic Logic Unit, of the Control Unit and of the plurality of internal registers, the instructions of the object code of the software program performing the authentication of the user to verify whether he is authorized to deliver the waste into the waste container, in particular by means of a verification of the validity of at least part of the user identifier.

[0072] Even more particularly, the Central Processing Unit 2 is configured to receive (from the identifier reading unit 20) the identifier reading signal S_tg indicative of the value of the user identifier, is configured to perform the authentication of the user to verify whether he is authorized to deliver waste into the waste container by means of a verification of the validity of the content of the user identifier that uniquely identifies the user, and is configured to generate, as a function of the outcome of said validity verification, a driving signal S_drv to lock or unlock an electro-mechanical lock of the waste container:

- in the case in which the user is authorized to deliver waste into the waste container, the Central Processing Unit generates the driving signal S_drv commanding the unlocking of an electro-mechanical lock of the waste container, thus allowing the opening of the lid thereof and therefore allowing the delivery of waste by the user;
- in the case in which the user is not authorized to deliver waste into the waste container, the Central Processing Unit 2 generates the driving signal S_drv commanding the locking of the electro-mechanical lock of the waste container, thus preventing the opening of the lid thereof and therefore preventing the delivery of waste by the user.

[0073] The term "validity" of the content of the user identifier that uniquely identifies the user (i.e. the unique identifier) means to verify that this comprises data uniquely associated with a waste delivery service and also to verify that said content of the user identifier (i.e. the unique identifier) is authentic, i.e. it has not subsequently been modified or duplicated by unauthorized persons.

[0074] The verification of the validity of the unique identifier of the user is carried out by means of a predefined mathematical function (for example, a mathematical algorithm) that takes as input at least part of the value of the user identifier and generates as output a calculated value by means of said function applied to said at least part of the value of the user identifier, then it is verified whether the calculated value is equal to an expected value or whether the calculated value respects a predefined mathematical rule.

[0075] The expected value may be predefined, i.e. it is known to the electronic system 1 in advance as it has been previously configured under safe conditions; alternatively, the expected value is contained within a field of the user identifier (separated from the field containing the information uniquely identifying the user) and is then received by the electronic system by means of the reading signal S_tg generated by the read unit 20.

[0076] For example, the mathematical function is a hash function receiving as input the field of the user identifier that contains the information uniquely identifying the user (i.e. the unique identifier) and generates therefrom as output an alphanumeric string of predefined length, then it is verified (by means of the Central Processing Unit 2) if at least part of said calculated alphanumeric string is equal to a predefined expected hash value or contained within a field of the same user identifier received.

[0077] Another example is to use a user identifier comprising a first field that contains information uniquely identifying the user (i.e. the unique identifier) and a second field that contains a checksum.

[0078] In this example the Central Processing Unit 2 receives (by means of the reading unit 20) the user identifier, extracts therefrom the first field and the second field containing the checksum, then it calculates a checksum as a function of the value of the first field, and finally it performs the comparison between the value of the calculated checksum and the value of the checksum received in the second field:

- in the case in which the values of the two checksum are equal, it means that the user identifier is valid, therefore the Central Processing Unit 2 generates the driving signal S_drv that unlocks the electro-mechanical lock, thus allowing the user to open the lid of the container and deliver the waste inside it;
- in the case in which the values of the two checksum are different, it means that the user identifier is invalid, therefore the Central Processing Unit 2 generates the driving signal S_drv that keeps the electro-mechanical lock locked (or simply keeps the value of the driving signal S_drv unchanged if the electro-mechanical lock is already closed), thus preventing the user from opening the lid of the container and thus preventing him from delivering the waste.

[0079] Note that the authentication of the user to verify whether he is authorized to deliver the waste is carried out by means of a verification of the validity of the first field of the read user identifier that does not require a storage of user access rights in the non-volatile memory 4 of the electronic system 1: in this way the security of the electronic system 1 is increased, since in the event of break-in of the electronic system 1 by malicious persons, they have no available sensitive data of the users.

[0080] According to another preferred embodiment, it is used an encryption of at least part of the value of the user identifier, in order to protect said part in the event of interception by malicious persons, for example in case of theft of the electronic tag storing the value of the user identifier or to make it very difficult to duplicate the user identifier itself.

[0081] For example, it is performed encryption of the writable information content (i.e. the second field) of an electronic tag (e.g., an NFC/RFID tag) containing a first (non-writable) field containing information to identify the user, using for example an asymmetric key encryption (e.g., RSA): a private key k1 is used when preparing the TAG (formatting) and a public key k2 is known to the authentication software program executed on the Central Processing Unit 2 and is used by the program itself during execution. In this case the user identification data (in particular the data contained in the second field) are encrypted in the transmission with the private key k1 and decrypted in the reception with the public key k2, then the plain data are used according to the procedures described above.

[0082] In this case the access verification software program (executed on the Central Processing Unit 2) comprises a further portion of code implementing a functionality of decryption of at least part of the value of the encrypted user identifier received by means of the reading unit 20, thus generating the plain value of the user identifier.

[0083] In addition, the operating system executed on the Central Processing Unit 2 can make use of the stable, secure and performing implementation of known, shared and reliable encryption libraries and programs (e.g.: RSA, AES, etc.) since they are available to operate within the operating system itself, regardless of the purpose of the overall system. Conversely, the implementation of new cryptographic algorithms that were necessary in environments for which there are no consolidated and verified software libraries, such as microcontrollers, is not recommended because it can manifest security flaws related to the implementation itself.

[0084] According to said further embodiment, the Central Processing Unit 2 is configured to receive the reading signal S_tg indicative of the value of the encrypted user identifier, it is configured to decrypt the value of the encrypted user identifier and to generate therefrom the plain value of the user identifier.

[0085] In this case, the above considerations relating to the verification of the validity of the first field of the user identifier with a mathematical function (for example, hash) or checksum are similarly applicable considering the plain value of the first field of the user identifier, i.e. after the first field of the encrypted user identifier has been decrypted.

[0086] Advantageously, the non-volatile memory 4 is configured to further store a whitelist containing a list of the user identifiers associated with users who are authorized to deliver waste into the waste container in which the electronic system 1 is mounted: in this case the Central Processing Unit 2 is further configured to read, from the non-volatile memory 4, the list of the authorized user identifiers, is configured to compare the value of the read user identifier with respect to the list of the authorized user identifiers, and is configured to generate, as a function of the outcome of the verification and of the comparison, the driving signal S_drv to lock or unlock the electromechanical lock of the waste container.

[0087] In particular:

- in the case in which the Central Processing Unit 2 detects that the read user identifier is valid and also the value of the read user identifier is included in the list of the authorized user identifiers, the Central Processing Unit 2 generates the driving signal S_drv having a first value (for example, a high logical value) to unlock the opening of the electro-mechanical lock of the waste container;
- in the case in which the Central Processing Unit 2 detects that the read user identifier is valid and the value of the read user identifier is instead not included in the list of the authorized user identifiers (for example because the user is trying to deliver waste in a container positioned in an area different from the one assigned to him based on the residence address), the Central Processing Unit 2 generates the driving signal S_drv having a second value (for example, a low logical value) to lock the opening of the electro-mechanical lock of the waste container;
- in the case in which the Central Processing Unit 2 detects that the read user identifier is not valid or that the value of the read user identifier is not included in the list of the authorized user identifiers, the Central Processing Unit 2 generates the driving signal S_drv having a second value (for example, a low logical value) to lock the opening of the electro-mechanical lock of the waste container.

[0088] Alternatively, the non-volatile memory 4 is configured to store a blacklist containing a list of the user identifiers associated with users who are not authorized to deliver waste into the waste container in which the electronic system 1 is mounted: the above considerations relating to the Central Processing Unit 2 for the whitelist apply similarly to the blacklist, with the difference that the opening of the lock is locked in the case in which the user identifier is included in the blacklist.

[0089] Preferably, time and/or position rules are defined based on which a user can deliver household waste only in the containers that are positioned within a certain distance from his home, or only in certain time slots (for example, only between 9:00 p.m. and 6:00 a.m.).

[0090] According to a second embodiment, the electronic system 1 does not necessarily comprise the identifier reading unit 20 and it further comprises a short-distance signal transceiver 5, 6 or 7 having the function of receiving, from a mobile electronic device external to the electronic system 1, an authenticated command indicative of an authorization granted to the user for the delivery of waste in the container or indicative of an invalidity command indicative of an authorization denied to the user for the delivery of the waste in the container.

[0091] The external mobile electronic device may for example be a smartphone, a tablet or a portable personal computer provided with a respective short-distance signal transceiver capable of exchanging data with the short-distance signal transceiver 5, 6 or 7 of the electronic system 1.

[0092] The second embodiment differs from the first one in that the verification of the authentication of the user to deliver the waste is carried out on the mobile electronic device external to the electronic system 1, instead of in the electronic system 1.

[0093] In particular, based on said second embodiment, the short-distance signal transceiver of the mobile electronic device is configured to transmit, towards the electronic system 1, the authenticated command or the invalidity command; the Central Processing Unit 2 is configured to execute, by means of the Arithmetic Logic Unit, of the Control Unit and of the plurality of internal registers, the instructions of the object code of the software program performing the authentication of the user to verify whether he is authorized to deliver the waste into the waste container, in particular by means of the verification of reception of the authenticated command or of the invalidity command.

[0094] Finally, the Central Processing Unit 2 is configured to generate, as a function of the outcome of said reception verification, a driving signal S_drv to lock or unlock an electro-mechanical lock of the waste container:

- in the case in which the authenticated command representative of an authorization granted to the user for the delivery of waste into the waste container is received, the Central Processing Unit generates the driving signal S_drv commanding the unlocking of an electro-mechanical lock of the waste container, thus allowing the opening of the lid thereof and therefore allowing the delivery of waste by the user;
- in the case in which the invalidity command representative of an authorization denied to the user for the delivery of waste into the waste container is received, the Central Processing Unit 2 generates the driving signal S_drv that commands the locking of the electro-mechanical lock of the waste container (or simply keeps the value of the driving signal S_drv unchanged if the lock is already closed), thus preventing the opening of the lid thereof and therefore preventing the delivery of waste by the user.

[0095] According to an embodiment of the invention, the Central Processing Unit 2, the clock signal generator, the volatile central memory 3, the non-volatile memory 4 and the battery 11 are mounted on a first printed circuit board 1-1, while the identifier reading unit 20 is mounted on a second printed circuit board 2-2 which is separated from the first board 1-1, wherein the first board 1-1 is electrically connected to the second board 1-2 by means of suitable electrical connections 1-3.

[0096] Therefore in this case the clock signal generator 12, the non-volatile memory 4, the volatile-type central memory 3, the electrical connectors 9-1, 9-2 and the power supply battery 11 are electrically connected to the Central Processing Unit 2 by means of respective metal tracks of the first board 1-1; moreover also the identifier reading unit 20 is electrically connected to the Central Processing Unit 2 by means of metal tracks of the first board 1-1 and of the second board 1-2 and of a suitable electrical connection between the two plates 1-1, 1-2.

[0097] The use of a second printed circuit board 1-2 separated from the first printed circuit board 1-1 has the advantage of providing greater flexibility to the electronic system 1, in case of modification of the user authentication method: in fact in the case in which it is necessary to replace the identifier reading unit 20 with another reading unit of different type (or with other peripherals), it is sufficient to replace only the second printed circuit board 1-2, while the hardware of the first printed circuit board 1-1 remains unchanged.

[0098] The first printed circuit board 1-1 can be made for example with the System-on-Module SAMA series from the company Microchip Technology Inc. or with System-on-Chip from the company Broadcom BCM series.

[0099] According to another embodiment, the identifier reading unit 20 is mounted on the same printed circuit board on which the Central Processing Unit 2, the clock signal generator, the volatile central memory 3, the non-volatile memory 4 and the battery 11 are mounted, therefore there is a single printed circuit board.

[0100] Advantageously, the Central Processing Unit 2 is able to operate with harvested energy, that is, capturing energy from the environment (for example, from the electromagnetic radiations) and converting it into electrical energy used to supply the Central Processing Unit 2.

[0101] Preferably, the electronic system 1 further comprises the first short-distance wireless signal transceiver 5 (e.g. Bluetooth Low Energy type) and/or the second short-distance wireless signal transceiver 6 (e.g. Wi-Fi or LoRa type) for connecting the electronic system 1 with an external electronic device placed in the vicinity of the waste container, such as for example a smartphone, a tablet or a portable personal computer.

[0102] The first transceiver 5 and the second transceiver 6 are supplied by the battery 11 and/or by the power grid and/or by an electromagnetic radiation source (for example, one or more photovoltaic panels) and are connected to the Central Processing Unit 2, by means of a respective wired connection.

[0103] In this case the operating system has the function of providing a further communication interface with the first short-distance wireless signal transceiver 5 and/or a further communication interface with the second short-distance wireless signal transceiver 6.

[0104] By means of the first transceiver 5 and/or of the second transceiver 6 it is possible to authenticate the user to access the waste container with authentication methods other than the one used with the identifier reading unit 20.

[0105] In particular, the first transceiver 5 and/or the second transceiver 6 are used to perform the user authentication as illustrated above for the second embodiment, i.e. by receiving an authenticated command indicative of an authorization granted to the user for the delivery of waste in the container or indicative of an invalidity command indicative of an authorization denied to the user for the delivery of the waste in the container.

[0106] For example, the user is provided with a smartphone and executes a suitable software application that requires the access with an authentication to one or more factors (for example, username and password in the case of a single factor): after the user has been successfully authenticated by means of the application executed on the smartphone, the user can generate the authenticated command by selecting a suitable command in the application itself, then the smartphone transmits an authenticated command towards the first transceiver 5 or towards the second transceiver 6, thus allowing the unlocking of the electro-mechanical lock.

[0107] In addition, by means of the first transceiver 5 and/or of the second transceiver it is possible to perform the following functionalities:

- to send to the electronic system 1 configuration parameters for the operation thereof;
- to perform an update of the authentication software program and/or of the operating system;
- to exchange data with the electronic system for the maintenance or diagnostics thereof;
- to carry out the delivery operations or to receive linked information associated with the delivery itself (such as for example an indication to use an adjacent container bin based on the filling state or operation of the one with which one is interacting).

[0108] The presence of both the identifier reading unit 20 and of one or more transceivers 5, 6 allows to authenticate the users based on two or more authentication methods, even very different from each other, thus allowing to have an authentication redundancy in case of impossibility to use one of the authentication methods.

[0109] Preferably, the electronic system 1 further comprises a medium-long distance signal transceiver 7 (e.g. of GPRS type) for connecting the electronic system 1 with a remote monitoring system (e.g. waste collection service manager), via a medium-long distance telecommunications network.

[0110] The telecommunications network can be of a fixed type (e.g. Internet) and in this case the medium-long distance signal transceiver 7 is for example an Ethernet interface.

[0111] Alternatively, the telecommunications network can be of the radio-mobile type and in this case the medium-long distance signal transceiver 7 is for example of the 4G or 5G type.

[0112] Alternatively, the telecommunications network comprises a radio-mobile type access network and a fixed type telecommunications network (e.g., in fibre optics).

[0113] The medium-long-distance signal transceiver 7 is powered by the battery 11 and/or by the power grid and/or by an electromagnetic radiation source (e.g. one or more photovoltaic panels) and is electrically connected to the Central Processing Unit 2, by means of a wired connection.

[0114] In this case the operating system has the function of providing a further communication interface with the medium-long distance wireless signal transceiver 7.

[0115] In particular, by means of the transceiver 7 it is possible to perform the following functionalities:

- to transmit towards the remote monitoring system messages indicative of the waste deliveries made by the users (such as for example the date of the delivery) and operating information (such as for example, geographical location of the waste container, state of charge of the battery 11);
- to transmit alarm messages towards the remote monitoring system, such as for example a container overturning, a block of the lock of the lid, a fire in the container, a too high filling level, abnormal geographical displacement of the waste container.

[0116] Preferably, the electronic system 1 further comprises (possibly in addition to the medium-long-distance signal transceiver 7) a localization unit 8 configured to generate a localization signal S_lcz indicative of the geographical position on Earth of the electronic system 1.

[0117] The localization unit may be of satellite type (e.g. GPS) or of terrestrial type (e.g. exploiting the medium-long distance signal transceiver 7 and the cell subdivision of the mobile radio network), or a combination thereof.

[0118] The localization unit 8 is powered by the battery 11 and/or by the power grid and/or by an electromagnetic radiation source (e.g. one or more photovoltaic panels) and it is electrically connected to the Central Processing Unit 2, by means of a wired connection.

[0119] In this case the operating system has the function of providing a further communication interface with the localization unit 8.

[0120] In particular, the Central Processing Unit 2 is configured to receive (from the localization unit 8) the localization signal S_lcz indicative of the geographical position on Earth of the electronic system 1 (and therefore of the waste container in which it is mounted), and is configured to carry out suitable processings of the geographical position on Earth of the electronic system 1 (and therefore of the waste container in which it is mounted).

[0121] Advantageously, the Central Processing Unit 2 is configured to forward to the medium-long-distance signal transceiver 7 information indicative of the geographical position on Earth of the electronic system 1 (and therefore of the waste container in which it is mounted).

[0122] In this case the medium-long distance signal transceiver 7 is configured to receive the information indicative of the geographical position on Earth of the electronic system 1 (and therefore of the waste container in which it is mounted), and is configured to transmit, towards the remote monitoring system passing through the telecommunications network, a message carrying the information indicative of the geographical position on Earth of the electronic system 1 (and therefore of the waste container in which it is mounted).

[0123] The remote monitoring system is such that it receives the information indicative of the geographical position on Earth of the electronic system 1 (and therefore of the waste container in which it is mounted), then this information is used by the remote monitoring system to perform one or more of the following functionalities:

- to map the geographical position on the territory of a plurality of waste containers, for example a homogeneous distribution in a given area;
- to optimise the emptying path of a plurality of containers in a given area, as a function of the filling level;
- to plan the emptying intervals of a plurality of containers in a given area;
- to lock the opening of a container, for example for the replacement thereof due to damages or due to the need to withdraw the container;
- transmission of warning messages for the users as a function of the position of the container, by means of a screen 10 of the electronic system 1 ;
- to detect an unauthorized movement of a waste container;
- to notify the users the availability of one or more waste containers, in order to encourage them to use the available containers.

[0124] Preferably, the electronic system 1 further comprises an inertial sensor 9 (commonly indicated with IMU), in order to detect the movement of the waste container in which the electronic system 1 is housed, such as for example an overturning of the waste container or a lifting of the container due to emptying by authorized personnel.

[0125] The inertial sensor 9 is an electronic device comprising one or more accelerometers and one or more gyroscopes, and it is such to generate a movement signal S_imu indicative of the values of the linear acceleration and of the rotation in the space of the electronic system 1 (and therefore of the waste container in which it is housed).

[0126] The inertial sensor 9 is powered by the battery 11 and/or by the power grid and/or by an electromagnetic radiation source (for example, one or more photovoltaic panels) and it is electrically connected to the Central Processing Unit 2, by means of a wired connection.

[0127] In particular, the inertial sensor 9 is mounted on the printed circuit plate 1-1 and thus the movement signal S_imu is indicative of the values of the linear acceleration and of the rotation of the printed circuit plate 1-1.

[0128] In this case the operating system has the function of providing a further communication interface with the inertial sensor 9.

[0129] The Central Processing Unit 2 is thus configured to receive the movement signal S_imu, it is configured to process the values of the linear acceleration and of the rotation in the space of the electronic system 1 (and thus of the waste container in which it is housed) and it is configured to generate a processed signal indicative of a displacement of the waste container, such as for example an overturning or a lifting.

[0130] Advantageously, the electronic system 1 further comprises a screen 10 having the function of displaying text messages and/or images to interact with the user, such as for example:

- to guide the user to use the electronic key or a smartphone for the delivery of waste;
- to generate warning messages in the case in which the user is not authorized to deliver the waste into the container;
- to warn the user in case of failure of the container and provide textual, graphic or sound indications of the position of other containers nearby.

[0131] Preferably, the screen 10 is of the touch type and it is configured to receive an access code to unlock the opening of the waste container, by typing the access code, by touching a virtual keyboard on the screen 10 or by displaying a QR code.

[0132] According to a third embodiment, the display 10 is configured to display a QR code to implement another method for enforcing the user's presence in front of the container downstream of the user's authentication, alternatively or in addition to the authentication methods of the first embodiment (identifier reading unit 20) and of the second embodiment (short distance wireless transceiver 5, 6).

[0133] In this case, the user is provided with a mobile electronic device (for example, a smartphone or tablet) with a camera and suitable software, which allow to acquire the QR code displayed on the screen 10.

[0134] The user then approaches the screen 10 and his presence is detected, for example by means of the proximity sensor: this activates the switching on of the screen 10 displaying the QR code and furthermore the Central Processing Unit 2 switches from the stand-by mode to the active one.

[0135] Subsequently, the user scans the QR code displayed on the screen 10 by means of the camera of his mobile electronic device and the user's access requirements are verified, wherein said verification can be carried out on the mobile electronic device itself or externally thereto, for example by means of a cloud service.

[0136] In case of positive verification, the mobile electronic device transmits towards the electronic system 1 the authenticated command, which is received by means of the transceiver 5 or 6, then the authenticated command is forwarded to the Central Processing Unit 2, which generates the driving signal S_drv to unlock the electro-mechanical lock, thus allowing the opening of the lid of the waste container.

[0137] Conversely, in case of negative verification, the mobile electronic device transmits towards the electronic system 1 the invalidity command, which is received by means of the transceiver 5 or 6, then the invalidity command is forwarded to the Central Processing Unit 2, which generates the driving signal S_drv to lock (or keep locked) the electro-mechanical lock, thus preventing the opening of the lid of the waste container.

[0138] The screen 10 is powered by the battery 11 and/or by the power grid and/or by an electromagnetic radiation source (for example, one or more photovoltaic panels) and it is electrically connected to the Central Processing Unit 2, by means of a wired connection.

[0139] In this case the operating system has the function of providing a further communication interface with the screen 10.

[0140] The Central Processing Unit 2 is thus configured to generate a driving signal S_dp of the screen 10, wherein said driving signal S_dp carries data representative of the text messages and/or images to be displayed on the screen 10.

[0141] In addition, the Central Processing Unit 2 is configured to receive the driving signal S_dp carrying the value of the access code to the waste container.

[0142] Preferably, the electronic system 1 further comprises a proximity sensor 21, in order to detect the presence of a user in the vicinity of the waste container.

[0143] The proximity sensor 21 is such to generate a vicinity signal S_prx indicative of the presence of a user positioned in proximity to the electronic system 1 (and therefore positioned in proximity to the waste container).

[0144] The proximity sensor 21 is powered by the battery 11 and/or by the power grid and/or by an electromagnetic radiation source (for example, one or more photovoltaic panels) and it is electrically connected to the Central Processing Unit 2, by means of a wired connection.

[0145] In particular, the proximity sensor 21 is mounted on the second printed circuit plate 2-2 and is electrically connected to the Central Processing Unit 2 by means of metal tracks of the first plate 1-1 and of the second plate 1-2 and of the electrical connection between the two plates 1-1, 1-2.

[0146] In this case the operating system has the function of providing a further communication interface with the proximity sensor 21.

[0147] The Central Processing Unit 2 is thus configured to receive the vicinity signal S_prx, and is configured to detect the presence or absence of a person positioned in proximity to the waste container on which the electronic system 1 is mounted.

[0148] In particular, the Central Processing Unit 2 is configured to receive the vicinity signal S_prx indicative of the presence of a person in proximity to the waste container, then the Central Processing Unit 2 switches from the stand-by mode to the active mode.

[0149] According to a preferred embodiment, the electronic system 1 further comprises a level sensor, in order to measure the filling level of the waste accumulated within the waste container.

[0150] The level sensor is such to generate a measurement signal indicative of the filling level of the waste accumulated within the container, expressed for example in centimetres.

[0151] In this case, the operating system has the function of providing a further communication interface with the level sensor.

[0152] The Central Processing Unit 2 is thus configured to receive the measurement signal indicative of the filling level of the waste accumulated within the container, it is configured to compare the value of the measurement signal with respect to a defined filling threshold value (for example, a value comprised between 70% and 90%), and it is configured to generate a filling alarm signal in the case in which the detected value of the measurement signal is greater than or equal to the filling threshold value.

[0153] Alternatively, the measured filling level value is transmitted (by means of the transceiver 7) to a remote server (e.g. a server of the manager of a remote monitoring system), which makes said comparison between the measured filling level value and a threshold value.

[0154] The alarm signal may be for example a textual or graphic message displayed on the screen 10, in which the message contains an indication to the user that it is not possible to deliver the waste into the container in question and invites the user to deliver the waste into one of the containers placed nearby.

[0155] The alarm signal can also be a sound signal generated by means of a miniaturized speaker mounted on the electronic board 1-1.

[0156] According to a variant, the Central Processing Unit 2 is configured to generate an alert signal in the case in which the filling level is comprised within a defined interval of alert values and an alarm signal in the case in which the filling level is greater than an alarm threshold equal to the extreme value greater than the defined range of values. For example, the alert value interval is comprised between 70% and 90% of the filling level of the waste container, and the alarm threshold value is equal to 90% of the filling level.

[0157] According to a preferred embodiment, the electronic system 1 further comprises a volumetric sensor to measure the filling level and the position of the waste accumulated within the waste container.

[0158] The above considerations relating to the level sensor are applicable similarly to the volumetric sensor and moreover the electronic system 1 can take advantage of the information relating to the position of the waste in the container, i.e. how they are arranged.

[0159] The electronic system 1 further comprises at least one photovoltaic panel configured to generate a direct current and voltage used to power the electronic and electrical components of the electronic system 1 (in particular, the Central Processing Unit 2), in addition to the power supply of the battery 11 and/or of the power grid.

[0160] In this case the electronic system 1 further comprises a circuit to manage the electrical energy flows of the battery 11, of the power grid and of the photovoltaic panel, thus the electronic and electric components of the electronic system 1 can be powered only by the battery 11, only by the power grid, only by the photovoltaic panel, or by the combination of the battery with the power grid, of the battery with the photovoltaic panel and of the power grid with the photovoltaic panel, or by the combination of the battery with the photovoltaic panel with the power grid.

[0161] The photovoltaic panel is suitably positioned on the waste container, for example it is fixed on a portion of the surface of the lid or it is fixed on a side wall of the container.

[0162] Preferably, the battery 11 is of the rechargeable type and the electronic system 1 further comprises an electrical connector to connect an external power supply source for recharging at least in part the battery 11: in this case the electronic system 1 comprises a charge management circuit having the function of carrying out an electronic control of the recharging of the battery 11.

[0163] Furthermore, in the case in which a photovoltaic panel is present, the battery 11 can be recharged by means of the electric current and voltage generated by means of the photovoltaic panel, i.e. by using the excess electric energy generated by the photovoltaic panel that is not used to power the electronic components of the electronic system 1.

[0164] It is known that a photovoltaic panel is designed for use in direct exposure to solar radiation, although with different inclinations, but not for operation in the absence of direct solar radiation, that is when only diffuse and indirect lighting is present.

[0165] According to the present invention, the photovoltaic panel is robustly fixed to the structure of the waste container and thus the photovoltaic panel follows the positioning of the waste container: this does not always allow to orient the photovoltaic panel in the best way, because it is possible that the waste container is constantly positioned in the shade of buildings, plants or other obstacles.

[0166] According to an embodiment of the invention, the first printed circuit board 1-1 comprises a portion dedicated to energy management, which allows to extract the maximum electrical energy from the at least one photovoltaic panel fixed to the waste container, both in case of direct irradiation condition, and in case of very low solar irradiation and/or low brightness condition.

[0167] In particular, the charge management circuit is connected in input with the output of the solar panel and with the output voltage of the rechargeable type battery 11, so that the components mounted on the first printed circuit board 1-1 can be powered only by the rechargeable battery 11, or only by the at least one photovoltaic panel, or only by the battery 11 which is actively being recharged by means of the at least one photovoltaic panel, or by means of the combination of the rechargeable battery 11 and of the at least one photovoltaic panel.

[0168] The Applicant carried out tests under conditions of indirect irradiation, using a photovoltaic panel designed to generate under direct irradiation conditions direct current of at least 800 mA (milli amps) in the active range [10 -12] Volts. The test showed that under conditions of indirect irradiation it was possible to generate a recharging current of the battery 11 of about 35 mA with a voltage of 6 Volts: this current and voltage value is sufficient to recharge the battery 11 when the electronic system 1 operates in the stand-by mode, which is the one in which the electronic system 1 is for most of the time, thus allowing to sufficiently recharge the battery 11 and thus greatly increasing the life time of the battery 11, i.e. without requiring the replacement thereof.

[0169] The Applicant carried out a second test under conditions of indirect irradiation, using a photovoltaic panel designed to generate under conditions of direct irradiation direct current of at least 800-900 mA (milli amps) at a voltage of 7 Volts (collected power about 6-7W). The test showed that under conditions of indirect irradiation it was possible to generate a recharging current of the battery 11 of about 30 mA with a voltage of 4.5 Volts (about 100mW): this current and voltage value is sufficient to recharge the battery 11 when the electronic system 1 operates in the stand-by mode, which is the one in which the electronic system 1 is for most of the time, thus allowing the battery 11 to be sufficiently recharged and thus greatly increasing the life time of the battery 11, i.e. without requiring the replacement thereof. It should also be added that in this embodiment it is possible to accumulate energy even by detecting voltages of 3.5V (about 50mW). These powers are extremely low when compared with those for the context of energy production, i.e. the context for which the photovoltaic panels are designed and produced, but they are very interesting for harvesting, since, given the reduced consumption of the system at stand-by (used for most of the time), they are sufficient for the average sustenance of the system and, with an indirect light easily obtainable under operating conditions, sufficient for recharging the battery 11.

[0170] With reference to Figure 2, it shows a diagram of a layered architecture implementing the electronic system 1 and the hardware peripherals connected thereto.

[0171] The purpose of the diagram of Figure 2 is to show how the software and the hardware implementing the electronic system 1 are organized.

[0172] The architecture comprises three layers:

- a hardware layer, which is the lowest one;
- a kernel layer of the operating system, which is the intermediate layer;
- a user layer, which is the highest one.

[0173] The hardware layer is implemented in hardware and it comprises the Central Processing Unit 2, the central memory 3 and one or more hardware peripherals indicated with the reference number 30.

[0174] The hardware peripherals 30 are components external to the electronic system 1, but they are connected thereto by means of wired connections between the connectors 9-1, 9-2 and the peripherals.

[0175] The hardware peripherals 30 may be mounted internally to the waste container or externally thereto, in the latter case for example by means of weather-resistant containers.

[0176] Some examples of hardware peripherals 30 that can be connected to the electronic system 1 are the following:

- the identifier reading unit 20;
- an electro-mechanical lock provided with an electric motor to actuate suitable pistons to unlock or lock the opening of the lid of the waste container;
- a sensor for detecting the filling level of the waste in the container, positioned inside the waste container;
- a fire sensor for detecting the presence of fire and/or smoke inside the container;
- a photovoltaic panel;
- sensors for detecting the opening or closing of the container or of a liquid discharge hole.

[0177] The kernel layer of the standard operating system is implemented in software.

[0178] The kernel of the operating system is suitably configured to provide support for hardware peripherals, by means of a plurality of drivers for interfacing one or more hardware peripherals external to the electronic system 1, wherein said drivers may be modules compiled together with the monolithic type kernel or may be binary files that are dynamically loaded by the hybrid type kernel.

[0179] The kernel of the operating system is updated when a new driver of a new peripheral for a monolithic kernel is added, thus ensuring maximum flexibility of the electronic system 1.

[0180] The user layer is also realized software and is in turn subdivided into two layers:

- libraries;
- high-level software layer.

[0181] The high-level software layer comprises the user programs, the software applications, and the system programs.

[0182] The libraries have the function of putting the operating system in communication with the user programs, the software applications and the system programs.

[0183] In particular, a software library of a hardware peripheral allows to provide the application with a simple-use and/or standard and/or high-level user interface for the same, for example by summing up and orchestrating over time more signals and activities of the peripheral so as to make available to the application program a functionality with a semantic level higher than that of the individual signals involved.

[0184] In other cases, the library plays the same role in a purely software context, making available computations at a high semantic or abstraction level (e.g.: operation of compressing an image according to the jpeg standard starting from a bitmap image), through a software function that specifies only two parameters: the memory areas of the bitmap image to be processed and that to be filled with the result of the compression thereof into jpeg.

[0185] User programs are software programs (executed by the Central Processing Unit 2) implementing functionalities of the electronic system 1 that are oriented to the delivery of waste by the user, such as for example:

- the control of the user access to open the container by means of one or more user authentication methods, as illustrated above for the first and second embodiments;
- the interaction with the user by means of text messages and/or images displayed on the screen 10 of the electronic system 1;
- interaction with the user by means of audio messages generated by means of a miniaturized loudspeaker of the electronic system 1;
- user interaction with the electro-mechanical lock;
- sending to the remote monitoring system information indicative of the waste deliveries of the user (such as for example the identity of the user who made the delivery, the date of delivery, the number of deliveries in a given period of time); sending to the remote monitoring system information indicative of the state of the waste container, such as for example its geographical location, the filling level of the waste.

[0186] Software applications are software programs (executed by the Central Processing Unit 2) for the operation and maintenance of the electronic system 1, such as for example:

- configuration of user access lists, such as a whitelist or blacklist;

- programming of the electronic system 1, such as for example update of the software program in case of addition of a new functionality associated with the delivery of waste of the user (or modification of an existing functionality) or update of the operating system or its configuration parameters, both locally and remotely;
- configuration of operating parameters of the various peripherals, such as for example for driving the servo motor of the lock, number of repeated measurements of the waste level, voltage thresholds of the photovoltaic panel and of the battery for the management of low consumption strategies;
- configuration of the application functionalities of the software program, such as for example internet addresses for the transmission of data to the service manager and for the transmission of telemetric monitoring data, setting of operating modes, availability for the delivery and timing of the same.

[0187] System programs are software programs (executed by the Central Processing Unit 2) implementing functionalities to interface the electronic system 1 with external systems, such as for example business process management software of a company (such as BPM/ERP), transmission of diagnostic and measurement data towards data analysis systems themselves, transmission of alarms generated by the electronic system 1 towards alarm analysis systems themselves.

[0188] In one embodiment in which the rechargeable type battery 11, at least one photovoltaic panel and the charge management circuit are present, the measurement of the accumulated current and of the voltage on the battery and of the photovoltaic panel is inserted into the software control of the operating system in order to be able to activate different energy saving strategies.

[0189] Therefore, in addition to an electronic control managing the recharging of the battery 11 by means of the at least one photovoltaic panel or the direct power supply of the components of the electronic board 1-1 by means of the at least one photovoltaic panel, there is also a software module executed on the Central Processing Unit 2 processing such data.

[0190] In particular:

- in the event of detection of insufficient electrical energy generated by the photovoltaic panel, by means of the software control an operating anomaly is detected with respect to an expected value of electrical energy from the photovoltaic panel, then an operating strategy of the electronic system 1 oriented to energy saving is activated, such as for example the activation of a switched off mode of the electronic system 1 during the night hours (in the switched off mode the lock can be maintained in the locked state thus preventing the opening of the lid of the container and the delivery of waste during night hours, or the lock can be maintained in the unlocked state thus allowing the opening of the lid and the delivery of waste during the night hours, as a function of the software configuration of the electronic system 1);
- in the event of restoration of sufficient electrical energy generated by the photovoltaic panel, by means of the software control the electronic system 1 switches automatically from the shutdown mode to the stand-by mode and possibly to the active mode;
- the electronic system transmits a notification of malfunction of the at least one photovoltaic panel to the remote monitoring system;
- a maintenance of the photovoltaic panel is carried out: when the maintenance has been carried out correctly, by means of the software control the electronic system 1 switches automatically from the shutdown mode to the stand-by mode and possibly to the active mode.

[0191] With reference to Figure 3, it shows a waste container 50 according to the invention.

[0192] It can be seen that the electronic system 1 and the electro-mechanical lock 30 are present, which are suitably fixed to the structure of the container 50.

[0193] It can also be noted that there is a photovoltaic panel 35 fixed on the upper surface of the container 50, or integrated within the upper portion of the structure (or casing) of the container 50.

[0194] Finally, it can be noted that the sensor 31 is present for measuring the filling level of the container 50.

Claims

1. Electronic system (1) to control the access of a user to a waste container, the system comprising a Central Processing Unit (2), a volatile central memory (3), a non-volatile memory (4), a short-distance wireless signal transceiver (20, 5, 6, 7), a photovoltaic panel, a circuit to manage electrical energy flows and a power supply battery comprising an output terminal adapted to generate a supply voltage of the volatile central memory, of the non-volatile memory and of the short-distance wireless signal transceiver (20, 5, 6, 7),

wherein the photovoltaic panel comprises an output terminal adapted to generate a direct current and voltage as a function of the intensity of solar radiation impinging on the surface of the photovoltaic panel,

wherein the volatile central memory, the non-volatile memory and the short-distance wireless transceiver are electrically connected to the Central Processing Unit, wherein the management circuit is connected in input with the output terminal of the battery and with the output terminal of the photovoltaic panel and comprises an output terminal adapted to generate a supply

voltage for the Central Processing Unit as a function of the output voltage of the battery and of the output terminal voltage of the photovoltaic panel,
the non-volatile memory being configured to store an object code of a software program and an object code of an operating system,
the central memory being configured to store the object code of the running operating system and the object code of the running software program and data of the software program,
wherein the Central Processing Unit is configured to execute the object code of the operating system,
the operating system being configured to:

- enable the execution of the software program and provide therefrom a communication interface with the short-distance wireless signal transceiver (20) and provide a further communication interface with an electro-mechanical lock of the waste container;
- manage a central memory allocation to store data and the object code containing instructions for the execution of the software program;

wherein the software program comprises a code portion configured to control the access to the waste container,
the short-distance wireless signal transceiver being configured to generate a signal indicative of the value of a user identifier, or indicative of an authenticated command representative of an authorization granted to the user for the delivery of waste in the container or an invalidity command representative of an authorization denied to the user for the delivery of waste in the container,
and wherein the Central Processing Unit is further configured to execute the object code of the software program and it is configured to:

- receive the signal (S_tg) indicative of the value of the user identifier or indicative of the authenticated command or the invalidity command;
- verify whether the user is authorized to deliver waste in the waste container, by means of a verification of the validity of at least part of said user identifier or by means of the verification of reception of said authenticated command or said invalidity command;
- generate, as a function of the outcome of said verification, a driving signal (S_drv) to lock or unlock the electro-mechanical lock of the waste container.

2. Electronic system according to claim 1, wherein the power supply battery is of the rechargeable type, and wherein the management circuit is further configured to receive the voltage of the output terminal of the photovoltaic panel and it is configured to at least partially recharge the battery as a function of the current flowing through the output terminal of the photovoltaic panel,
and wherein the management circuit is configured to power the Central Processing Unit:

- only as a function of the output voltage of the rechargeable battery;
- only as a function of the voltage of output terminal of the photovoltaic panel;
- as a function of both the output voltage of the rechargeable battery and of the voltage of the output terminal of the photovoltaic panel.

3. Electronic system according to claim 1 or 2, wherein the output terminal of the management circuit is further configured to power at least one of the central volatile memory (3), the non-volatile memory (4) and the short-distance wireless signal transceiver.

4. Electronic system according to any one of the preceding claims, wherein the short-distance wireless signal transceiver is an identifier reading unit (20) configured to generate a reading signal (S_tg) indicative of the value of the user identifier,
wherein the Central Processing Unit is configured to carry out said validity verification, alternatively, by means of:

- calculate, by means of a defined mathematical function, a value as a function of said at least part of the content of the user identifier, compare the calculated value with respect to an expected value defined or contained in another part of the user identifier received by means of the reading signal, and generate the driving signal of the electro-mechanical lock as a function of the outcome of said comparison, in particular the mathematical function is a hash function;
- calculate, by means of a defined mathematical function, a value as a function of at least part of the content of the user identifier, verify whether the calculated value complies with a defined mathematical rule and generate the driving signal of the electro-mechanical lock as a function of the outcome of said comparison;
- calculate a checksum as a function of the value of data contained in a first field of the received user identifier, compare the calculated value of the checksum with respect to a value contained in a second field of the received user identifier and generate the driving signal of the electro-mechanical lock as a function of the outcome of

said comparison.

5. Electronic system according to claim 4, wherein the software program further comprises a code portion configured to carry out a decryption of at least part of the value of an encrypted user identifier,

and wherein the Central Processing Unit is further configured to:

- receive the reading signal indicative of said at least part of the value of the encrypted user identifier;
- decrypt said at least part of the value of the encrypted user identifier and generate therefrom a plain value of the at least part of the user identifier;

and wherein said calculation of the mathematical function or checksum is carried out by taking the plain value of said part of the user identifier as input.

6. Electronic system according to any one of the preceding claims, wherein the short-distance wireless signal transceiver (5, 6) is configured to receive a short-distance wireless signal (S2_sd, S3_sd) carrying the authenticated command or the invalidity command,
wherein the Central Processing Unit is further configured to:

- receive the short-distance wireless signal (S2_sd, S3_sd) carrying the authenticated command or the invalidity command;
- verify whether the user is authorized to deliver waste in the waste container, by verifying reception of said authenticated command or said invalidity command;
- generate, as a function of the outcome of said verification, the driving signal (S_drv) to lock or unlock the electro-mechanical lock of the waste container.

7. Electronic system according to any one of the preceding claims, wherein the processing unit is further configured to:

- manage a virtual memory for the authentication software program;
- separate the memory space allocated in the volatile memory (3) for the object code and data of the authentication program with respect to the memory space allocated in the volatile memory (3) for the object code and data of the operating system.

8. Electronic system according to any one of the preceding claims, wherein the non-volatile memory (4) is configured to store an access list containing a list of user identifiers authorized or not authorized to deliver waste into the waste container,
the Central Processing Unit being further configured to:

- read, from the non-volatile memory (4), the list of user identifiers of the access list;
- compare the value of said at least part of the user identifier with respect to the list of user identifiers;
- generate, as a function of the outcome of said verification and of said comparison, a driving signal (S_drv) to lock or unlock the electro-mechanical lock of the waste container.

9. Electronic system according to any one of the claims 2 to 8, wherein the Central Processing Unit is configured to operate:

- in an active mode, in which the Central Processing Unit (2) is configured to execute the software program for controlling user access to the waste container;
- in a stand-by mode, in which the Central Processing Unit (2) is configured to deactivate the operation of at least part of its combinational logic and sequential circuits;
and wherein the Central Processing Unit is configured to switch from the stand-by mode to the active mode in the event of reception of the reading signal carrying the value of the user identifier or in the event of reception of the authenticated command;
and wherein the management circuit is configured to recharge the battery when the Central Processing Unit operates in the stand-by mode

10. Electronic system according to any one of the preceding claims, wherein the Central Processing Unit is implemented by means of a microprocessor, and wherein the Central Processing Unit comprises an Arithmetic Logic Unit, a Control Unit connected with the Arithmetic Logic Unit and a plurality of internal registers connected with the Arithmetic Logic Unit and with the Control Unit, wherein:

- the Arithmetic Logic Unit comprises a plurality of logic ports configured to carry out, as a function of data received from the plurality of registers, as a function of at least one control signal and as a function of said reading signal, a plurality of logic and arithmetic operations to execute the object code of the operating system and the object code of the software program;
- the plurality of internal registers is configured to store the temporary results of at least part of

the logic and arithmetic operations;
- the Control Unit comprises a plurality of logic ports and sequential circuits configured to read from the central memory and process a sequence of instructions of the object code of the operating system and the object code of the software program, execute the sequence of instructions by means of the Arithmetic Logic Unit and generate therefrom said at least one control signal of the Arithmetic Logic Unit.

11. Waste container comprising:

- an electro-mechanical lock adapted to control the locking/unlocking of the container opening;
- an electronic system according to any one of the preceding claims; wherein the lock is configured to switch between a closed position and an open position, as a function of the value of the driving signal;

wherein the photovoltaic panel is fixed to the structure of the waste container.

12. Container according to claim 11, further comprising a level sensor configured to generate a measurement signal indicative of a filling level of the waste accumulated within the container,
wherein the Central Processing Unit is configured to generate an alarm signal in case the value of the measurement signal is greater than a threshold value.

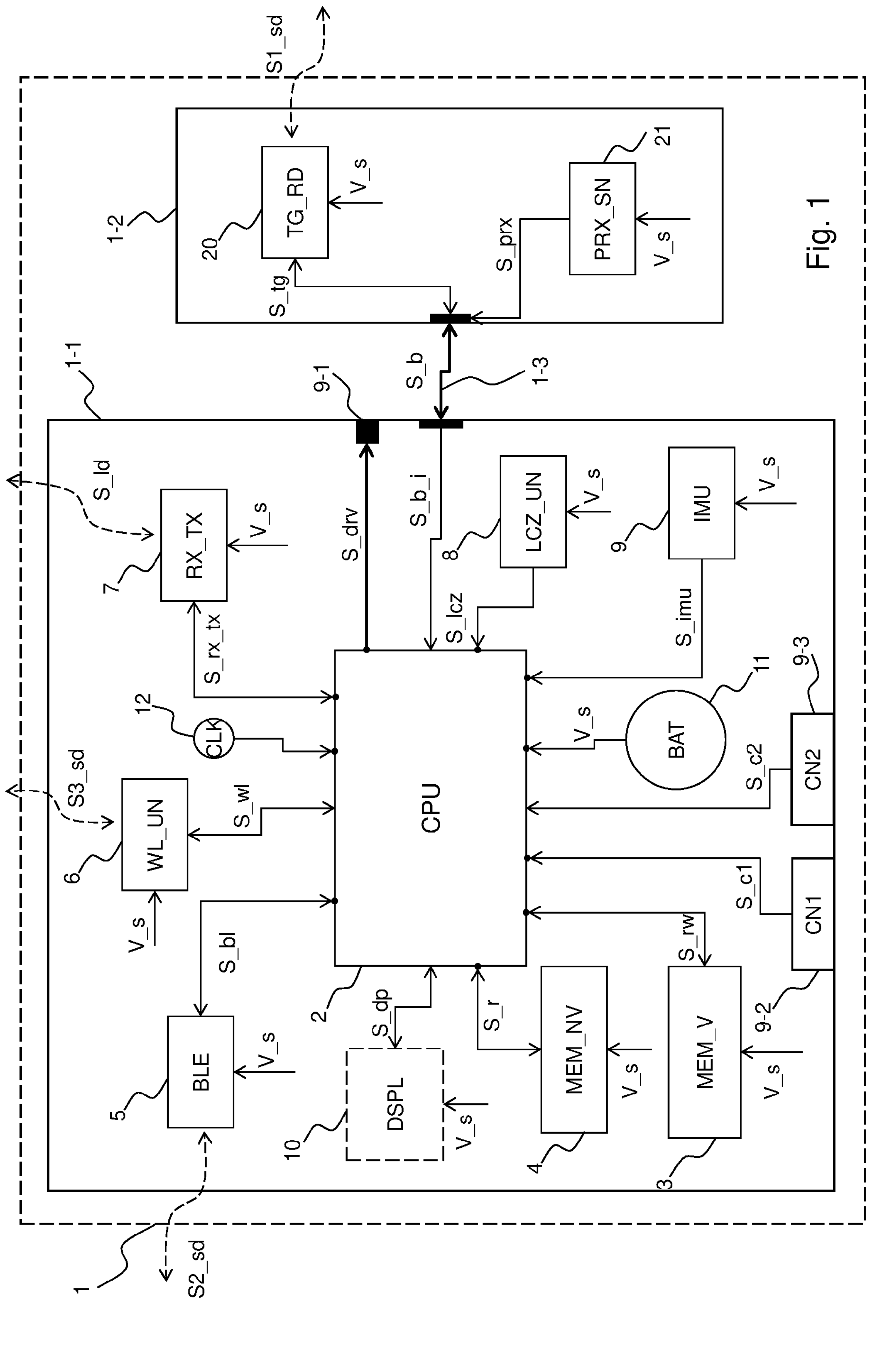
1
1-1
1-2
1-3
S1_sd
S2_sd
S3_sd
S_ld
TG_RD
20
V_s
PRX_SN
21
S_prx
S_tg
S_b
9-1
S_drv
S_b_i
RX_TX
7
S_rx_tx
LCZ_UN
8
S_lcz
IMU
9
S_imu
CLK
12
CPU
2
WL_UN
6
S_wl
BAT
11
CN2
9-3
S_c2
CN1
S_c1
9-2
S_rw
BLE
5
S_bl
DSPL
10
S_dp
S_r
MEM_NV
4
MEM_V
3

Fig. 1

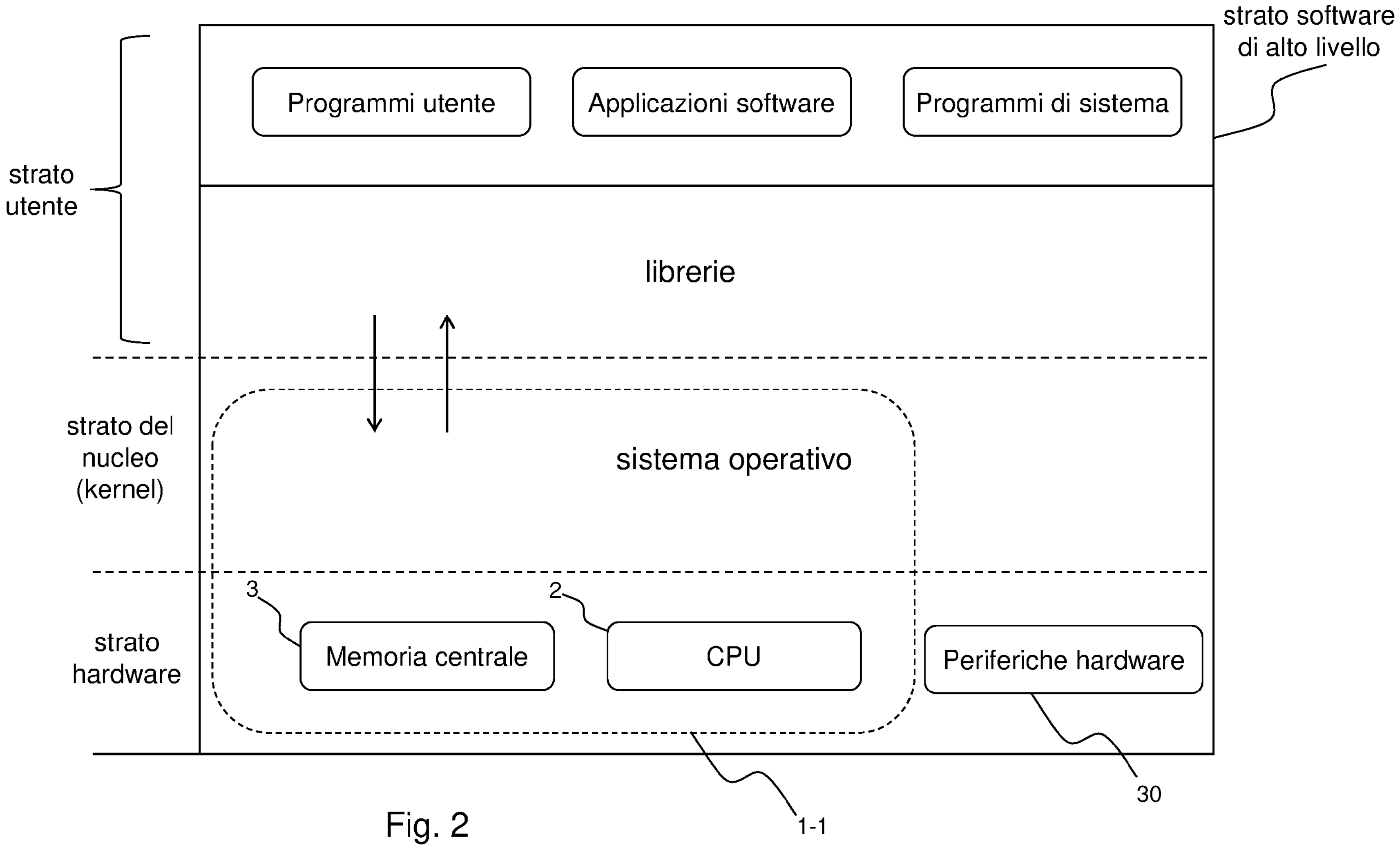
strato software
di alto livello
Programmi utente
Applicazioni software
Programmi di sistema
strato
utente
librerie
strato del
nucleo
(kernel)
sistema operativo
strato
hardware
3
2
Memoria centrale
CPU
Periferiche hardware
30
1-1

Fig. 2

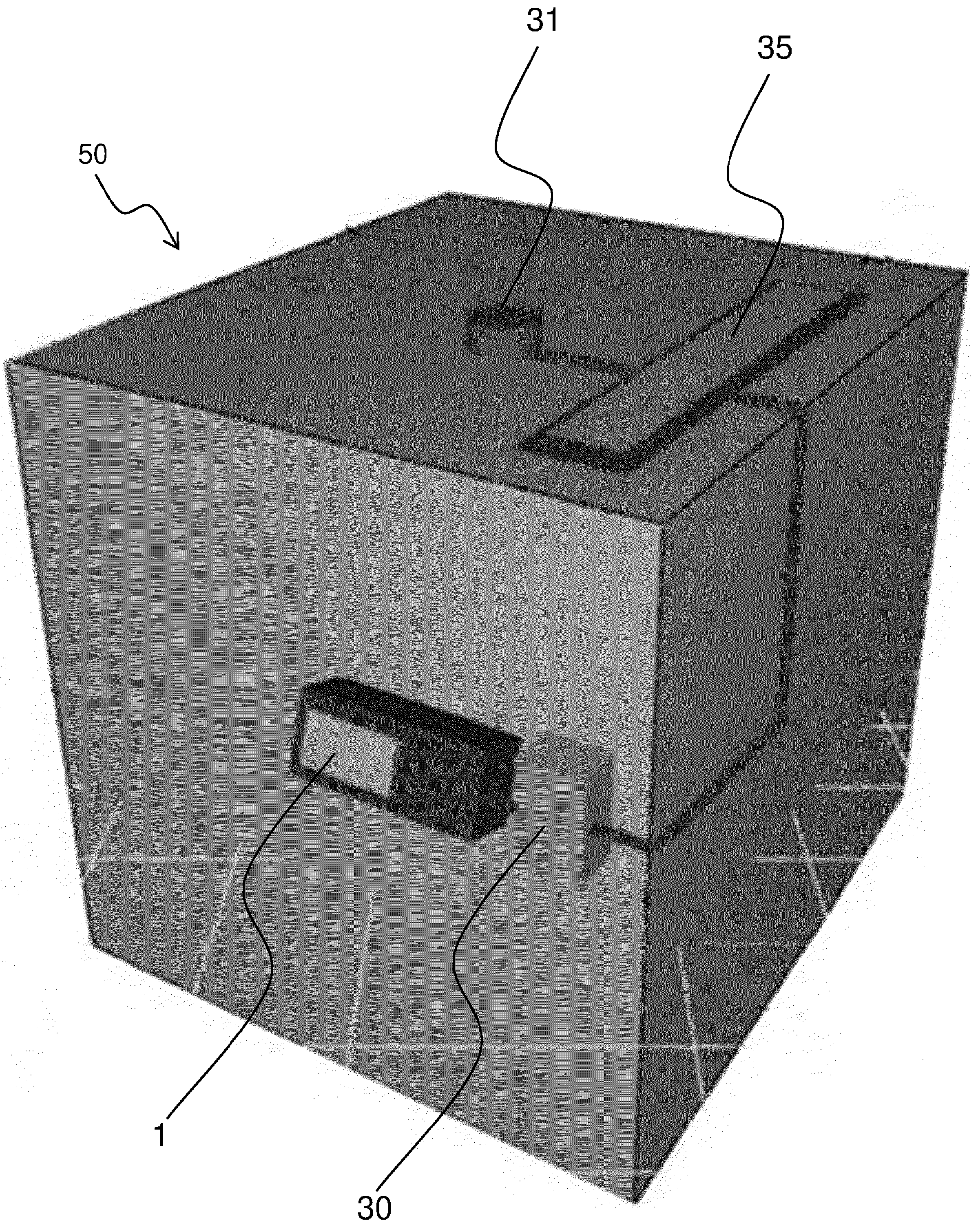

Fig. 3

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 23 16 0018

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
Y	EP 3 905 632 A1 (BH TECH [FR]) 3 November 2021 (2021-11-03) * abstract * * paragraph [0008] - paragraph [0024] * * paragraph [0026] - paragraph [0095] * * figures * -----	1-12	INV. G07C9/00 B65F5/00
Y	US 2021/021232 A1 (AUTIO PETRI [FI] ET AL) 21 January 2021 (2021-01-21) * abstract * * paragraph [0010] - paragraph [0050] * * paragraph [0066] - paragraph [0078] * * figure 1 * -----	1-12	
Y	US 2021/188541 A1 (KURANI HEMAL B [US] ET AL) 24 June 2021 (2021-06-24)	9	
A	* paragraphs [0122], [0159], [0450] * -----	1,11	
A	US 2015/307273 A1 (LYMAN JEFFERSON [US]) 29 October 2015 (2015-10-29) * abstract * * paragraph [0004] - paragraph [0009] * * paragraph [0023] - paragraph [0032] * * paragraph [0043] - paragraph [0047] * * paragraph [0052] - paragraph [0057] * * figures * -----	1-12	TECHNICAL FIELDS SEARCHED (IPC) G07C B65F
A	US 2013/278067 A1 (POSS JAMES ANDREW [US] ET AL) 24 October 2013 (2013-10-24) * paragraph [0057] - paragraph [0063] * * paragraph [0068] - paragraph [0071] * -----	1-12	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	28 June 2023	Miltgen, Eric

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons
& : member of the same patent family, corresponding document

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO.

EP 23 16 0018

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

28-06-2023

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 3905632 A1	03-11-2021	EP 3905632 A1	03-11-2021
		FR 3109689 A1	29-10-2021
US 2021021232 A1	21-01-2021	DK 3769415 T3	12-06-2023
		EP 3768612 A1	27-01-2021
		EP 3769415 A1	27-01-2021
		EP 4213379 A1	19-07-2023
		FI 20185277 A1	23-09-2019
		US 2021016965 A1	21-01-2021
		US 2021021232 A1	21-01-2021
		WO 2019180205 A1	26-09-2019
		WO 2019180211 A1	26-09-2019
US 2021188541 A1	24-06-2021	NONE	
US 2015307273 A1	29-10-2015	NONE	
US 2013278067 A1	24-10-2013	CA 2806876 A1	02-02-2012
		EP 2598410 A1	05-06-2013
		EP 3290359 A1	07-03-2018
		ES 2909249 T3	05-05-2022
		US 2013278067 A1	24-10-2013
		US 2016355308 A1	08-12-2016
		WO 2012015664 A1	02-02-2012

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82