

Device for accessing an underground or surface civil engineering infrastructure, comprising an intrusion detection device

5

The present invention concerns the field of solutions for accessing underground or overground civil engineering infrastructures of any type. The access to the infrastructures is generally made via an access door also called access cover or plug.

10

A door in particular enables access to the underground or overground civil engineering infrastructures for their inspection or checking. By civil engineering is meant in particular public or private networks (hydraulic, electrical, gas, communication, etc.), with the exception of domestic applications such as homes.

15

The infrastructures concerned are, non-exhaustively:

- public infrastructure networks, such as networks for accessing natural resources or public energy: water networks (in particular reservoirs of drinking water or storage towers of water tower type, purification networks dedicated to rain water and waste water, fire service outlets – also called fire
20 hydrants – and the corresponding networks), electrical energy networks, including electric cabinets (which may be installed overground, or be underground, buried or partly buried), networks for passage of communication cables (telephone, optic fiber, etc.);

- private infrastructure networks: water, energy, underground
25 communication infrastructures (cabled) or aerial communication infrastructures (antenna networks for example).

A complete access solution generally comprises an access cover (door, or plug), a frame to which the access cover is linked and which is for example sealed into the ground or on a fixed infrastructure, and a chamber
30 located under (or behind) the access cover.

It is important to ensure the checking of the resources distributed by these infrastructures (natural resources, energy or information sources). This

constitutes a matter of public and economic concern. For some applications, it is important to be able to check the infrastructures at any time, that is to say to ensure continuity in the availability of the information concerning them.

5 Access doors by definition constitute a point of access to an infrastructure. Although operations for checking or maintenance of the infrastructure may be necessary via these access points, they nevertheless constitute weaknesses in relation to the security of the infrastructures, in that they may constitute points of intrusion. For numerous applications, it is thus
10 important to be able to detect unauthorized accesses to the infrastructures.

It should be noted that in the whole of the present document, the term intrusion is employed to designate any unauthorized access, and comprises in particular breaking into an access device.

Document US 8976038 describes a device making it possible to
15 ensure that an access door, in particular a manhole cover, is in closed position. The described device comprises a sensor positioned in the chamber under the door and configured to pick up an acoustic signal emitted at the location of the sensor and reflected by the door. When the door is open, the signal is not reflected and the opening of the door can thus be determined. In response, an
20 image sensor is able to sense an image of the scene, and/or the information of opening the door can be communicated by a wireless network.

Nevertheless, the known systems in the state of the art make it possible at best to detect an opening of a door, but they do not solve the issue of intrusion into an infrastructure, since an intrusion is potentially already in
25 course, or the moment (for example the opening) of the door does not correspond to an intrusion.

The invention seeks to provide an access device for accessing an underground infrastructure solving part or all of the aforementioned issue.

30 Thus, the invention relates to an access device for accessing an underground or overground civil engineering infrastructure, comprising an access door having a closed position in which it shuts a chamber and an open

position in which it gives access to said chamber. The access device comprises at least one sensor configured to measure a quantity and to deliver a signal corresponding to the measured magnitude. The measured quantity represents a mechanical or thermal action on the door and an analysis module configured to

5 analyze the signal so as to detect information characteristic of an attempted intrusion into the chamber, and, in case of detection of said characteristic information, to generate an attempted intrusion warning. The access device comprises a communication module configured for the emission of said attempted intrusion warning. The analysis module detects the information

10 characteristic of an attempted intrusion by analysis of the temporal change in the measured quantity.

The processing of the signal or signals coming from one or more sensors makes it possible in the invention to detect whether an attempted intrusion is in course. This makes it possible, thanks to the communication

15 module, to send a warning before the intrusion into the chamber of the access device has actually taken place. Measures can thus be taken very rapidly. Among these measures, the sending of an intervention team may be envisioned. Various measurements may also be taken relating to the infrastructure concerned. For example, for a communication network (for

20 example a fiber-optic network), it is possible to immediately cease the exchange of information over that network. For a water network, the passage of water may be cut off upstream or downstream of the access point concerned.

The analysis module can in particular detect the information characteristic of an attempted intrusion on the basis of a correlation of

25 parameters of a same signal or of parameters of signals coming from different sensors.

The communication module may in particular comprise wired or wireless communication means.

The communication module may be of multi-protocol type.

30 The access device may comprise a shock or vibration sensor.

The access device may comprise an acoustic sensor.

The detection of the information characteristic of an attempted intrusion may be based at least in part on the frequency of shocks, vibrations, or sounds (detected by the sensor). The frequency may advantageously be correlated with data on intensity of the shocks, vibrations, or sounds, for the
5 detection of the information characteristic of an attempted intrusion.

The access device may comprise a temperature sensor or an optic sensor for detecting thermal radiation. The detection of the information characteristic of an attempted intrusion may be based at least in part on a temporal change in the temperature or in the thermal radiation.

10 The access device may comprise at least one sensor of opening or of closing of the door from: a mechanical contact sensor, a sensor of angular position of the door, an accelerometer, an optical sensor.

The access device may comprise a battery enabling the supply, as main supply or in the event of a fault in a main electric source, of the
15 communication module.

Still other particularities and advantages of the invention will appear in the following description.

In the accompanying drawings, given by way of non-limiting example:

- 20 - Figure 1 shows an access device in accordance with an embodiment of the invention;
- Figure 2 represents another example embodiment of an access device in accordance with the invention;
- Figure 3 is a diagrammatic representation of a communication
25 module able to be implemented in the invention.

Figure 1 represents a door 1 and the frame 2 to which it is connected, which are provided to shut a chamber (not shown in Figure 1) or to enable access thereto. Figure 1 is intended to present an example of physical constitution for an access device, but the invention is applicable to numerous
30 other constitutions.

The door 1 is represented in an open position, enabling access to the chamber via the opening 21 formed by the frame 2.

The door 1 may have various constitutions. In the example shown in Figure 1, the door is formed from galvanized steel. According to other possible constitutions, the door 1 may be of cast iron (ductile, grey), of stainless steel, of composite material. The door may thus be constituted from a single material, or
 5 may combine different constituent materials. Thus, part of the surface of the plug may be made from a first material and the complementary surface may be made from another material. In particular, the plug may combine a galvanized steel with a part comprising a particular coating or for instance be of cast iron having an insert of another material.

10 This may in particular assist in enabling the transmission of electromagnetic waves through the door 1, as detailed below.

In the example of Figure 1, the door comprises a rigid outer skin 11, for example of galvanized steel. The outer skin corresponds to the visible part of the door 1 when this is in closed position. The outer skin 11 covers or provides
 15 surface continuity with the frame 2. Of course, the door 1 may be slightly proud relative to the frame 2, and/or have a non-planar surface which is wholly or partly proud relative to the frame 2.

Under the outer skin 11, ribs 12 form compartments 13, 13'. The ribs 12 are substantially at right angles to the outer skin 11.

20 The frame 2 may also be formed from steel. The other aforementioned constituent materials may alternatively be employed. The frame 2 may in particular be of the same material as the door 1.

It has sealing members 21 for its definitive fastening by sealing at the opening of a chamber (not shown in Figure 1). The chamber may, for
 25 example, for infrastructures for which security is to be provided, be formed from reinforced concrete or from mortar with a fiber filler. The chamber may be of composite material or any other material used in the field of civil engineering.

The door 1 has a seat, that is to say a zone of contact in closed position, which may simply be laid on the frame 2 or be held in the frame 2.

30 The door 1 is linked to the frame so as to be able to take an open position and a closed position. For example, the door 1 may be pivotally mounted relative to the frame 2, by a pivot 15. The door 1 may have simple

opening, that is to say that the door 1 may be opened using a simple lifting key, or it may have a locking system of higher or lower complexity (for example only allowing the opening of the door 1 with use of a specific key). The locking system 16 may comprise two locking latches which can be turned so as to bear
 5 under the frame 2, preventing the opening of the door 1.

The door 1 is equipped in the invention with a communication module
 3.

The communication module 3 may comprise in particular an electronic unit 31 provided with at least one antenna 32 enabling the emission
 10 of a signal over a wireless network. Alternatively or in addition, the communication module 3 may allow wired communication.

The communication module 3 may be disposed in a compartment 13 formed under the outer skin 11 by the ribs 12. The compartment 13 receiving the communication module 3 is closed by an inner skin 14. The inner skin 14 is
 15 rigid. The inner skin 14 may be of inorganic or organic material (for example of plastic, of composite material) which may be reinforced to withstand attacks that are mechanical (for example using cutting tools) or thermal (for example with a blow-torch). It may be of metal, for example of hot-galvanized steel, or of stainless steel.

20 It provides protection for the communication module 3. One, several or all the compartments 13, 13' formed by the ribs 12 may be closed by an inner rigid skin 14.

The antenna 32 of the communication module 3 may be positioned in the same compartment as the rest of the communication module 3.
 25 Alternatively, the antenna may be positioned in another compartment. The positioning of the antenna is important in order to enable the transmission of waves from the plate 1. The antenna 32 (or one or more of the antennas of the communication module) may be disposed in a compartment other than that of the electronic unit 31.

30 The position of the antenna is advantageously optimized so as to have the best possible transmission of the electromagnetic waves through the door 1. Nevertheless, in certain applications the constraint of protecting the

antenna against external action (attempt to break in through the door, for example) may be taken into account. The configuration and the position of the antenna may in particular take into account the configuration of the ribs 12, as well as the presence on the door 1 of zones of lesser damping for the electromagnetic waves: zones of smaller thickness than the rest of the door 1, or constituted by a material different from the rest of the door enabling better passage of the waves, the presence of a key-hole in the door, etc.

When the communication module is configured to enable wireless communication, said communication module is integrated (positioned) in fixed or adjustable manner, to provide the best transmission performance of the signal and, as a corollary, the least possible energy consumption.

Figure 2 represents another example embodiment of an access device in accordance with the invention. Figure 2 illustrates in particular another example of access device physical constitution to which the invention is applicable. Figure 2 represents an access door 1 which, contrary to the door of the device of Figure 1, is substantially circular.

The frame 2 is substantially circular to match. It gives access to a chamber 4.

In the example represented here, the plug or door 2 is typically of cast iron (for example of ductile cast iron). The frame 2 is formed from the same material. The door 1 is hinged by a pivot 15 to the frame 2. A locking means 16 enables the door 1 to be held in closed position.

Ribs 12 form compartments 13, 13' under the upper skin 11 of the door 1. The compartments are open, that is to say no inner skin closes them. In one of the compartments, the communication module is installed, fastened to the inside face of the upper skin 11 of the door 1. The fastening of the communication module 3 may be by conventional mechanical fasteners, for example with screw fasteners. Other fastening means, for example by magnets, may be employed.

More specifically, the electronic unit 31 of the communication module and the antenna 32 are fastened into a same compartment 13.

An example of a communication module 3 which may be employed in the invention is represented diagrammatically in Figure 3.

The communication module represented comprises an electronic unit 31 and an antenna 32. The unit 32 incorporates a microprocessor 33 configured
5 to receive the signals coming from at least one sensor 34. In this case, two sensors 34 are employed in the embodiment example represented.

The sensors 34 may be incorporated into the electronic unit 31 or are linked to said unit, as in the represented example, by sensor ports 35. The electronic unit 31 may advantageously be water-tight, and possibly air-tight. It
10 may comprise a casing of plastic material or of steel. The ports of the electronic unit 31, whether they be the ports of the sensor 35 or, as described below, the ports for connection of a source of electrical supply, or for instance for the connection of an antenna, may be advantageously fluid-tight. The ports not used may be covered by a fluid-tight plug.

15 The signal emitted by each sensor 34, which represents a measured quantity, may be analyzed to determine whether an attempted intrusion into the chamber of the access device has taken place. In particular, an analysis module analyzes the signal delivered by the sensor 34 to identify therein information characteristic of an attempted intrusion into the chamber. This
20 characteristic information may come from a parameter of the signal, or from a correlation of parameters of a same signal or of signals from different sensors.

In the example represented here, the analysis module is formed by the microprocessor 33 of the electronic unit 31. In particular, the analysis module executes a computer program according to instructions enabling the
25 analysis of the signal (or of the signals) for the purpose of determining the information characteristic of an attempted intrusion.

Thus, the analysis module may be integrated into the communication module, or distinct from the latter, according to the embodiment envisioned.

The sensors 34 may be of various types, to measure various
30 quantities of which the analysis of the value and/or of the change makes it possible to determine the information characteristic of an attempted intrusion.

The sensor 34 may in particular measure a quantity representing a mechanical or thermal action on the door 1.

In the represented example, a first sensor 34 is a shock or vibration sensor. A second sensor 34 is a temperature sensor.

5 The shock or vibration sensor may for example be based on an accelerometer. It makes it possible to detect a vibration type or violent mechanical action applied to the door 1. The detection of the information characteristic of an attempted intrusion may then be based on the frequency of the shocks or vibration detected. The intensity or power of one or more detected
10 shocks may be employed as main or additional parameter, in correlation with the frequency. This makes it possible for example to detect both an attempt to break in by repeated shocks on the door or in its immediate environment, and an attempt to break in by a violent mechanical attack, for example by explosion of an explosive charge.

15 This detection function could be provided alternatively or in addition by an audio sensor, based on the same provisions.

 The temperature sensor is disposed so as to measure the temperature either at the location of the inner surface of the door 1, or at a given point of the chamber 3 of the access device. The sensor may comprise
20 various known technologies, requiring a contact with the zone of which the temperature is measured or contactless (for example a laser sensor). It may also be an optical sensor configured to detect thermal radiation, for example an infra-red video camera. A fast rise in the temperature may be the sign of an attempted intrusion by mechanical cutting or thermal cutting (for example using
25 a cutting torch) of the door 1 or of its link with the frame 2 of the access device.

 The sensors 34 may furthermore comprise a sensor of open or closed position of the door, for example a mechanical contact sensor, a sensor of angular position of the door, an accelerometer, or an optical sensor. Such a sensor makes it possible to detect total or partial opening of the door. If opening
30 is detected further to the detection of information characteristic of an attempted intrusion, this enables the intrusion into the infrastructure via the access device considered to be confirmed.

When information characteristic of an attempted intrusion is detected, the analysis module emits an attempted intrusion warning. The intrusion warning is then emitted by the communication module, over one or more wireless networks and/or by wired communication. The communication module
5 may comprise a means for encrypting the data transmitted.

The example shown in Figure 3 is a wireless communication module. This communication module 3 comprises at least one radio frequency module 37 able to emit in accordance with at least one wireless communication protocol. It is notable that the communication module may also be of multi-
10 protocol type, that is to say configured to emit in accordance with at least two word and/or wireless communication protocols (simultaneously or alternatively, for example according to the availability of the networks).

The protocols employed may in be chosen for example particularly from the protocols of the Internet of things.

15 The protocols that may be implemented in the invention can be categorized as follows.

The protocols employed may comprise one or more wired communication protocols. For example, these wired communication protocols may be configured for communication by optic fiber or cable.

20 The protocols employed comprise at least one wireless communication protocol. The wireless communication protocols may be short-range communication protocols, and/or medium-range or long-range communication protocols.

The wired networks and the short-range communication networks are
25 thus mainly non-operated, that is to say independent of an antenna network deployed by an operator.

In particular, the short-range wireless communication protocols may be chosen from: NFC, RFID, Bluetooth, in particular Bluetooth Low Energy, Lifi, and Zigbee (registered trademarks). The use of alternative protocols of this
30 type, known or to come, may be envisioned.

The medium-range or long-range communication protocols may be chosen from 4G, 5G, LoRa, Sigfox, NB-IoT, LTE-M, GPRS, GSM (registered

trademarks). The use of alternative protocols of this type, known or to come, may be envisioned.

The medium-range or long-range communication networks may be of operated or non-operated type. Currently, most of the networks providing at the same time a very long range, portability and optimum coverage whatever the geographical position, are operated. They give rise to charging by the operator.

Generally, preference is given to low-consumption, long-distance transmission technologies. They may in particular employ the 868Mhz-914Mhz band. In certain cases of use, short-distance or medium-distance transmission technologies may be used. These technologies may employ the 433Mhz band for example. A relay is then provided for the transmission of the data over a long-distance network to enable the control of the access device from a remote platform.

As regards cellular communication protocols (GSM, GPRS, EDGE, UMTS/HSPA, LTE), these have the advantage of good network availability.

The communication module comprises a source of electrical supply. This source of electrical supply may be a battery 36, and/or a connection to an electrical supply network (for example a national distribution network) and/or a local source (hydro-electric turbine, wind turbine, solar panel, etc.). The battery 36 may be of different types, in particular of lithium-ion type. It makes it possible to ensure sufficient autonomy for the communication module 3, for example two years in normal conditions of use.

The battery 36 may be integrated into the electronic unit 31, or be external to that unit as in the example shown in Figure 3. Other energy sources, that are complementary or alternative may be employed: photovoltaic cells, connection to an electrical network, etc.

The invention developed may be included within a system for managing a set of devices for accessing one or more underground or overground civil engineering infrastructure as described above.

The system comprises access devices for accessing at least one underground or overground civil engineering infrastructure, which have centralized management.

The attempted intrusion warning, and optionally the confirmation of an intrusion supplied by a sensor for detection of the position of the door, are sent by the communication module to a server. This warning is alerted to an operator in charge of taking suitable measures, or that warning is processed by an automatic system which takes suitable measures.

Of course, in order for the suitable measures to be taken, it may be necessary to identify the access device concerned. For this, for example, each access device of the system can be associated with an identifier. When an access device communicates with the server, it sends its identifier to enable its identification. In a manner that is known per se, recognition algorithms may be used at the time of the communication between the access device and the server, in order to enable respective authentication to provide security for the communication.

The identification of the access device makes it possible to access information concerning it. In particular, the access device may be geolocated, for example by loading position information associated with said access device at the time of its installation. This position information (for example the coordinates of latitude and longitude of the access device) may be recorded in a computer memory on installing the access device. This memory may be comprised at the location of the server S or be remote from it.

Alternatively, position information may be recorded in a memory located at the access device (for example in the communication module 3), this position information being attached with the data transmitted by the access device.

The invention thus developed provides an access device for accessing an underground or overground civil engineering infrastructure, providing means making it possible to detect an attempted intrusion into the access device, for example particularly a break-in attempt. Different forms of intrusion may be taken into account by the device, according to the sensors which are implemented as well as the processing of the signal or signals from the sensors that is carried out. The detection of information characteristic of an

attempted intrusion, possibly complemented by confirmation of the intrusion, makes it possible to take the measures suited to the situation as soon as possible.

CLAIMS

1. Access device for accessing an underground or overground civil engineering infrastructure, comprising an access door (1) having a closed position in which it shuts a chamber (4) and an open position in which it gives access to said chamber (4),
the access device comprising at least one sensor (34) adapted to measure a quantity representing a mechanical or thermal action on the door (1) and to deliver a signal corresponding to the measured quantity, and an analysis module configured to analyze the signal so as to detect information characteristic of an attempted intrusion into the chamber (4), and, in case of detection of said characteristic information, to generate an attempted intrusion warning,
the access device comprising a communication module (3) configured for the emission of said attempted intrusion warning,
characterized in that the analysis module detects the information characteristic of an attempted intrusion by analysis of the temporal change in said measured quantity.
2. Device according to claim 1, wherein the analysis module detects the information characteristic of an attempted intrusion on the basis of a correlation of parameters of a same signal or of parameters of signals coming from different sensors (34).
3. Access device according to claim 1 or claim 2, comprising a shock or vibration sensor, or an acoustic sensor, wherein the detection of the information characteristic of an attempted intrusion is based at least in part on the frequency of shocks, vibrations, or sounds detected.
4. Access device according to claim 3, wherein the frequency is correlated with data on intensity of the shocks, vibrations, or sounds, for the detection of the information characteristic of an attempted intrusion.

5. Access device according to one of claims 1 to 4, comprising a temperature sensor or an optic sensor for detecting thermal radiation.

5 6. Access device according to claim 5, wherein the detection of the information characteristic of an attempted intrusion is based at least in part on a temporal change in the temperature or in the thermal radiation.

7. Access device according to one of the preceding claims, wherein
10 the communication module comprises wired or wireless communication means.

8. Access device according to claim 7, wherein the communication module is of multi-protocol type.

15 9. Access device according to one of the preceding claims, comprising at least one sensor of opening or of closing of the door from: a mechanical contact sensor, a sensor of angular position of the door, an accelerometer, an optical sensor.

20 10. Access device according to one of the preceding claims, wherein the device comprises a battery (36) enabling the supply, as main supply or in the event of a fault in a main electric source, of the communication module (3).