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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 May 2009 (14.05.2009)

PCT

(10) International Publication Number
WO 2009/059386 A2

(51) International Patent Classification:
G01R 11/24 (2006.01)

(21) International Application Number:
PCT/BR2008/000308

(22) International Filing Date: 17 October 2008 (17.10.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 0705720-2 23 October 2007 (23.10.2007) BR

(71) Applicant and
(72) Inventor: **DE QUEIROZ SILVA, Renato** [BR/BR]; Rua Ricardo Mariano 138/602, Recreio dos Bandeirantes, Rio de Janeiro-RJ, Cep: 22790-840 (BR).

(72) Inventors: **MENEZES CZERTOK, Andrey**; Av. Roberto Silveira 517/201-Icaraí, Niterói-RJ, Cep: 24230-153 (BR). **FRAUCHES CAREGA, Felício**; Rua Artur Posolo 50-102, Recreio dos Bandeirantes, Rio de Janeiro-RJ, Cep: 227-90-220 (BR). **CALDAS MENEZES, Leonardo**; Rua Domingues de Sá 425/1102-Icaraí, Niterói-RJ, Cep: 24220-009 (BR).

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

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

Published:
— *without international search report and to be republished upon receipt of that report*

WO 2009/059386 A2

(54) **Title:** (ANTI-THEFT DEVICE) - "INTELLIGENT DIFFERENTIAL SELFSURVEILLANCE POWER ANTI-THEFT SYSTEM (PROCESSES, COMPONENTS AND SCHEMES) MONITORED BY GPS OR REVERSE GEOCODING"

(57) **Abstract:** A system for detecting and preventing power theft on a branch distributor conduit (9) between, a transformer/distribution circuit (13) and an electricity meter (M) at a registered customer (1) of a power distribution company is provided. The system comprises first sensors (4A) and a first converter unit (5A) located within a sealed box (2) of an electricity meter (M) at the customer (1) for determining a frrst current value representing the current in the power feeding cables (7) and second sensors (4B) and a second converter (5B) located within a connection box (3B) measuring a second current value representing the current in the branch distributor conduit (9). The connection box (3B) comprises further a first electronic unit (10A) which determines the difference between the said first current value and the said second current value, If the difference is above a threshold value power theft is determined and a signal is transmitted from the first electronic unit (10A) to a server (11) located in the power distribution company for registering power theft, determining the location of the registered customer (1) and/or brunch distributor conduit (9) and for switching off the branch on which power theft is determined by means of a switch (8A). In addition the system may also be used to alert unauthorised opening of the door of the sealed box (2) and to determine tampering with the electricity meter (M). In an alternate embodiment the connection boxes (3B, 3C) may directly transmit their current values to the server (11) for detecting and preventing power theft.

- Description -

(ANTI-THEFT DEVICE) – "INTELLIGENT DIFFERENTIAL SELFSURVEILLANCE POWER ANTI-THEFT SYSTEM (processes, components and schemes) MONITORED BY GPS OR REVERSE GEOCODING".

The present invention refers to intelligent differential self-surveilled schemes to track or prevent power theft by the so-called "hooking" in power-supplied areas, and offers the possibility for a remote reading of power consumed in **(1) Registered Customers** of a Power Distribution Concessionaire.

The numbers in bold type before each **component** mentioned in this Report, in the Summary, and in the Requirement refers to the description of the solutions put forward for the **"SYSTEM"**, for the drawings shown in **ANNEX I**, and unifilar schematic in **ANEX II**. As for schematic representations, components such as boxes, boards, sources and circuits present no proportionality in said drawings and are listed below in accordance to their sequencing in **ANEX II**. Functions that come repeated have the same numbering, therefore:

- **(1) Registered Customer**.
- **(2)Sealed Meter Box** containing the **(M) Meter Reader** and the **(3A) Meter Reader of the Output Side of the Connection Box**. This box, in its turn, contains the **(4A) Current Sources** in conjunction with the meter reader and the **Digitalized and Communication Circuits**.
- **(M) Energy Meter.**
- **(7) Power Feeding Cable of the Registered Customer.**
- **(6) Control and Communication Cable,** if this is the case, or another **(6A) Communication Means** that conveys the image data from the **(4A) Current Sources** and power consumption readings, and if the **(M) Energy Meter** is digital to the **(10A) IDEE – Intelligent Differential Electronic Equipment**.
- **(3B) Connection Box of the Power Feeding Cable** of a **(1) Registered Client** to the **(9) Branch Distributor** containing the **(4B) Current Sources**, the **(10A) IDEE – Intelligent Differential Electronic Equipment,** and, optionally, the **(8A) Contactor** of the **(1) Registered Customer**.
- **P_A, P_B and P_C** – connection points from the **(7) Power Feeding Cable** to the **(9) Branch distributor.**
- **(6B) Control Cables** or another type of communication means that, should that be the case, convey the data of the current-images from the **(3B) Connection Boxes of the Power Feeding Cable** of each **(1) Registered Customer** so that the total sum of the currents may be compared to the output current of the **(13) Transformer or Distribution Circuit**.
- **(3C) Connection Box** of the **(9)Branch Distributor** to the **(13) Transformer or Distribution Circuit** containing the **(4C) Current Sources**, the **(5B) Digitalized and Communication Circuits**, the **(5B) IDEE – Intelligent Differential Electronic Equipment**, and, optionally, the **(8B) Contactor of the Branch Distributor**.
- **(12) Communication means** between **(10A)** and **(10B) IDEEs- Intelligent Differential Electronic Equipment** and the **(11) Company's Server**.

Energy theft (also known as *hooking*) is made by totally or partially stealing power directly from the **(7) Power Feeding Cable of the Registered Customer** positioned before the **(M) Energy Meter**, as well as by tempering with **(M) Energy Meters** or by directly *hooking* to the **(9) Branch Distributor.**

Some customers, generally in poverty-stricken places, are not registered as consumers of the local Power Distribution Company, and power theft through *hooking* is mostly easily identifiable and unskillfully made in the **(9) Branch Distributor** or in the **(13) Transformer or Distribution Circuit**, giving rise to a chaotic dense tangle of wires as shown attached **(Annex III)**.

Power theft originating in the **(1) Registered Customer** is more elaborate, usually unidentifiable, etched into the masonry, likely to be handled unobtrusively and placed before the energy meter, tempering with the latter. This kind of installation also allows for a parallel deviation, namely before the energy meter or the general circuit breaker, feeding part of the power, there being theft of the power consumed at that moment. Therefore, the energy meter reads only part of the electrical energy, so the consumer will not be at risk of being caught when the power company employee comes in to check the meter. More sophisticated **"hooking"** utilizes elaborate controls to automatically switch off in the case the power company employee switches off the **(7) Power Feeding Cables of the Registered Customer** at any given point.

In an attempt to deter power theft, some power distribution companies have decided to make energy meters as visible as possible, and some companies even place them as close as possible to the **(9) Branch Distributor**. The latter practice has been facing antagonism on the part of consumers as they are unable to have access to reading the energy meter, a practice the Electric Sector enforces.

The present Application for Patent (AP) tracks or prevents the above described **"hookings"** at the registered no matter if they are unsophisticated or skillfully made.

This AP also proposes that the readings produced by local digital energy meters be readable and processed remotely at the Power Company's Control Centers, so local readings may only be resorted to in the case doubts arise, therefore interrupting a long-standing policy on the part of the Power Sector, but also making power invoicing processing less costly.

The **"System"** is dubbed self-surveilled because if any of its circuits are tempered with, the lack of reception of any entry data will make remote alarms go off, pointing toward the occurrence of an abnormality or describing this same abnormality depending on how sophisticated the process applied is. Alarms will also go off in the case the door of the **(2) Sealed Box of the Energy Meter** is open or if there is an attempt to temper with the magnetic field around the energy meter, in the case of electro-dynamic energy meters.

Although the **"System"** detects all forms of power theft, the integrity of the **(2) Sealed Box of the Energy Meter** should be given priority.

The principle backing the **"SYSTEM"** is that it is **DIFFERENTIAL** for any given anti-theft scheme, i.e., the potency that leaves the **(9) Branch Distributor**, disconsidering marginal losses, must be equal to the potency that passes through the **Energy Meter (M)**.

Therefore, in order to oversee a **(1) Registered Customer**, the **"System"** checks the current that leaves the **(9) Branch Distributor** toward the **(1) Registered Customer** is the same that flows into the **(7) Power Feeding Cable of the Registered Customer**, which must be the same as the current that leaves the **Energy Meter (M)** of the **(1) Registered**

Customer. This holds true except for a small value adopted as a safety threshold due to the losses in the circuit, transformation ratio, energization current, etc...

What has been devised to avoid power theft in this kind of customer is to have every power feeding line coming from the **(9) Branch Distributor** to the **(1) Registered Customer** through the **(7) Power Feeding Cable of the Registered Customer** with these two connection boxes, as described below:

One **(3A) Meter Reader of the Output Side of the Connection Box** containing the **(4A) Current Mono-phase Sources** etched into the **(2) Sealed Box of the Energy Meter (M)**, which will send the output data from the **(M) Energy Meter** to the **(5A) Digitalized and Communication Circuits** which, in turn, will send the resulting current signals flowing through the **(M) Energy Meter** to the **(10A) IDEE – Intelligent Differential Electronic Equipment** localized in the **(3B) Connection Box of the Power Feeding Cable** connected to the **(9) Branch Distributor** . The resulting current data may be sent through the **(6A) Control Cables**, Infrared, Optical Fiber, Radio Frequency or any other new technology such as Bluetooth, working under a communication protocol.

The resulting data of mono-, bi- or tri-phase currents produced by **(5A)** and **(5B) Digitalized and Communication Circuits** must equal the sum of a certain number of amplitudes at a given time interval and must be compared.

From four to eight control cables or from three to five data cables come from the **(3A) Meter Reader of the Output Side of the Connection Box** to the **(3B) Connection Box of the Power Feeding Cable**, depending on the data release model adopted between these boxes, and on whether the power feeding scheme of the **(2) Registered Customer** is mono-, bi- or tri-phase. Two pairs will be used for the door and magnetic field surveillance relays, localized in the **(9) Sealed Box of the Energy Meter**, if that is the case. Digital energy meters do not need relays to detect magnetic field variation. If the data between these connection boxes is wireless, the **(3A) Meter Reader of the Output Side of the Connection Box** should also contain a board bearing the function **CLP** associated to a **transmitter**. It is preferable that the transmission between these boxes be made by cable as the distances are relatively marginal and constant.

Another box, the **(3B) Connection Box of the Power Feeding Cable** that links the **(9) Branch Distributor** to the **(7) Power Feeding Cable of the Registered Customer** may have, optionally, a **(8A) Contactor** between the phases of these cables. If this is the case, it may have local or remote re-switching, depending on the philosophy adopted by the Power Distribution Company.

Initially, we will examine the status of one **(1) Registered Customer**, and, should power theft be traced, legal action may be taken on the part of the Power Distribution Company.

The **Connection Box (3B)** shall also have the **(5B) Digitalized and Communication Circuits**, which will transmit the signs resulting from the current demanded by the **(7) Power Feeding Cable of the Registered Customer** to the **(10A) IDEE – Intelligent Differential Electronic Equipment** localized in the **(3B) Connection Box of the Power Feeding Cable** to the **(9) Branch Distributor** . In the **(10A) IDEE – (Intelligent Differential Electronic Equipment)** an **IDC (Intelligent Differential Circuit)** compares the data of the current that flows from the **(4A) (4B) Mono-phase Current Sources** to a

reading above a given security threshold, where a mismatch points toward power theft. In this case, therefore, there will be a **GPS** (Global Positioning System) signal output or a **Transmitter/Receptor** of any communication means commonly used such as Radio Frequency, Cellular Telephony, Fixed Telephony, Satellite, Cable, Infrared or Optical Fiber which will transmit and/or receive a signal concerning the customer, therefore tracking it.

If the **IDEE** does not utilize **GPS**, the **(1) Registered Customer** must be previously geo-codified by a **GPS** in order to be registered in a **Reverse Geo-coding** program installed in the **(11) Server** localized at the Power Company's Distribution Control Center, allowing the Company to decide toward action-taking according to its own policy. This former method should be given preference. Because they are fixed customers, a mobile **GPS** is only necessary when the customer is first registered, which makes the **"SYSTEM"** more affordable as a whole.

The **(10A) IDEE (Intelligent Differential Electronic Equipment)** may be able to detect the occurrence of power theft and proceed to the automatic switch-off or restart of the power supply as much as to receive remote commands to switch off or restart the power supply of the **(1) Registered Customer**, and should it be the Power Company's choice, the **(3B) Connection Box** may have the **(10A) Contactor**.

The situations giving rise to power theft are reported to the Power Company's Control Center, informing the address of the customer where the power theft has been traced, thus triggering several **(MMI)** man-machine-interactions. For instance, power theft may be reckoned as an occurrence backing future action-taking, such as checking on the customer to collect data on a legal basis so the Power Supply Company can prove revenue loss, or activating a remote signal toward the connection key, switching off the power that is being stolen. Decisions guiding the **"System"** project are to conform to the Company's entrepreneurial policy.

From the **(10A) IDEE (Intelligent Differential Electronic Equipment)** of each **(1) Registered Customer**, the data resulting from the input current in the **(9) Power Feeding Cable of the Registered Customer** that feeds the control of the **(9) Branch Distributor** at the **(11) Server** will be sent to the **(11) Server** by those communication means commonly used Conversely, this same data produced on the current will be sent through the **(6B) Control Cable** or Another Communication Means to the **(10B) IDEE – (Intelligent Differential Electronic Equipment** in the **(3C) Connection Box of the Delivery Point** to the **(11) Transformer or Distribution Circuit**. In this case, control will be performed at the **(10B) IDEE** and the result will only be sent in the case of power theft. This solution is probably not the best one due to the large number of **(1) Registered Customers** along the lengthy range of delivery points.

Finally, for those customers that are not yet registered, whose *hooking* gives rise to the chaotic dense tangle of wires as shown attached **(Annex III)**, the solution proposed by the **"System"** is to check on each **(9) Branch Distributor** separately so that the difference between the total sum of the potencies required by the several **(7) Power Feeding Cables of the Registered Customers** of a given **(9) Branch Distributor** toward the **(13) Transformer or Distribution Circuit** equals zero, unless a mismatch occurs. Therefore, when a *hooking* attempt along the **(9) Branch Distributor** is made, the potency required at this **(9) Branch Distributor** will be different from the potencies that are required by the several **(1) Registered Customers**. The control over the **(9) Branch Distributor** will be

made preferably in the control software of the **(11) Power Supply Company's Server** associated to the **Reverse Geo-coding** software. Each **(9) Branch Distributor** connected to the **(13) Transformer or Distribution Circuit**, previously geo-codified, constitutes a control group that contains the data produced on all the **(1) Registered Customers** that belong to a given **(9) Branch Distributor**.
The information on the potency that is required from the **(11) Transformer or Distribution Circuit** is produced in the **(3C) Connection Box** of the **(9) Distribution Cable** and sent to the **Transformer** or **Distribution Circuit (11)**. This **(3C) Connection Box** has the **(4C) Sources of Current**, the **(5C) Digitalized and Communication Circuits** and the **(10B) IDEE – Intelligent Differential Electronic Equipment**, which may not have **GPS** and **IDC** functions, working via radio in the case the Scheme should use **Reverse Coding** and the control of the **(9) Branch Distributor** should be made at the Power Company's Distribution Control Center, respectively. The **(10B) IDEE – Intelligent Differential Electronic Equipment** may be able to detect both the occurrence of power theft and to switch off or restart power supply automatically as well as to be remotely controlled to switch off or restart power supply at the **(9) Branch Distributor**, should the Power Company choose a scheme with the **(8B) Contactor** and the **IDC** functions in the **(10B) IDEE – Intelligent Differential Electronic Equipment**. Data **(12) Transmission/Reception** between the **IDEE** and the **Company's Server (11)** may be made the same way as the former one, i.e., through any communication means commonly used.

The comparison between the apparent potencies in the **Power Circuit (7)** output, in the **(9) Branch Distributor** and in the **Energy Meter (M)** input is attained by comparing the differences between the current image obtained by the sources of current (TC). Such secondary currents are between 4 to 20 mA.

The **(5A, B** and **C) Digitalized and Communication Circuits** as well as the **(10A)** and **(10B) IDEE – Intelligent Differential Electronic Equipment** are fed by sources of 100mA of 12V, and communication between these equipment is conducted via a no-parity asynchronous communication protocol of 9600 bits/s and 1-stop bit.

Should it be necessary to receive the data on the electric active energy of each **(1) Registered Customer** at the Operation and Distribution Center, the computed information should be done ideally with digital meters extending to the **(3B) Connection Box of the Power Feeding Cable** through cables such as USB, RS485 or RS232, and then sent to the Company through any of the communication means previously mentioned. Unlike telephony, the Power Industry does not commonly proceed to measuring the consumption of electricity remotely. Initially, though, it is perfectly feasible to proceed to a remote measuring, and to resort to a local measuring only when doubts about invoicing arise, which is a cost-saving approach. In a second instance, both measuring the consumption and proceeding to meter reading may be done remotely.

The **"SYSTEM"** allows for several processes, depending on how convenient it might be or not to use **(10A)** and **(10B) Contactors** in accordance with the scheme used by the Company, and the legal conduct and entrepreneurial policy adopted by the Company. Among the several arrangements and **processes** that may be chosen from, the following must be mentioned:

a) Only remote assessment and simultaneous tracking of the **(1) Registered Customer** and/or, in the case of a non-registered customer, of the **(9) Branch Distributor** where power theft is occurring.

b) Automatic switch-off and restart of power supply, when *hooking* is done and undone, respectively, at the **(1) Registered Customer** and/or, in the case of non-registered customers, at the **(9) Branch Distributor**, and through remote assessment and simultaneous tracking of where the power theft attempt is being made. Locally, there may be a visual or sound signalization pointing toward an abnormality so that the power theft agent at a given **(9) Branch Distributor** feels constrained and deterred from going on with the power theft. If power theft occurs at a **(1) Registered Customer**, the former should be notified that the theft has been traced. In the case of a *hooking* attempt on the part of a non-registered customer, the consumer(s) deemed a **(1) Registered Customer** should be communicated that power outage occurs due to power theft attempts in his/her/their neighborhood.

c) Remote assessment of the **(1) Registered Customer** and of the **(9) Branch Distributor**, as well as simultaneous tracking of where power theft is occurring, and remote control to switch off and restart power supply providing *hooking* is eliminated. Visual signs and/or sound alarms should be made available in the sites where abnormalities are detected.

d) Other combinations of systems may be used by the Power Company, according to its own convenience, in order to switch off or restart automatically or remotely one of the power feeding alternatives above mentioned, giving rise to other men-machine-interactions and legal action as the Company deems necessary.

ANNEX I presents a diagram of the situation and ANEX II an electrical schematic diagram of the **(ANTI-THEFT DEVICE) – "INTELLIGENT DIFFERENTIAL SELFSURVEILLANCE POWER ANTI-THEFT SYSTEM (processes, components and schemes) MONITORED BY GPS OR REVERSE GEOCODING"** above exposed. Annex III shows a picture of the dangerous and chaotic dense tangle of wires provoked by *hooking* that non-registered customers make in the Distribution Networks.

- Claims -

This is a Claims for Registration of Patent of **(ANTI-THEFT DEVICE) – "INTELLIGENT DIFFERENTIAL SELFSURVEILLANCE POWER ANTI-THEFT SYSTEM (processes, components and schemes) MONITORED BY GPS OR REVERSE GEOCODING"**, which consists of an intelligent differential self-surveillance system to track or prevent power theft, offering the possibility for remote reading of

the **(1) Registered Customers** of a **Power Distribution Concessionairy.**

Energy theft (also known as *hooking*) is made by totally or partially stealing power directly from **(7) Power Feeding Cables of the Registered Customer** localized before the **(M) Energy Meter**, as well as by tempering with **(M) Energy Meters,** or by directly hooking to the **(9) Branch Distributor**, which may be blatantly identifiable as these connections are unskillfully made to the **(9) Branch Distributor**, which gives rise to the chaotic dense tangle of wires as shown attached **(Annex III)**.

The "SYSTEM" in this Claims consists of differentiated schemes that track and compare on an ongoing basis, through current images, the apparent potencies that run through the **(M) Energy Meters** of each **(1) Registered Customer** and the apparent potencies solicited from the **(9) Branch Distributor**. Likewise, they track and compare the sum of the apparent potency being demanded by the several **(1) Registered Customers** and the apparent potency being demanded by the correspondent **(13) Transformer or Distribution Circuit**. Should this comparison show a mismatch between the current and the assumed safety threshold, the **"SYSTEM"** acknowledges this as power theft and through the communication means listed in the report, transmits a signal to one **(11) Server** located in the Company. Depending upon the scheme selected, the **"SYSTEM"** will either register the power theft or will prevent the occurrence altogether by furnishing the exact localization of the customer or the **Branch Distributor**.

The **"SYSTEM"** also tracks, on an ongoing basis, the gate-keeping status of the **(2) Sealed Meter Box** and that of the permanence of the magnetic field reading that is restricted to the meter, in the case of electro-dynamic readers.

The above mentioned assessment of the apparent potencies are made by means of the images of the corresponding currents which in **(5A, 5B and 5C) Digitalized and Communication Circuits** are modified to resulting-currents, constituted by the total sum of a certain number of amplitudes of the images of current considered at a certain time interval, which are then sent to the corresponding **(10A and 10B) IDEE – Intelligent Differential Electronic Equipment**, according to a no-parity, asynchronous communication protocol of 9600 bits/s.

In order to track the **(1) Registered Customers**, the **(7) Power Feeding Cables of the Registered Customers**, and the **(9) Branch Distributor**, the reading furnished by the images of current is provided by **(4A, 4B and 4C) Sources of Current** and are received by **(5A, 5B and 5C) Digitalized and Communication Circuits**, which in their turn are sent to **(10A and 10B) IDEE – Intelligent Differential Electronic Equipment**. In the **(10A and 10B) IDEE – Intelligent Differential Electronic Equipment** an **IDC** function **(Intelligent Differential Circuit)** compares the readings of the current against a given safety threshold, and should a mismatch occur, the system interprets it as power theft. In this case, there will be a signal output either for a **GPS** function **(Global Positioning System)** or for a Transmitter/Receptor of any communication means commonly utilized such as Radio Frequency, Cellular Telephony, Fixed Telephony, Satellite, Cable, Infrared or Optical Fiber that will transmit/receive a signal inherent to the customer, thus tracing it.

Depending on the scheme adopted, the **IDEE** may not have **GPS** and/or **IDC** function. If **GPS** is not available, the **(3B) Connection Boxes of the Power Feeding Cable** of each **(1) Registered Customer** of a given **(9) Branch Distributor**, and the **(3C) Connection Box of the Power Distribution Cable** to the **(13) Transformer or Distribution Circuit** will need to be geo-referenced only at the installation point, or when connection boxes are checked. The registered customers and its **(9) Branch Distributor** will be tracked by **REVERSE GEOCODING**.

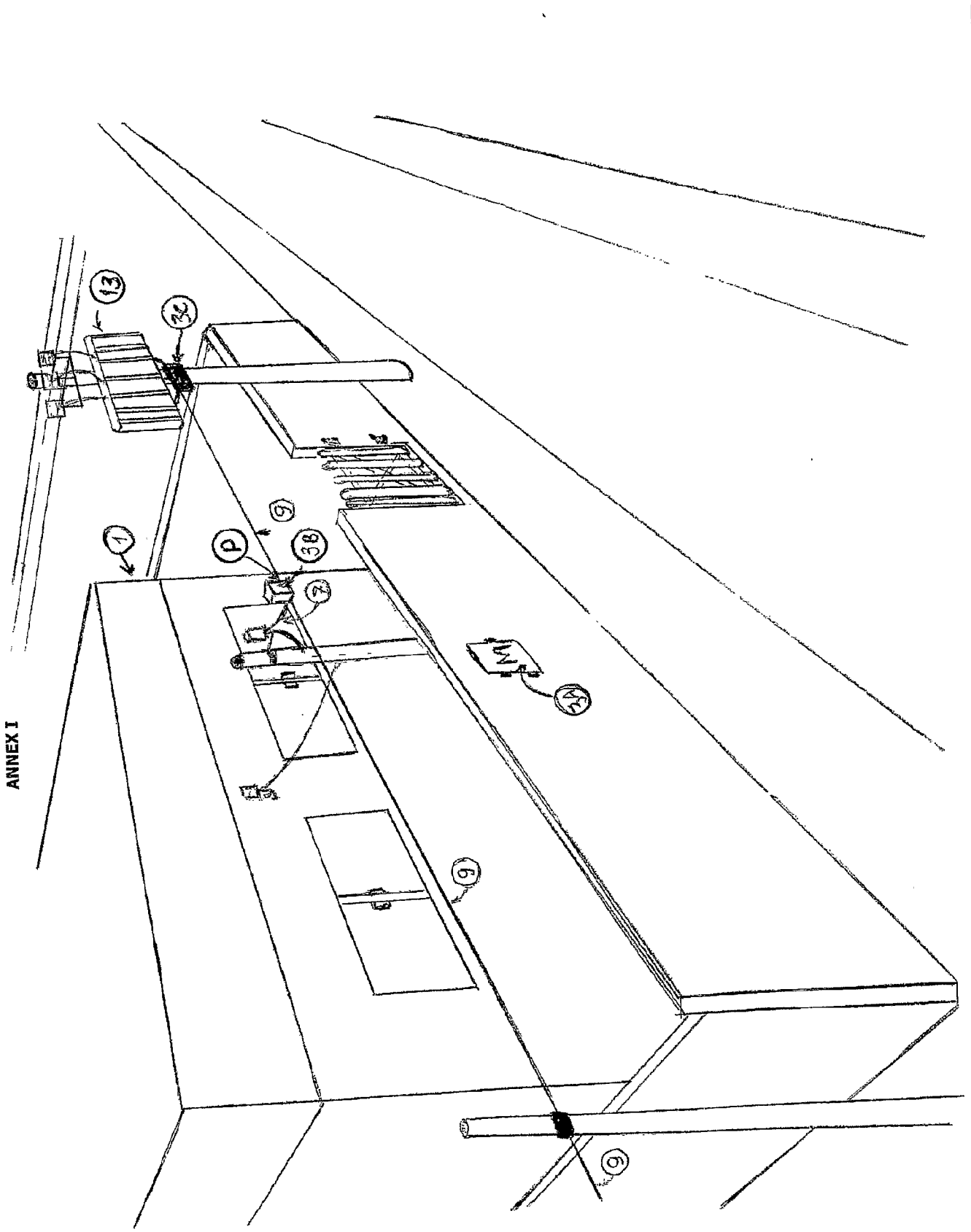
In there being no **IDC** function, information on current is sent to the **(11) Server** to be analyzed differentially. Supervision of the **(9) Branch Distributor** will be done in the program, associating to the number of customers of this delivery point the power it demands, and comparing this demanded power to that demanded by the several **(1) Registered Customers** of this same **(9)Branch Distributor**.

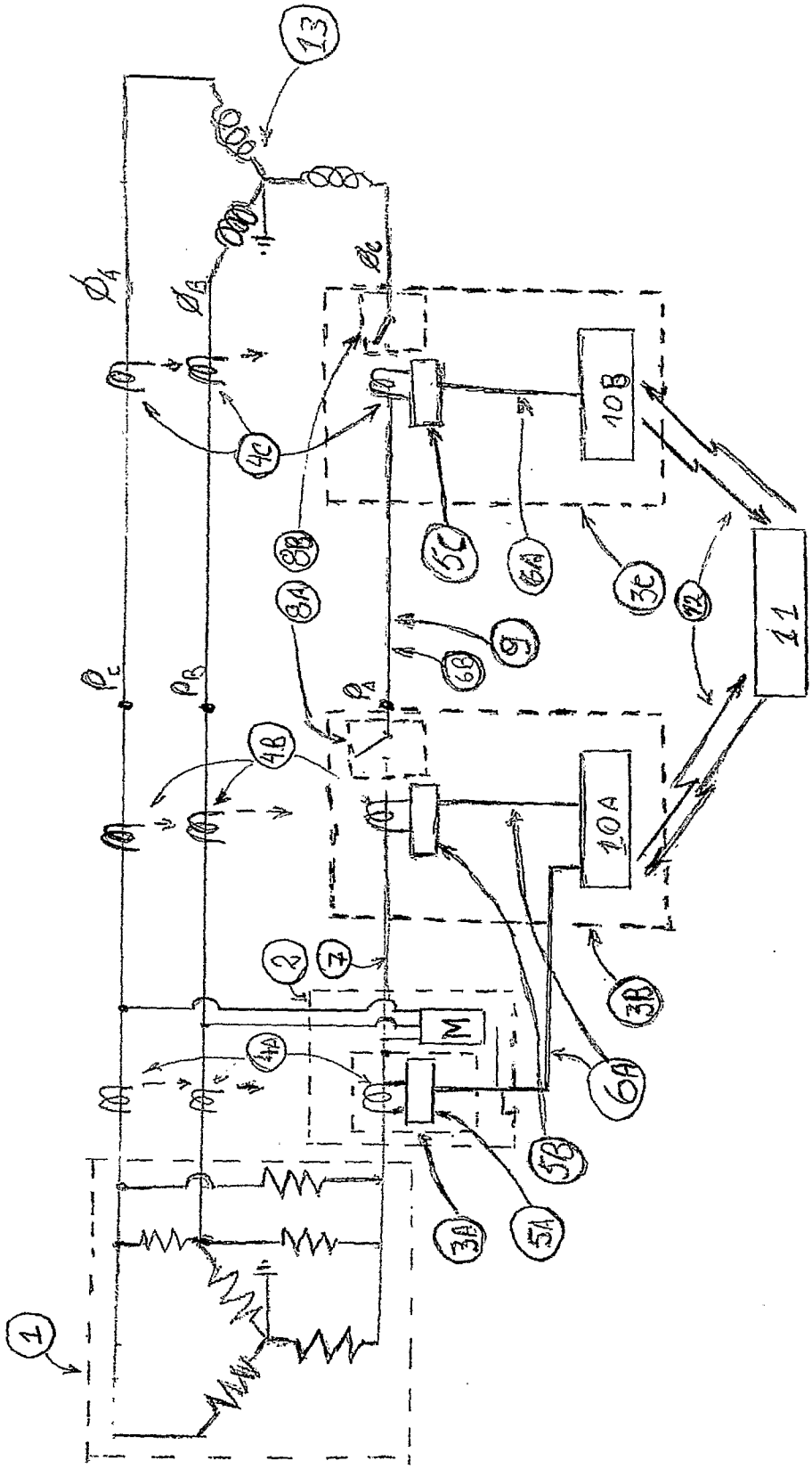
With the data and information collected, and if it is its policy, the Company may switch off remotely energy supply to the **(1) Registered Customer** or to the **(9) Branch Distributor** depending on whether or not *hooking* is being made at the registered customer, or proceed to any other measure that proves revenue loss. Depending on the scheme adopted, the **"SYSTEM"** allows for automatic switch-off/on, when *hooking* is done/undone at the **(1) Registered Customer**, and/or should it be done at a customer that is not registered at the **(9) Branch Distributor**. Such automatic action-taking are assessed remotely along with simultaneous tracking of where energy theft is being attempted. Locally, there may be a visual or sound signalization pointing toward an abnormality so that the power theft agent at a given **(9) Branch Distributor** or **(1) Registered Customer** feels constrained and deterred from going on with the power theft. Other action-taking may be adopted and are described in the Report on the Claims for.

The "System" is dubbed self-surveilled because it may trace remotely attempts to temper with the **(2) Sealed Box of the Energy Meter** as well as external changes in the magnetic field of the energy meter, when applicable. Moreover, any harm caused to the

circuits will trigger an entry data error at the **IDEE** (Intelligent Differential Electronic Equipment), thus making a remote alarm that detects problems in the **"SYSTEM"** go off.

ANNEX I




13
ϕ_A
ϕ_B
ϕ_C
4C
8B
8A
5C
6A
3C
12
9
6B
10B
11
ϕ_C
ϕ_B
ϕ_A
4B
10A
2
7
M
4A
3B
6A
5B
3A
5A
1

Annex III