(19) DANMARK

(10) DK/EP 2608981 T3

(12) Oversættelse af europæisk patentskrift

Patent- og Varemærkestyrelsen

(51) Int.Cl.: *B 60 L 11/18 (2006.01)* *G 04 G 5/04 (2006.01)* *G 04 G 7/00 (2006.01)*

(45) Oversættelsen bekendtgjort den: **2018-05-28**

(80) Dato for Den Europæiske Patentmyndigheds bekendtgørelse om meddelelse af patentet: **2018-02-28**

(86) Europæisk ansøgning nr.: **11749755.2**

(86) Europæisk indleveringsdag: **2011-07-20**

(87) Den europæiske ansøgnings publiceringsdag: **2013-07-03**

(86) International ansøgning nr.: **EP2011062409**

(87) Internationalt publikationsnr.: **WO2012025311**

(30) Prioritet: **2010-08-27 DE 102010035685**

(84) Designerede stater: **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 MK MT NL NO PL PT RO RS SE SI SK SM TR**

(73) Patenthaver: **innogy SE, Opernplatz 1, 45128 Essen, Tyskland**

(72) Opfinder: **GAUL, Armin, Hirschwiese 41, 59379 Selm, Tyskland**

(74) Fuldmægtig i Danmark: **Dennemeyer & Associates S.A, P.O. Box 700425, DE-81304 Munich, Tyskland**

(54) Benævnelse: **Sikring og synkronisering af systemtiden i en ladestation**

(56) Fremdragne publikationer:
WO-A2-2010/042550
US-A1- 2009 177 580
US-A1- 2010 006 356

SECURING AND SYNCHRONIZING THE SYSTEM TIME OF A CHARGING STATION

The invention relates to a method for synchronising a time information provided in a charging station with a system time. The invention also relates to a charging station as well as a testing location, and a system comprising a charging station and a testing location. In particular, the invention relates to devices and methods in the field of electric mobility, in particular the charging stations for electrical vehicles, and the billing of the electrical energy received by electrical vehicles.

The spread of electrically operated vehicles is expected to increase rapidly in the near future. The spread of electrical vehicles that are operated with an electric motor will, however, require that these vehicles can be supplied with energy in the simplest possible manner. A functional infrastructure needs to be made available for this purpose.

In particular, it needs to be possible for electrical vehicles to receive energy in public areas. With the currently available range for electrical vehicles being between fifty and a few hundred kilometres, it is possible that the vehicles will be charged away from the home environment. For this purpose, charging stations should be made available in public areas to provide a constant availability of energy for electrical vehicles through an electricity supply network. This availability of electrical energy and/or charging stations is an important criterion for the acceptance of electrical vehicles.

When charging stations are installed in public areas, it must be ensured that the customer pays for the energy received. The customer also needs to be aware of the expected cost of the electrical energy received. Just as with the conventional filling process, the customer should know the expected costs directly before charging the battery. Thus, the customer should know, for example, the price of a kilowatt-hour. In addition, it should be ensured that the customer is actually charged only for the amount of energy received.

There is a political will to provide different tariffs for electrical energy received at different times of day. In particular, a plurality of different time-related tariffs should be offered in future, so that there is a plurality of tariff switching times per day. Tariff switching times are always associated with changing unit rates, i.e. changing cost per unit of energy received, in particular per received kilowatt-hour of electrical energy.

In current facilities, in which there is usually only one tariff change per day, for example in the case of business and corporate customers as well as for storage heating customers, it is possible for the customer to read the time of day on the calibrated counter for the electricity (energy counter, electricity meter), and to verify whether the time agrees with the time as perceived by him. Thus the calibration authorities could assume that the

customer could always verify whether the clock associated with his counter displayed the correct time of day for determining the tariff.

However, if more than two tariff changes occur per day, the customer can no longer automatically determine whether the tariff switching times are correct. In particular, in the case of real time variability, when a plurality of tariff changes occurs per day, this is hard for the affected customer to achieve.

This problem is additionally exacerbated by energy counters having an assigned clock which is not freely accessible to the customer. Therefore it is planned, for example at charging stations for electrical vehicles, to provide these charging stations without visual displays, due to which the customer can no longer read the time of the counter. If the time base inside the charging station now deviates from the actual time, then it may happen that the amount of energy received is billed at an incorrect tariff. The customer might be able to detect this deviation because his billing document (filling receipt) shows a different charging time from the one he has noted. However, the measuring station manager at the charging station has no possibility to verify whether the time of day is correct.

Therefore, the problem addressed by the invention is that of synchronising time information provided in a charging station, secured against manipulation and falsification.

This problem is solved according to a first aspect by a method according to claim 1. In addition, this problem is solved by a charging station according to claim 11, a verification device according to claim 12 and a system according to claim 13.

During the charging procedure, the electrical vehicle receives electrical energy from the charging station. In the charging station, this electrical energy is measured using a measuring device (counter). During the charging procedure, as well as at the end of the charging procedure, it is necessary that the amount of energy received (e.g. the count of the measuring device counter) is acquired for billing purposes and the user of the vehicle is informed of the amount of energy received.

In addition to acquiring the amount of energy received and the customer information concerning the amount of energy received, it is necessary to be able to determine the tariff assigned to the received energy. In particular in the case of time variability, it can occur that during a long charging procedure, which last longer than for example six hours, a plurality of tariff changes takes place. In order to be able to accurately represent these tariff changes, it is necessary that the time information provided in the charging station is correct.

In the context of the invention, time information may be a data record which contains the time of day or date. The time information can also be a sequential number (time index), which can be converted into a time of day with a resolution of at least one second, preferably 0.1 seconds. The time information should be statutorily calibrated, so that a tariff-dependent billing is error-free and cannot be legally objected to. It is therefore necessary to ensure that the time information provided in the counter (of the charging station) is synchronised with a system time. The system time is generally the time that is used for billing by the energy supplier.

Document US2009177580 is considered to be the closest prior art and discloses the features of the preamble of independent claim 1.

According to the invention, the charging station acquires the time information. This may mean that the time information is read out and made available from a timer inside the charging station. It can also mean that the charging station consists of a charging station control device and an energy counter, and that time information is provided in the energy counter alongside information relating to the energy received. In this case, the time information acquired from the energy counter can be read out from the charging station control device via an appropriate interface.

The acquired time information is processed inside the charging station in such a way that it can be transmitted to a central testing location. This transmission can be made for example by radio, for example over a mobile telephone network. It is also possible that the transmission of the time information is made by means of Power-Line Communication over the energy cable via which the charging station is connected to a transformer station and to the energy supply network connected thereto. Other transmission methods are also possible.

A monitoring circuit can be installed in the energy counter or the charging station, with the aid of which each modification to the time can be determined. In such a case, an error index intended for this purpose can be modified, preferably incremented. This can mean that each setting of the time of day causes a modification of the error index. The monitoring circuit can be configured such that a tolerance threshold makes it possible to distinguish between a modification of the time of day and a synchronisation. Such a tolerance threshold could be, for example, less than 30 seconds, preferably less than 27 seconds or also less than 23 seconds or also less than 10 seconds. A modification of the error index may only be necessary in the case of a change of the time that is greater than the tolerance threshold.

In such a method according to the invention, it is proposed to transmit the current time information acquired after step a) and the value of the error index after step b).

The transmission can be secured. In particular, it is proposed that the exchange of the time information between the charging station and the testing location is carried out using the NTP protocol. In this way, the Autokey method can also be used. The Autokey method ensures that the transmitted information is secured against manipulation. In this way, it is possible that the transmitted information items are transmitted with a signature. In this way, it is possible, for example that the data record (data packet) containing the time information is signed and/or encrypted with a private key of the charging station (and/or of the counter). The charging station number, a status word, a counter count, counter status or the like can also be contained in the data record alongside the time information and the error index.

After the error index and the current time information are transmitted to the testing location, it is proposed according to the invention that a new time information is requested by the charging station from the testing location according to step c). In this way a secure communication can occur, in particular according to the NTP v.4 protocol. Step c) can be secured according to the Autokey method. In step c), a system time is transmitted from the testing location to the charging station. This system time is then used to synchronise the charging station with the testing location.

The testing location transmits a new time information to the charging station in step c). This means that a transmission latency can already be taken into account. Thus signal propagation times between testing location and charging station in the context of the communication between testing location and charging station can be measured and the new time information can already be adjusted around the measured latency. The transmission of the new time information from the testing location to the charging station can take place without a signature and/or encrypting. This is particularly necessary if the transmitted time information needs to be available as soon as possible in the charging station. The checking of a signature and/or the decrypting of the new time information in the charging station can give rise to a time delay, which is undesirable. Because the time required for checking a signature and/or a decryption is variable, the time delay cannot be taken into account in advance, which means that after checking the signature and/or the decryption in the charging station, the new time no longer agrees with the system time and there can be a difference of 10 seconds to 3 minutes.

Subsequently, a comparison can be made in the charging station between the requested new time information and the current time information already provided in the charging station. Because the latency of the new time information has already been corrected, the new time is almost synchronous with a current acquired time in the charging station or the energy counter, provided that the current time has not been modified since the last synchronisation and the clock has not gone wrong. In the sense of this comparison, synchronous can mean a difference of less than one a minute, preferably less than 27 seconds.

If the current time is no longer synchronous with the new time, then it can be concluded that the time in the counter has been manipulated or the clock in the counter has not correctly acquired the time, for example is faulty.

If the current time information does not agree with the new time information, then the current time information must be reset in the counter. It is possible to differentiate between a resetting and a synchronising of the current time information with the new time information, in such a way that a synchronisation involves a modification of the current time information of less than 30 seconds, preferably less than 27 or 20 seconds, whereas a resetting involves a greater modification of the current time information.

It is also proposed that, according to step e) an error index is modified in the charging station if a difference is found between the requested new time information and the current time information provided in the charging station, which is greater than a threshold value. As explained above, the threshold value makes it possible to distinguish between a synchronisation and a resetting. As already explained, the error index is also modified in the case of other events. A resetting or other modification of the current time thus causes a modification of the error index.

The current time is set to the new time, as proposed according to step f). This can involve either a synchronisation or a resetting.

Then, the current time information set according to step f) together with the value of the error index is transmitted to the testing location. Here too, the NTP protocol can be used, in particular with the use of the Autokey method. Before step g), it is possible that the current time information is first given a signature.

In step g), the charging station can transmit, to the testing location, the most recent stored time information with a signature, the current time information and the value of the error index. These can be sent together with an "End Session Signal" to the testing location, in order to close a communication channel.

Then, the values of the error indices which were transmitted in steps b) and g) can be compared in the testing location. The comparison of the error index transmitted in step b) with an error index previously transmitted during a time comparison in a step g) can make apparent a manipulation of the time in the counter. If the time information has not been manipulated, then the error index must remain unchanged. Thus it can be established at the testing location, in which interval a change in the time information has taken place in the charging station.

If the error indexes agree, then the current time information is synchronised with the new time information, as described above. Otherwise, the current time information is reset with the new time information, and it can be concluded that the current time information has been falsified in the period since the last synchronisation. It can then be determined how large the actual time difference was. Since, according to the invention, in step b) the old current time information and in step g) the new current time information were transmitted, a comparison of these time information items can provide information regarding how large the time error was.

It is also proposed that the charging station stores the current time information, in particular before steps b) and/or f) and/or at regular, preferably uniform intervals, with a signature. Storage with a signature makes it possible to check, retrospectively, the time information items in the charging station. The signing makes subsequent manipulation of this data difficult.

It is also proposed that a charging station identifier is additionally acquired in step a), and that the charging station identifier and/or the most recent time information stored with a signature is additionally transmitted in step b), and/or that the charging station identifier and/or the most recent time information stored with a signature is additionally transmitted in step f).

With the aid of the charging station identifier, it is possible to identify the charging station in the testing location. The testing location can be sent a so-called NTP "Start Session" signal together with the charging station identifier. This is a signal according to the NTP standard. This allows a time synchronisation to be initiated, which can take place over a secure communication channel. Such a communication channel can be kept open over a time window of, for example, several minutes, e.g. 30 minutes. In step c), the new time information can be transmitted over this communication channel.

Through the transmission of the stored time information with a signature, it is possible at the testing location to check the identity of the charging station, wherein the signature is

checked. The transmission of the time information items already stored with a signature, eliminates the need for the time-consuming signing of the current time information at the time of synchronisation.

It is also proposed that the information items transmitted in step b) and/or in step f) are stored in the testing location respectively with a signature and/or with time information items of the testing location. The testing location can provide the received information items with its own time information items and then store them. These values can be stored together with the charging station identifier. The times at which the communication channel was opened and closed can also be stored. The storage can take place using a signature of the testing location. This increases data security against manipulation. The transferred data is thus stored in the testing location secured against manipulation.

It is also proposed that after reception of the charging station identifier transmitted in step b), the testing location keeps a communication channel open for a request according to step c) by the charging station identified by means of the charging station identifier. As previously explained, the communication channel can be kept open for a specified time. A synchronisation can take place within the time window of the communication channel. The testing location can monitor, or within the time window receive, a signal according to step g). In this way, it can be checked whether the charging station identifier according to step b) corresponds with the charging station identifier according to step g), whereby it can be ensured that the requesting charging station also completes the time synchronisation.

It is also proposed that a threshold value of more than 10 seconds, preferably more than 20 seconds, particularly preferably more than 23 or 27 seconds, is specified in step e). As already explained, it is possible to distinguish between a synchronisation and a resetting of the current time information. Only in the case of resetting is it necessary to record an alarm entry in a logbook, which can be followed up.

It is also proposed that the testing location closes the communication channel after reception of the charging station identifier transmitted in step f). In this case, the synchronisation is completed and the secure communication channel can be removed. In this case, it can also be concluded that the synchronisation was actually carried out. Otherwise, an alarm entry can be written in a logbook.

It is also proposed that an alarm signal is generated if there is a difference between the values of the error indices in step h), and/or an alarm signal is generated if information is

missing in the testing location according to step g). An alarm signal can cause an alarm entry in a logbook.

It is also proposed that a list of charging station identifiers is stored in the testing location, and that information items transmitted according to step b) are tested for their permissibility with the aid of stored charging station identifiers. Thus it is possible to determine whether a synchronisation request comes from an already known charging station and whether this request is permissible. It is possible that a request comprising a charging station identifier, which is not yet known, is refused or remains unanswered. The request can also be answered and the charging station identifier included in the list.

It is also possible that a list of charging station identifiers is stored in the testing location, and that a check is made at regular intervals as to whether the associated charging stations have transmitted information items according to steps b) and g). This makes it possible to check whether all charging stations synchronise their time. If a charging station from the list has undertaken no synchronisation within a specified time window, for example 24 hours, an alarm entry can likewise be generated in a logbook.

The terms “signature”, “to sign”, etc., can be understood in the sense of an electronic data signature. The electronic signatures of the data packets can also ensure that these have not been subsequently manipulated.

A signature can be computed using a unique, preferably binary, key generated from the data packet and assigned to the measuring device (counter) or the charging station or the testing location. A reference value can be computed from the data packet, for example a hash code. This reference value can also be used to calculate the signature. This signature can be computed, for example using the hash codes and a key assigned to the measuring device (counter) or the charging station or the testing location. A signature can also be directly computed from the data packet and the key assigned to the measuring device (counter) or the charging station or the testing location.

Signing can involve generation of a cryptogram as a signature using a preferably binary key, wherein using the key and the data packet to be signed, or the reference value computed therefrom, a preferably binary cryptogram is generated. It is possible, by means of such a cryptogram, to verify whether the data packet was indeed generated by the charging station.

An electronic signature can also be understood to mean data combined with electronic information, with which the signer or signature creator can be identified and the integrity of the electronically signed information can be checked. This electronic information

usually concerns electronic documents. Therefore the electronic signature fulfils the same purpose, from a technical perspective, as a handwritten signature on a paper document. An electronic signature can comprise, inter alia, a digital signature. The digital signature can be the pure, data-technology cryptographic signature, to which cryptographic mathematical methods are applied. “Electronic signatures” can be data in electronic form, which accompany other electronic data or are logically associated with same, and which serve as authentication.

A signature can be generated by means of an SHA-256 method. A variant FIPS 180-2 can also be used for this purpose. In particular, a signature can be generated using an elliptic-curve cryptographic (ECC) method. Here it is possible, for example, to use an ECC method with 192 bits.

The signature of the data packet is used to ensure that the information items contained in the data packet are inseparably connected. If one of the information items is modified, then a different signature would result.

Comparison in the sense of the invention can be understood to mean that the time of day associated with the current time information and/or the date associated with the current time information can be compared with a time of day and a date of a new time information. A comparison may include determining a difference.

An advantageous exemplary embodiment proposes that the time information is provided in a counter, a counter device or an auxiliary device of the charging station connected with these. In this way, it is possible that the time information is made available by the device, which is also statutorily calibrated for the measurement of the received amount of energy. In particular, the time information should be made available by a device inside the charging station.

The features of the methods and systems can be freely combined with one another. In particular, features of the dependent claims, bypassing the features of the independent claims, can be inventive in their own right, individually or freely combined with one another.

The above mentioned methods can also be carried out as a computer program or as a computer program stored on a storage medium. For this purpose, a microprocessor on the vehicle, charging station and/or billing centre (testing location) can be suitably programmed for carrying out the respective method steps using a computer program.

The invention is explained in more detail below on the basis of drawings depicting an exemplary embodiment. The figure shows:

figure 1, a schematic design of a system for charging an electrical vehicle;

figure 2, a schematic design of a testing location; and

figure 3, a flow diagram of a method according to a first exemplary embodiment.

Figure 1 shows a charging station 2 which is connected to a vehicle 6 by means of a connecting cable 4. A connection socket 8 is provided in the charging station 2 for connection of the connecting cable 4. Both energy transfer and data exchange are carried out between vehicle 6 and charging station 2 over the connecting cable 4.

The electrical power is received via an electrical connection 12 of an electrical energy supply network 14.

A measurement device 10a and a clock 10b can be arranged in a counter 10.

A computing unit (control device) 16 comprising a communications unit 16a and a signature unit 16b is coupled to the measuring device 10a. The signature unit 16b can have a unique identification assigned to the charging device 2 and/or the measuring device 10a, for example a private measuring device key 18a. It can also comprise a public measuring device key 18b. The signature unit 16b can also be a component of the counter 10.

The computing unit 16 is connected to a billing centre 22 via a data network 20.

The connection socket 8 is electrically connected to the measuring device 10a. The measuring device 10a measures the electrical power which is supplied via the connection socket 8 to the vehicle 6 via the connecting cable 4. In addition a clock 10b is coupled to the measuring device 10a. The clock 10b generates local time information and makes this available. This time information can be made available in the form of a data record.

The clock 10b can be adjusted by means of an external control signal A memory (not illustrated) is provided in or on the clock 10b, in which the local time information items are stored at intervals.

The stored time information items can be signed by the signature unit 16b, wherein the signature can be produced using the measuring device key 18, preferably the private measuring device key 18a. The signed time information items can be stored. The counter counts can be stored together with the stored time information items. Thus data records consisting of at least counter count and time information can be stored in the memory.

Further, a testing location 23 is provided which is logically and spatially separated from the billing centre 22 and the charging station 2. In particular, the testing location 23 can be connected to the data network 20, e.g. a wide area network, for example the Internet.

The testing location 23 can be operated for example on the premises and/or under the supervision of a calibration authority.

The testing location 23 can be connected with a time server 23a and obtain time information from the time server, e.g. also via the data network 20. The time server 23a can be under the supervision of a calibration authority.

In particular, it is possible to obtain the time information items from the clock 10b and make them available for further processing. This may include the local time information being transmitted to the testing location 23 over the data network 20. Further, the testing location 23 can also access the local time information over the data network 20. The data records with time information and measuring device counter count stored in the memory can also be called up and loaded by the testing location 23.

The clock 10b can be controlled by an external time signal (control signal). In this case, the clock 10b can receive a time signal from a timer, in a wireless e.g. via DCF77 or wired manner, e.g. over the data network Using this signal, it is possible to keep the local clock 10b as accurate as possible. However, it is possible to manipulate this time signal. A manipulation causes the clock 10b to provide incorrect time information. The clock 10b can also be self-adjusted.

The method for synchronising the clock 10b with the time of the testing location 23 or of the time server 23a, and for checking whether the clock 10b has been manipulated, is illustrated in figure 3.

A manipulation of the time information can be detected locally in the charging station 2, by regularly comparing the current time information items with stored time information items. The current time information must always be more recent than the stored time information items. Otherwise, a protocol entry can be generated and stored. Protocol entries can also be sent to the testing location 23. Finally, a status bit (measuring device status) can be set for a detected error.

A communication unit 28 is provided in the vehicle 6, in addition to a battery 26 connected to a connector 29. The communication unit 28 enables sending and receiving of data on the connecting cable 4. A signature unit 30 is connected to the communication unit 28. The signature unit 30 can obtain a unique identification 32 from the vehicle 6.

During the charging procedure of the vehicle 6 at the charging station 2, energy from the energy supply network 14 is stored in the battery 26 of the vehicle 6. The amount of stored energy is acquired by means of the measuring device 10a. The amount of energy, for example a counter count of the measuring device 10a, as well as other data, such as the

identification of the charging station 2 and/or the identification of the measuring device 10a, time information items such as a time stamp, a time of day, a date and/or a time index of the clock 10b, a status of the charging station 2 and/or a status of the measuring device 10a, a starting counter count, an end counter count and/or the like, can be transmitted via the connecting cable 4 to the vehicle 6 and/or the billing centre 22 and/or the testing location 23.

For this purpose, the communication unit 16a transmits a data packet. The stated measurement values can be stored in the data packet. A public measuring device key 18b can also be stored in the data packet. As well as the data packet, the public measuring device key 18b and/or signatures can be exchanged between charging station 2 and vehicle 6 and/or billing centre 22 and/or testing location 23.

Figure 2 shows a schematic structure of a testing location 23. It can be seen that the testing location is connected to the data network 20 via a communications unit 34 and time information and measuring device counter counts can be received from the charging station 2 over this connection. The exchange of time information items and measuring device counter counts can be carried out using push or pull methods.

A comparator device 36 is arranged in the testing location 23 and in a memory 38. Together with the time information items, the received measuring device counter counts that are assigned to the time information items can also be stored in the memory 38.

The testing location can receive an internal or external time signal from a timer 23a. The timer 23a is preferably a calibrated timer, the time standard of which is recognised by the testing location 23 as reliable and legally permitted.

In particular, in the case of charging stations 2 for electrical vehicles 6, charging times are particularly long, usually more than one hour Due to the need to make available time-variable tariffs, a tariff change can occur during a charging process. Such tariff changes result in different electricity prices, so that it is necessary that the time-base by means of which the amount of received energy is calculated, is correct.

Manipulations of the time base are to be avoided and, should manipulations occur, these must be identified as certainly as possible.

The synchronisation of the time information items in the charging station 2 is schematically illustrated in figure 3.

Figure 3 illustrates the course of a communication between a counter 10, the computing unit 16, the testing location 23 and the timer 23a.

It can be seen that time information items of the clock 10b are stored (40) in the counter 10 at regular intervals. This can be every few minutes, for example every 2 minutes, every 6 minutes, every 10 minutes, etc. In this way, the time information can be saved with a signature, with the aid of the measuring device key 18. The storing (40) can take place in a memory in the counter 10.

It can also be seen that the testing location 23 receives (41) time information items from the timer 23a at regular intervals. This can take place in the context of an NTP time synchronisation between the testing location 23 and the timer 23a.

At a point in time, at which a synchronisation of the time information between the clock 10b and the testing location 23 is required, e.g. regularly once per day, or every 6 hours or the like, a request (42) is triggered by the computing unit 16 directed to the counter 10, by means of which the computing unit 16 requests at least the most recent stored value of time information with a signature, which was stored in step 40, the current time information of the clock 10b, a counter identification and a value of an error index.

The error index can be monitored by a monitoring circuit in the clock 10b. This monitoring circuit constantly checks (at monitoring intervals of, for example, 1 second, 5 seconds, 10 seconds, etc.), whether the time of day in the clock 10b is strictly monotonically greater and whether there are time jumps. In this way, the monitoring circuit can monitor a threshold value. The time of day in the clock cannot differ by more than the threshold value between two monitored intervals. In this way it can be checked, for example, whether or not the time of day in the clock has changed in the monitoring interval by more than the threshold value. If the time of day changes by more than the threshold value, a value of the error index can be incremented, e.g. by 1. If the time of day changes by less than the threshold value, a synchronisation can be carried out, which is not a reportable event.

The requested values are transmitted (44) from the counter 10 to the computing unit 16. A data packet is formed in the computing unit, from at least the requested values of the time information with a signature, the current time information, the counter identification and the value of the error index.

This data packet is transmitted (46) together with a Start Session signal from the computing unit 16 to the testing location 23.

The testing location 23 receives the data packet and the Start Session signal. Then the testing location checks (48) whether the counter identification corresponds with a counter

identification stored in a list. If not, the testing location 23 can reject the request 46 leaving it unanswered or add the corresponding counter identification in the list.

Then the testing location 23 checks (50) the validity of the request on the basis of the signature of the signed time information and the counter identification.

Finally, the testing location 23 adds its current time information to the data packet and signs the thus supplemented data packet. This data packet with a signature is stored (51) in a memory 23b of the testing location 23.

In addition, a data channel for an NTP synchronisation is opened with the requesting charging station 2.

The computing unit 16 starts a time synchronisation attempt 52. This can take place using the Autokey protocol of the NTP protocol. In this case the computing unit 16 sends the counter identification to the testing location 23. On the basis of the counter identification, the testing location 23 can check whether the time synchronisation attempt 52 originates from the previously requesting charging station 2, since the counter identification would already have been previously transmitted and the communication channel can be assigned to the counter identification.

The testing location then transmits (54) a new time information to the computing unit 16, taking account of signal propagation times. The NTP protocol is used for this purpose, which ensures short signal propagation times and takes account of the propagation time latency.

The computing unit transmits (56) the received new time information to the clock 10b of the counter 10.

The time information in the clock 10b is set (58) to the value of the new time information.

The monitoring circuit checks (60) the value of the modification of the time information. If this is less than the threshold value, the error index remains unmodified. Otherwise, the error index is modified. This means that if either at the time of synchronisation (58) or at an earlier point in time, the time of day was reset or manipulated, then the error index is modified

Then, in accordance with step 42, the computing unit again requests (62) data from the counter. These data contain the most recent time information stored with a signature, the current time information, the error index and the counter identification. These data are transmitted 64 from the counter 10 to the computing unit 16.

The computing unit sends (66) an End Session signal together with the previously received data to the testing location 23.

In the testing location, it is checked (68) whether a communication channel is open for the included counter identification. If so, the communication channel is closed (70). If not, the message is discarded.

Then the testing location 23 adds the received data to its current time information and supplements (72) the data packet with a signature.

The supplemented data packet is then stored (74) in the memory 23b.

It is then noted in the list that a time synchronisation has been carried out for the associated counter identification. Thus it can be checked in the list for which counter and in which time period, time synchronisations were carried out. If a counter has carried out no identification in a specified time period, a logbook entry is generated.

In addition, the error indices stored in steps 51 and 74 can be compared with one another. If the counter index has changed, then a resetting of the time of day of the clock 10b is carried out, and a logbook entry is likewise generated.

In this way, it can be checked at which point in time the error was established.

With the aid of the described method, it is possible to establish whether a time of day has been manipulated in a counter. In addition, through regular synchronisation of the clock 10b, it is ensured that the clock 10b is generally synchronous with the time base in the testing location.

Sikring og synkronisering af systemtiden i en ladestation

Patentkrav

1. Fremgangsmåde til indstilling af en tidsinformation i en ladestation (2) til elkøretøjer (6), omfattende:

a) registrering af den aktuelle tidsinformation, der leveres i ladestationen (2), og af en værdi i et fejlindeks, der kan ændres i forbindelse med en ændring af tiden over en tolerancetærskel,

b) overførsel af den aktuelle tidsinformation sammen med værdien fra fejlindekset fra ladestationen (2) til et centralt kontrolsted (23), der er rumligt adskilt fra ladestationen (2),

c) forespørgsel om en ny tidsinformation fra ladestationen (2) i det centrale kontrolsted (23),

d) sammenligning af den forespurgte nye tidsinformation med den aktuelle tidsinformation, der leveres i ladestationen (2), i ladestationen (2),

e) ændring af et fejlindeks, hvis en konstateret afvigelse mellem den forespurgte nye tidsinformation og den aktuelle tidsinformation, der leveres i ladestationen, er større end en grænseværdi, i ladestationen (2),

f) indstilling af den aktuelle tidsinformation i ladestationen (2) til den nye tidsinformation,

g) overførsel af den aktuelle tidsinformation, der er indstillet i henhold til trin f), sammen med værdien fra fejlindekset til det centrale kontrolsted (23),

h) sammenligning af værdierne, der er overført i trin b) og g), fra fejlindeksene i det centrale kontrolsted (23).

2. Fremgangsmåde ifølge krav 1, **kendetegnet ved**, at ladestationen (2) gemmer den aktuelle tidsinformation signeret, særligt inden trin b) og/eller f) og/eller i regelmæssige, fortrinsvis ensartede intervaller.

3. Fremgangsmåde ifølge krav 1 eller 2, **kendetegnet ved**, at der i trin a) desuden registreres en ladestationsidentifikation, og at ladestationsidentifikationen og/eller den seneste tidsinformation, der er gemt signeret, desuden overføres i trin b), og/eller at ladestationsidentifikationen og/eller den seneste tidsinformation, der er gemt signeret, desuden overføres i trin f).

4. Fremgangsmåde ifølge et af kravene 1 til 3, **kendetegnet ved**, at informationerne, der overføres i trin b) og/eller i trin f), hver især signeres i det

centrale kontrolsted (23) og/eller gemmes med tidsinformationer fra det centrale kontrolsted (23).

5. Fremgangsmåde ifølge et af kravene 3 til 4, **kendetegnet ved**, at det centrale kontrolsted (23) efter modtagelsen af ladestationsidentifikationen, der overføres i trin b), opretholder en kommunikationskanal til en forespørgsel i henhold til trin c) fra ladestationen (2), der er identificeret ved hjælp af ladestationsidentifikationen.

6. Fremgangsmåde ifølge et af kravene 1 til 5, **kendetegnet ved**, at der i trin e) er fastlagt en grænseværdi, der er større end 10 sekunder, fortrinsvis større end 20 sekunder, særligt foretrukket større end 23 henholdsvis 27 sekunder.

7. Fremgangsmåde ifølge et af kravene 5 til 6, **kendetegnet ved**, at det centrale kontrolsted (23) efter modtagelsen af ladestationsidentifikationen, der overføres i trin f), lukker kommunikationskanalen.

8. Fremgangsmåde ifølge et af kravene 1 til 7, **kendetegnet ved**, at der, hvis værdierne i fejlindeksene i trin h) afviger fra hinanden, genereres et alarmsignal, og/eller at der, hvis der mangler en information i henhold til trin g) i det centrale kontrolsted (23), genereres et alarmsignal.

9. Fremgangsmåde ifølge et af kravene 1 til 8, **kendetegnet ved**, at der i det centrale kontrolsted (23) er gemt en liste med ladestationsidentifikationer, og at informationer, der overføres ved hjælp af de gemte ladestationsidentifikationer i henhold til trin b), kontrolleres med henblik på deres tilladelighed.

10. Fremgangsmåde ifølge et af kravene 1 til 9, **kendetegnet ved**, at der i kontrolstedet er gemt en liste med ladestationsidentifikationer, og at det i regelmæssige intervaller kontrolleres, om de tilhørende ladestationer (2) har overført informationer i henhold til trin b) og g).

11. Ladestation (2) til elkøretøjer, der omfatter anordninger til udførelse af trinnene i fremgangsmåden ifølge kravene 1-10 og desuden omfatter:

- en tæller (10b), der er indrettet til at levere en lokal tidsinformation,
- registreringsanordninger, der er indrettet til registrering af tidsinformationen, der leveres i ladestationen (2), kommunikationsanordninger (16), der er indrettet til at sende aktuelle tidsinformationer og modtage nye tidsinformationer,
- sammenligningsanordninger (36), der er indrettet til at sammenligne de aktuelle tidsinformationer med de nye
- tidsinformationer og til at ændre et fejlindeks, der kan ændres ved en ændring af tiden over en tolerancetærskel, hvor
- kommunikationsanordningerne (16) er indrettet til at sende fejlindekset.

12. Kontrolanordning, der omfatter anordninger til udførelse af trinnene i fremgangsmåden ifølge kravene 1-10 og desuden omfatter:

- overførselsanordninger (34), der er indrettet til at modtage en værdi for et fejlindeks fra en ladestation (2), der kan ændres ved en ændring af tiden over en tolerancetærskel,
- sammenligningsanordninger (36), der er indrettet til at sammenligne det modtagne fejlindeks med et fejlindeks, der er gemt i det centrale kontrolsted (23), og
- lagringsanordninger (38), der er indrettet til at gemme en fejlpostering.

13. System med i det mindste en ladestation (2) ifølge krav 11 og en central (23) ifølge krav 12.

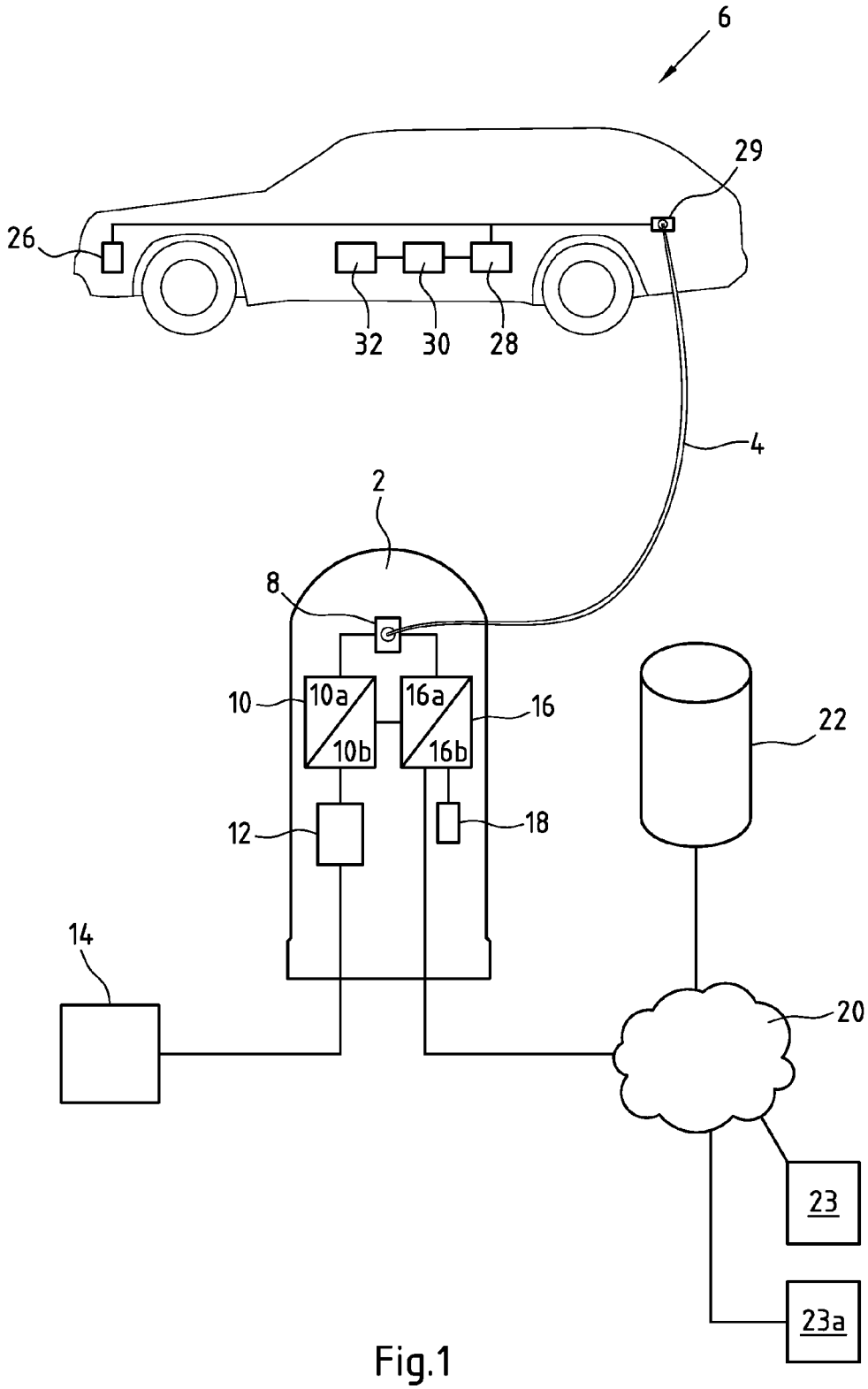


Fig.1

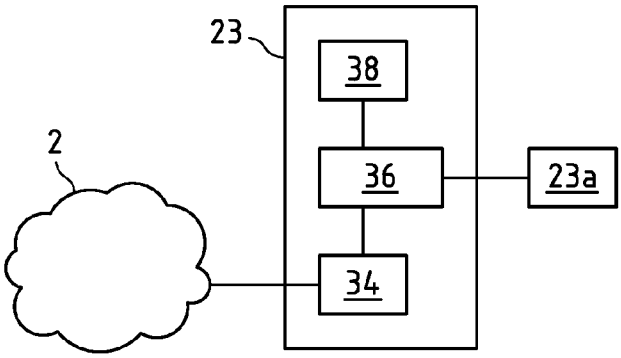


Fig.2

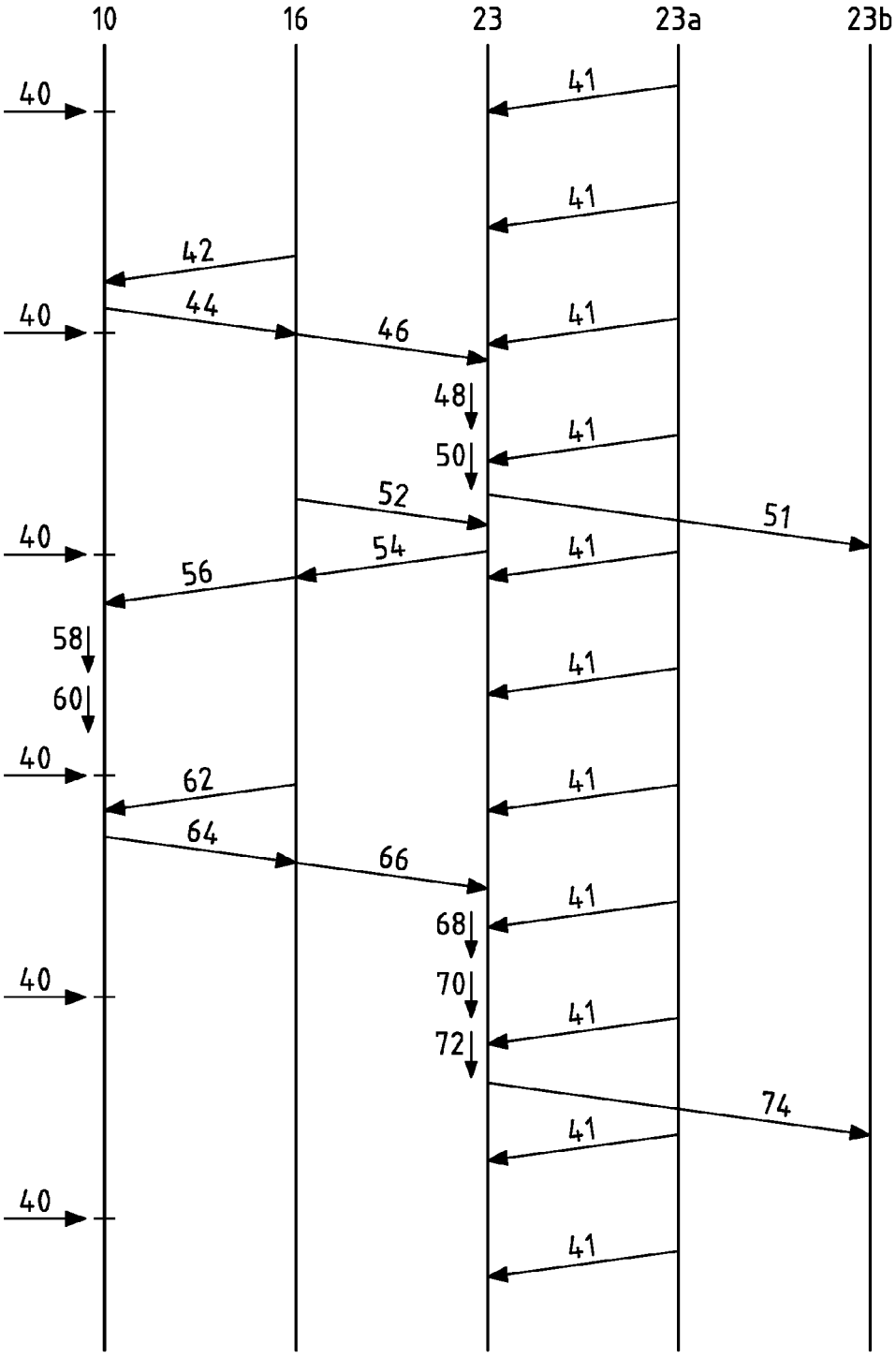

10
16
23
23a
23b
40
41
42
44
46
48
50
52
51
54
56
58
60
62
64
66
68
70
72
74

Fig.3