

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
3 August 2006 (03.08.2006)

PCT

(10) International Publication Number
WO 2006/080863 A2

(51) International Patent Classification:

H02J 13/00 (2006.01) **H01R 13/70** (2006.01)
G06Q 10/00 (2006.01)

(21) International Application Number:

PCT/PT2006/000004

(22) International Filing Date: 25 January 2006 (25.01.2006)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

103228 25 January 2005 (25.01.2005) PT

(71) Applicant and

(72) Inventor: **NEVES DUARTE, Luis, Augusto** [PT/PT];
Praceta 1° de Maio, N°12-5° Drt., P-2745-316 Queluz (PT).

(74) Agent: **SARDIÑA DE BARROS, Joãos, Carlos**; Praça
Duque da Terceira, N°24-3°Esq., P-1200-161 Lisboa (PT).

(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,

AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,
CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI,
GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV,
LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI,
NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG,
SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US,
UZ, VC, VN, YU, ZA, ZM, ZW.

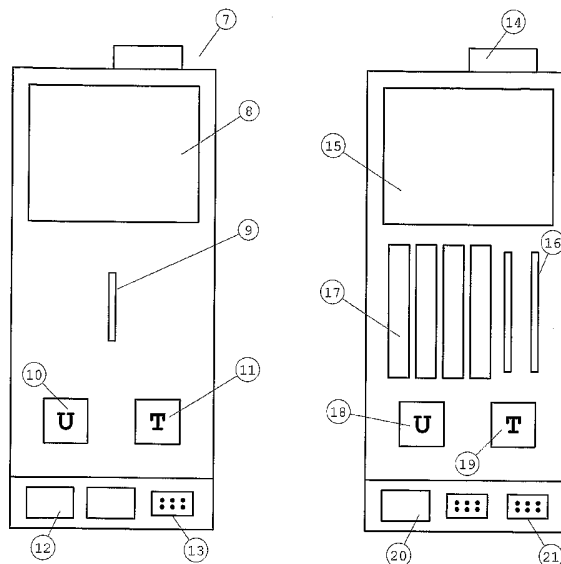
(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,
ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, 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

For two-letter codes and other abbreviations, refer to the "Guid-
ance Notes on Codes and Abbreviations" appearing at the begin-
ning of each regular issue of the PCT Gazette.

(54) Title: REMOTE SAFETY SYSTEM



(57) Abstract: The Remote Safety System is an electronic system that avoids the peril of electrocutions in high-tension electrical grids. It is characterized in that each switch has a lock with a safety key, which is blocked/unblocked by a remote unit (fig. 1), and in that it exists a remote unit (fig. 2) for every point of the electrical grid needing repairs. The remote unit has set of working cards (17) that are distributed to workers, which are returned after the repairs have finished. When the safety key is blocked inside the central unit, the working cards (17) are unblocked inside the remote unit, and vice versa. The safety key is never unblocked at the same time of the working cards. Each central unit communicates with every remote unit using modems, or transceivers, or mobile phones.

WO 2006/080863 A2

REMOTE SAFETY SYSTEM

Introduction

The Remote Safety System provides a safe environment to workers repairing electrical grids as well as equipment in big industrial compounds. As the Remote Safety System is specially devised to be employed in high-tension electrical grids, so, from now on, the description will use as an example of application a high-tension electrical grid.

Nowadays, when there is the necessity to repair a malfunction in a high-tension electrical grid, the safety officer turns the switch off in order to disconnect the electric power, locks it with a padlock, and communicates via transceiver, telephone, mobile phone, Internet, etc., to the repairing team manager that the electrical power is already disconnected. When the repairs have finished, the repairing team manager communicates back to the safety officer that the repairs finished and therefore he can unlock the switch and connect the electric power. Due to the long distance between the point of the electrical grid needing to be repaired and the switch that disconnects it, the following safety problems could arise:

- Workers can have doubts about whether the electrical grid has been disconnected before starting the repairs.
- The electrical grid can be improperly connected when workers are proceeding with the repairs
- The safety officer can have doubts about whether workers have already finished the repairs at the time he wants to connect the electrical power.

The Remote Safety System overcomes the abovementioned safety problems. It ensures to workers going to repair an electrical grid that it is disconnected beforehand. It also ensures to workers that during the repairs it is impossible to connect the electrical power.

Otherwise, the safety officer can only connect the electrical power when all workers have already finished doing the repairs.

Basic and minimalist composition of the Remote Safety System

The Remote Safety System is basically and minimally composed of:

- One locking device (figs. 1 and 2) - The locking device must be attached to the switch that disconnects the electrical grid. It is used to lock the respective switch in the off position, using for this a unique safety key.
- One central unit (fig. 3) - The central unit should be near to the switch to be turned off. It is used to receive and block the safety key, and afterwards, to send a message to the remote unit indicating that the safety key is blocked, and consequently that the respective switch is locked in the off position. It is also used to receive a message from the remote unit telling that all the respective working cards are blocked. Afterwards the safety key is unblocked, and using it the safety manager can unlock and turn on the respective switch.
- One remote unit (fig. 4) - The remote unit should be near to the point of the electrical grid needing repairs. It has a set of working cards. The remote unit, after receiving a message from the central unit indicating that the safety key is blocked and consequently the respective switch is off and locked, unblocks the working cards. Then, each worker, before starting working, picks one working card from the remote unit. When all the repairs have finished, each worker puts back his working card into the remote unit, where all of them are blocked. Afterwards, the remote unit sends a message to the central unit indicating that all working cards are blocked, and consequently the repairs on the electrical grid have already finished.
- Two communication units - One is attached to the central unit, and another is attached to the remote unit. They allow the exchange of messages between the central unit and the remote unit.

Additional notes

In order to avoid critical moments in terms of the safety of the workers, the Remote Safety System has the following constraint: the safety key in the central unit and the working cards in the remote unit are never unblocked at the same time.

The above-mentioned description refers to a relation from only a central unit to only a remote unit. There can be relations from each of several central units to several remote units.

Description of the components**The locking device of the switch****Composition**

Each switch that disconnects the electrical power must have a locking device attached. The locking device (figs. 1 and 2) is composed of:

- A curved bar (2) with a window (3), which curved bar is bonded to the lever (1) of the switch.
- A lock (5) with a rotating bolt (4)
- A safety key (6);

Functioning

The lock (figs. 1 and 2) (5) must have the following mechanical restrictions:

- The safety key (fig. 2) (6) can only be taken out from the lock (5) when the lever (1) of the switch is in the off position and the lock is in the locked position.
- The safety key (fig. 1) (6) remains blocked inside the lock (5) when the lever (1) of the switch is in the on position and the lock is in the unlocked position.

The safety key (fig. 5) (31) is unique in relation to the switch at which it belongs (it cannot be used unduly in another switch). It also must have a unique code that identifies uniquely the switch at which it belongs. The code can be either of optical type or electronic type. In the case of the code being of optical type, then the key must have a set of holes (30) representing a code, which must be read by an optical array. In the case of the code being of electronic type, it must be provided by a Radio-Frequency Identification (RFID) tag embedded in the safety key. In this case, the code of the safety key must be read by a RFID transceiver.

The safety key is also composed of a notch (29) and a ramp (28).

When the lever (fig. 1) (1) of the switch is in the on position, the safety key (6) remains blocked inside the lock (5). At this position it is impossible to rotate it because the solid part of the curved bar (2) prevents the bolt (4) from rotating. Thus, the safety key cannot be taken out from the lock with the aim of using it improperly.

To disconnect the electrical power, the safety officer must pull the switch lever into the off position (from fig. 1 to fig. 2). At this position (fig. 2), the safety key (6) must be turned, and consequently, the mechanism of the lock forces the bolt (4) to rotate into the window (3). Due to this action, the lever (1) of the switch gets locked into the off position, and after that the safety key (6) can be taken out.

To connect again the electrical power (from fig. 2 to fig. 1), the safety officer must put the safety key (fig. 2) (6) in the lock (5), and turn it into the opposite direction of the above-mentioned direction. Consequently, the mechanism of the lock (5) forces the bolt (4) to rotate out of the window (3), thus unlocking the lever (1) of the switch. Afterwards, the safety officer must push the lever (1) of the switch into the on position. At this position, the safety key remains blocked inside the lock.

The communication units

The communication unit enables the communication between each one of several central units and one or more remote units. So, each central and remote unit must have a communication unit attached through the communication connector ((fig. 3) (7) and (fig. 4) (14)). The communication units can be transceivers, modems, mobile phones, etc. They must have a communication protocol capable of recovering transmission errors.

The central unit

Composition

The central unit (fig. 3) has a unique code and is composed of a portable box with the following devices:

- Microcontroller - It controls every device and every event of the respective central unit.
- Lodging slot (fig. 3) (9) of the safety key - It is used to lodge the safety key.
- Blocking device (fig. 5) (A) of the safety key - It is used to block/unblock the safety key (31) and it is composed of a blocker (22) with a beveled tip, a spring (24), a spring support (23), an electromagnet (25), and a stop (26). When the safety key (31) is inserted into the lodging slot (fig. 3) (9), it remains blocked, because at the beginning the ramp (fig. 5) (28) starts to push the blocker (22) outwards, and then, due to the force of the spring (24), the blocker (22) is forced to be lodged in the notch (29). The electromagnet (25), when actuated, attracts the blocker (22) out of the notch (29), thus unblocking the safety key (31).
- Limit-switch (fig. 5) (27) - It is used to detect the presence of the safety key (31) inside the lodging slot (fig. 3) (9).
- Code reader of the safety key - Reads the code of the safety key. If the code is represented by a set of holes (fig. 5) (30)

in the body of the safety key (31), then the code reader must have an optical array in order to detect the existence or not of holes. If the code is provided by an RFID tag embedded in the safety key, the code reader must be a RFID transceiver.

- Linkers (fig 3) (12) - They are detachable electronic circuits that have a unique code. Each central unit has their own set of linkers. The code of the linker identifies itself and the central unit at which it belongs to. When a linker is transferred from one central unit to one remote unit, it is created a communication link (communication channel) between the two units (fig. 7). As each central unit has several linkers, one can transfer several linkers to several remote units (one linker for each remote unit). This way, communication channels are created between each central unit and every remote unit (figs. 8, 9 and 10). Every linker also has a non-volatile read/write memory. Therefore, in each linker can be written the following additional information: the code of the safety key; the code of the remote unit to where the linker will be transferred; the name and/or the geographical coordinates of the point of the electrical grid needing repairs. If this additional information is written directly into the linkers using a computer with appropriate software, there will be a minimization of the configuration errors.
- Linker connectors (fig. 3) (13) - These are the connectors where the linkers (12) are connected.
- Display (fig. 3) (8) - It is used to show relevant information to the operator of the central unit.
- Communication connector (fig. 3) (7) - This is the connector where the communication unit is connected.
- Unblocking button (fig. 3) (10) of the safety key - When this button is pressed, the electromagnet (fig. 5) (25) of the blocking device (A) of the safety key attracts the blocker (22) out of the notch (29), thus unblocking the safety key (31).
- Transmission button (fig. 3) (11) - When this button is pressed, the central unit transmits through the communication unit one or more messages with the code of the safety key to one or more remote units that have linkers from the referred central unit

(figs. 7, 8, 9 and 10). The sent message indicates that the safety key is blocked, and consequently indicates that the respective switch is in the off position and locked (fig. 2).

The remote unit

Composition

The remote unit (fig. 4) has a unique code and is composed of a portable box with the following devices:

- Microcontroller - It controls every device and every event of the respective remote unit.
- Working cards ((fig. 4) (17) and (fig. 6) (49)) - They are the cards that are distributed to workers. While a worker owns a working card, he has the assurance that the electrical power is disconnected. Each remote unit has a unique set of working cards. In each set, all working cards are equal. A working card (fig. 6) (49) is composed of: a handler (50); a blocking ramp (38); a notch (37); a positioning ramp (42); a dent (43); an indentation (40).
- Complementary indentation (fig. 6) (41) - This complementary indentation is the complement of the above-mentioned indentation (40).
- Lodging slots (fig. 4) (16) of the working cards - They are the slots where the working cards (17) are put in.
- Blocking device (fig. 6) (B) of the working cards - It blocks/unblocks the working cards (49) and it is composed of a blocking bar (32) with a beveled edge, a spring (34), a spring support (33), an electromagnet (35), and a stop (36). When a working card (49) is inserted into the lodging slot (fig. 4) (16), it remains blocked, because at the beginning the ramp (fig. 6) (38) starts to push the blocking bar (32) outwards, and then, due to the force of the spring (34), the blocking bar (32) is forced to be lodged in the notches (37) of all working cards already inserted. The electromagnet (35), when actuated, at-

tracts the blocking bar (32) out of the notches (37) of all working cards, thus unblocking them.

- Positional device (fig. 6) (C) of the working card - There is one positional device for each working card. Each positional device positions the respective working card in the right place inside the respective lodging slot (fig. 4) (16). It is composed of a positioner (fig. 6) (48) with a rounded tip, a spring (46), a spring support (47), a guide (44), and a stop (45). When a working card (49) is inserted into the lodging slot (fig. 4) (16), it remains in the right position, because at the beginning, the ramp (fig. 6) (42) starts to push the positioner (48) outwards, and then, due to the force of the spring (46), the positioner (48) is forced to be lodged in the dent (43). When someone pulls a working card after being unblocked by the blocking device (B), the positioner (48) is pushed outwards due to the dent (43) being rounded, releasing, in this way, the working card. The positional devices are needed to hold the already inserted working cards in the right position, because when a working card is inserted in the current remote unit or the electromagnet (35) is actuated, the working cards remain released for a few moments.
- Limit-switches (fig. 6) (39) - They are used to detect the presence of the working cards (fig. 4) (17) inside the lodging slots (16). There is one limit-switch for each working card. If the indentation (fig. 6) (40) of a working card does not fit in the complimentary indentation (41) of the remote unit, it is an indication that the working card is alien to the current remote unit. In this case, the respective limit-switch (39) is not actuated.
- Display (fig. 4) (15) - It is used to show relevant information to the operator of the remote unit.
- Linker connectors (fig. 4) (21) - These are the connectors where the linkers (20) are connected. When a linker is transferred from a central unit to a remote unit a communication link (communication channel) is created between them (fig. 7).
- Communication connector (fig. 4) (14) - This is the connector where the communication unit is connected.

- Unblocking button (fig. 4) (18) of the working cards - When this button is pressed, the electromagnet (fig. 6) (35) of the blocking device (B) attracts the blocking bar (32) out of the notches (37) of all working cards (49), thus unblocking all of them.
- Transmission button (fig. 4) (19) - When this button is pressed, the remote unit transmits through the communication unit a message with the code of the current remote unit to every central unit, from which there were linkers transferred (fig. 7, 8, 9, and 10). The sent message indicates that all working cards are blocked, and consequently indicates that all workers have finished the repairs on the electrical grid.

Global functioning of the Remote Safety System

Introduction

In order to repair a high-tension electrical grid, firstly it is needed to identify each switch that disconnects it, and each point of the electrical grid needing to be repaired. For each switch that disconnects the electrical grid is assigned one central unit. For each point of the electrical grid needing to be repaired is assigned one remote unit. Let m the number of central units ($m > 1$), and let n the number of remote units ($n > 1$), then the following configurations are arisen:

- One central unit and one remote unit - 1:1 configuration (fig. 7).
- One central unit and several remote units - 1:n configuration (fig. 8).
- Several central units and one remote unit - m:1 configuration (fig. 9).
- Several central units and several remote units - m:n configuration (fig. 10).

The 1:1 configuration

Usually a malfunction of an electrical grid occurs at only one point, and there is only one switch that disconnects it. So, in this particular case, the chief safety officer must assign one central unit to the switch to be off and one remote unit to the point of the electrical grid to be repaired. Then, to create a communication link (communication channel) between the two units, the chief safety officer must transfer one linker (fig. 3) (12) from the central unit to the remote unit (fig. 4) (20) (the central unit loses 1 linker; the remote unit gets 1 linker). In this way, the central unit knows which remote unit must communicate with, because the microcontroller of the current central unit knows the code of the missing linker. Otherwise, the remote unit knows which central unit must communicate with, because the microcontroller of the current remote unit knows the code of the linker that is connected to it. In the fig. 7 is depicted, in terms of communications, a 1:1 relation.

In order to repair a point of an electrical grid, the safety officer must turn off the respective switch, and lock it with the respective locking device (figs. 1 and 2). To do so, he must pull the lever of the switch from the on (fig. 1) (1) to the off position (fig. 2) (1), and must turn the safety key (6) in such a way that the switch remains locked. Then the safety officer takes the safety key (6) out of the lock (5) and inserts it into the lodging slot (fig. 3) (9) of the central unit, where it remains blocked due to the action of the blocking device (fig. 5) (A). Meanwhile, the safety key (31) actuates the limit-switch (27), which sends a signal to the microcontroller indicating that the safety key is present. Then, the microcontroller orders the code reader of the safety key to read the code. At this time, the code is displayed on the display (fig. 3) (8) in order to the safety officer verify if the code is the expected one. If the code of the safety key is the expected one, then the safety officer presses the transmission button (11). At this time, the transmission button sends a signal to the microcontroller, which in turn deactivates the unblocking button

(10) of the safety key. Even if someone presses the unblocking button, the safety key remains blocked. At the same time, the microcontroller sends a message with the code of the safety key to the remote unit through the communication unit. The code of the safety key sent to the remote unit indicates that the switch associated with the code is off and locked.

The remote unit (fig. 4), after being configured, has the unblocking button (18) of the working cards deactivated, and consequently the working cards (17) remain blocked. When the remote unit receives a message with the code of the safety key from the central unit, the microcontroller activates the unblocking button (18) of the working cards. Then, the repairing team manager verifies on the display (15) if the code of the safety key is the expected one. If so, he presses the unblocking button (18) of the working cards, which actuates the electromagnet (fig. 6) (35) that pulls the blocking bar (32), thus unblocking all working cards (49). While the unblocking button (fig. 4) (18) is pressed, each worker takes out one working card (17) from the respective remote unit. While a worker owns a working card, he has the assurance that the electrical power is disconnected.

After having done the due repairs on the electrical grid, each worker puts back his working card into a lodging slot (fig. 4) (16) of the respective remote unit. Each working card (fig. 6) (49) inserted into a lodging slot is immediately blocked due to the action of the blocking device (B). At the time in which each working card (49) is blocked, the respective limit-switch (39) is actuated. When all the working cards have already been inserted back into the current remote unit, the repairing team manager presses the transmission button (fig. 4) (19). Then the microcontroller verifies through the limit-switches (fig. 6) (39) if all the cards are present. If so, the microcontroller deactivates the unblocking button (fig. 4) (18) of the working cards. Even if someone presses the unblocking button, the working cards remain blocked. Then, the microcontroller sends through the communication unit a message to the central unit with the code of the current remote unit. This message

indicates that all working cards are blocked and consequently all the repairs have finished.

The central unit receives a message from the remote unit where a linker was transferred to. This message has the code of the referred remote unit and indicates that all the working cards are blocked, and consequently that all the workers have already finished the repairs on the electrical grid. Then, the microcontroller displays the code of the remote unit on the display (fig. 3) (8), and at the same time, activates the unblocking button (10) of the safety key. After that, the safety officer verifies if the code is the expected one, and if so, he presses the unblocking button (10) of the safety key, which actuates the electromagnet (fig. 5) (25) that pulls the blocker (22), thus unblocking the safety key (31).

Then the safety officer takes the safety key out of the lodging slot (fig. 3) (9) of the central unit, inserts it into the lock (fig. 2) (5), unlocks the switch, and then turn it on (fig. 1). While the switch remains on, the safety key (6) remains blocked inside the lock (5). This way, nobody can take out the safety key from the lock and misuse it.

The 1:n configuration

In some situations, several malfunctions of an electrical grid can occur at several points far from each other, and there is only a switch to disconnect the electric power. So, in this particular case, the chief safety officer must assign one central unit to the switch to be off and one remote unit to every point of the electrical grid to be repaired. Then, to create a communication link (communication channel) between the central unit and every remote unit, the chief safety officer must transfer one linker from the central unit to every remote unit (the central unit loses n linkers; each remote unit gets 1 linker). In this way, the central unit knows which remote units must communicate with, because the microcontroller of the current central unit knows the codes of the missing

linkers. Otherwise, every remote unit knows which central unit must communicate with, because the microcontroller of the current remote unit knows the code of the linker that is connected to it. In the fig. 8 is depicted, in terms of communications, a 1:2 relation.

In the functioning of the 1:n configuration, the following sequence of events occurs:

- 1) The switch that disconnects the electrical power is turned off and locked;
- 2) The safety key is taken out from the respective lock and inserted into the respective central unit, where it is blocked;
- 3) From the central unit, a message with the code of the respective safety key is sent to every remote unit;
- 4) Each remote unit, after receiving a message with the code of safety key from the central unit, unblocks the working cards;
- 5) In each remote unit, each worker picks one working card, and after all repairs have finished, all working cards are returned, and blocked afterwards;
- 6) In each remote unit, after the working cards having been blocked, it is sent a message with the code of the current remote unit to the central unit;
- 7) The central unit, after receiving a message with the code of every remote unit, unblocks the respective safety key;
- 8) The safety key is taken out from the respective central unit and used to unlock the respective switch;
- 9) The switch is turned on, and consequently the electrical power is connected.

The m:1 configuration

In an electrical ring grid (ring network) several switches are needed to be turned off in order to disconnect the electrical power. In the current configuration, it is considered that only one point of the electrical grid has a malfunction. So, the chief safety officer must assign one central unit to every switch to be off and one remote unit to the point of the electrical grid to be

repaired. Then, to create a communication link (communication channel) between every central unit and the remote unit, the chief safety officer must transfer one linker from each central unit to the remote unit (each central unit loses 1 linker; the remote unit gets m linkers). In this way, each central unit knows which remote units must communicate with, because the microcontroller of the current central unit knows the code of the missing linker. Otherwise, the remote unit knows which central units must communicate with, because the microcontroller of the current remote unit knows the codes of the linkers that are connected to it. In the fig. 9 is depicted, in terms of communications, a 2:1 relation.

In the functioning of the $m:1$ configuration, the following sequence of events occurs:

- 1) Each switch that disconnects the electrical power is turned off and locked.
- 2) Each safety key is taken out from the respective lock and inserted into the respective central unit, where it is blocked;
- 3) From each central unit, a message with the code of the respective safety key is sent to the remote unit;
- 4) The remote unit, after receiving a message with the code of safety key from every central unit, unblocks the working cards;
- 5) In the remote unit, each worker picks one working card, and after all repairs have finished, all working cards are returned, and blocked afterwards;
- 6) In the remote unit, after the cards have been blocked, it is sent a message with the code of the current remote unit to every central unit;
- 7) In each central unit, after receiving a message with the code of the remote unit, the respective safety key is unblocked;
- 8) Each safety key is taken out from the respective central unit and used to unlock the respective switch;
- 9) Each switch is turned on, and consequently the electrical power is connected.

The m:n configuration

In an electrical ring grid (ring network) several switches are needed to be turned off in order to disconnect the electrical power. In the current configuration, it is considered that several points of the electrical grid have malfunctions. So, the chief safety officer must assign one central unit to every switch to be off and one remote unit to every point of the electrical grid to be repaired. Then, to create a communication link (communication channel) between each central unit and every remote unit, the chief safety officer must transfer one linker from each central unit to every remote unit (each central unit loses n linkers; each remote unit gets m linkers). In this way, each central unit knows which remote units must communicate with, because the microcontroller of the current central unit knows the codes of the missing linkers. Otherwise, each remote unit knows which central units must communicate with, because the microcontroller of the current remote unit knows the codes of the linkers that are connected to it. In the fig. 10 is depicted, in terms of communications, a 2:3 relation.

In the functioning of the m:n configuration, the following sequence of events occurs:

- 1) Each switch that disconnects the electrical power is turned off and locked.
- 2) Each safety key is taken out from the respective lock and inserted into the respective central unit, where it is blocked;
- 3) From each central unit, a message with the code of the respective safety key is sent to every remote unit;
- 4) Each remote unit, after receiving from every central unit a message with the code of safety key, unblocks the working cards;
- 5) In each remote unit, each worker picks one working card, and after all repairs have finished, all working cards are returned, and blocked afterwards;
- 6) In each remote unit, after the cards have been blocked, it is sent a message with the code of the current remote unit to every central unit;

- 7) In each central unit, after receiving a message with the code of every remote unit, the respective safety key is unblocked;
- 8) Each safety key is taken out from the respective central unit and used to unlock the respective switch;
- 9) Each switch is turned on, and consequently the electrical power is connected.

**The use of the memory of the linkers in order to minimize
configuration errors**

To minimize configuration errors, the memory of the linkers must be loaded by a computer with the following information:

- The code of the safety key that will be received by a pre-designated remote unit;
- The code of the above-mentioned remote unit to where the linker will be transferred;
- The name and/or the geographical coordinates of the point of the electrical grid needing repairs.

With this kind of information, each remote unit compares its own code with the code contained in each linker. It also compares the code of the safety key received from each central unit with the code contained in every linker. If there is some code not corresponding with the codes contained in the linkers, the working cards are not unblocked and an error message is displayed on the display.

The computer that is used to load the information into the memory of the linkers must have software capable of representing graphically the topology of the high-tension electrical grid in a dynamic mode. So, when the chief safety officer, using the mouse, clicks on a point of the electrical grid needing repairs, the computer loads automatically the information into the memory of the linkers.

CLAIMS

1. The Remote Safety System ensures in a remote way that in an high-tension electrical grid, and similarly in a industrial compound, there is the certainty of whom is going to do repairs in the referred grid that one or more switches that disconnect it are turned off beforehand, and otherwise ensures to whom is going to turn them on, that the workers have finished the repairs beforehand, **characterized in that** is composed of one locking device attached to every switch, one central unit assigned to every switch used to connect/disconnect the power of the electrical grid, one remote unit assigned to every point of the electrical grid needing repairs, and one communication unit assign to every central unit and remote unit.
2. The Remote Safety System according to claim 1, **characterized in that** the locking device is composed of a curved bar (2) with a window (3), which curved bar is bonded to the lever (1) of the switch, a lock (5) with a rotating bolt (4), and a safety key (6) that drives the referred lock, which locking device functions in the following way: in order to turn off and lock the switch, the lever (1) of the switch is pulled from the on to the off position, the safety key (6) that is inserted into the lock (5) is turned to the locked position, and consequently the bolt (4) rotates into the window (3), locking this way the lever (1) of the switch; in order to turn the switch on, the safety key (6) is turned to the unlocked position, and consequently the bolt (4) rotates out of the window (3), unlocking this way the lever (1) of the switch, making possible the lever (1) of the switch be pushed into the on position.
3. The Remote Safety System according to claim 1, **characterized in that** the central unit has a unique code and is composed of a portable box with the following devices: a microcontroller that controls every device and every event; a lodging slot (9) of the safety key; a blocking device (A) of the safety key; a limit-switch (27) that detects the presence of the safety key

(31); a code reader of the safety key; linker connectors (13); linkers (12) that are as much as the respective connectors (13); a display (8); a communication connector (7) that connects the communication unit; an unblocking button (10) of the safety key; a transmission button (11).

4. The Remote Safety System according to claim 1, **characterized in that** the remote unit has a unique code and is composed of a portable box with the following devices: a microcontroller that controls every device and every event; lodging slots (16) of the working cards; working cards (17) (49); positional devices (C) of the working cards; a blocking device (B) of the working cards; a complementary indentation (41); limit-switches (39) that detect the presence of the working cards (17) (49); a display (15); linker connectors (21); a communication connector (14) that connects the communication unit; an unblocking button (18) of the working cards; a transmission button (19).
5. The Remote Safety System according to claim 1, **characterized in that** the communication units are modems, or mobile phones, or transceivers, using them a communication protocol capable of recovering transmission errors, allowing them the communication between each central unit and every remote unit, and being connected to the communication connectors (7) (14).
6. The Remote Safety System according to claims 1 and 2, **characterized in that** the safety key (6) (31) has the following characteristics: it can only be taken out from the lock (5) when the lever (1) of the switch is in the off position and the lock is in the locked position; it remains blocked inside the lock (5) when the lever (1) of the switch is in the on position and the lock is in the unlocked position; when the lever (1) of the switch is in the on position and the lock (5) is in the unlocked position, it is impossible to rotate it to the locked position, because the solid part of the curved bar (2) prevents the bolt (4) from rotating; it must have a unique code that identifies uniquely the switch at which it belongs, which code

is represented by a set of holes (30) in its body, or it must has a Radio-Frequency Identification (RFID) tag embedded in it; it has a ramp (28); it has a notch (29).

7. The Remote Safety System according to claims 1, 3 and 6, **characterized in that** the blocking device (A) of the safety key is composed of a blocker (22) with a beveled tip, a spring (24), a spring support (23), an electromagnet (25), and a stop (26), which blocking device functions in the following way: when the safety key (31) is inserted into the lodging slot (9) of the central unit remains blocked, because at the beginning, the ramp (28) starts to push the blocker (22) outwards, and then, due to the force of the spring (24), the blocker (22) is forced to be lodged in the notch (29); when the operator of the central unit wants to unblock the safety key (31), he presses the unblocking button (10) of the safety key, which in turn actuates the electromagnet (25), attracting in this way the blocker (22) out of the notch (29), thus unblocking the safety key.
8. The Remote Safety System according to claims 1, 3 and 6, **characterized in that** the code reader of the safety key is composed of one of the following options: if the code is represented by a set of holes (30) in the body of the safety key (31), then the code reader must have an optical array in order to detect the existence or not of holes; if the code is provided by an Radio-Frequency Identification (RFID) tag embedded in the safety key, the code reader must be a RFID transceiver.
9. The Remote Safety System according to claims 1 and 4, **characterized in that** the working card (49) is composed of a handler (50), a blocking ramp (38), a notch (37), a positioning ramp (42), a dent (43) and an indentation (40), which indentation has the following functionalities: if the indentation (40) dovetails with the complementary indentation (41), the limit-switch (39) is actuated, indicating in this way to the micro-controller that the referred working card is present; if the indentation (40) does not dovetail with the complementary in-

dentation (41), the limit-switch (39) is not actuated, indicating in this way to the microcontroller that the referred working card is not present.

10. The Remote Safety System according to claims 1, 4 and 9, **characterized in that** the blocking device (B) of the working cards is composed of a blocking bar (32) with a beveled tip, a spring (34), a spring support (33), an electromagnet (35), and a stop (36), which blocking device functions in the following way: when a working card (17) (49) is inserted into a lodging slot (16) of the remote unit remains blocked, because at the beginning, the ramp (38) starts to push the blocking bar (32) outwards, and then, due to the force of the spring (34), the blocking bar (32) is forced to be lodged in the notches (37) of all working cards; when the operator of the current remote unit wants to unblock all working cards (17) (49), he presses the unblocking button (18), which in turn actuates the electromagnet (35), attracting in this way the blocking bar (32) out of the notch (29).
11. The Remote Safety System according to claims 1, 4 and 9, **characterized in that** the positional device (C) of the working card is used to hold a working card (17) (49) in the right position inside a lodging slot (16) of a remote unit when the cards are unblocked, and it is composed of a positioner (48) with a rounded tip, a spring support (47), a spring (46), a guide (44), and a stop (45), which positional device functions in the following way: when a working card (49) is inserted into the lodging slot (16) remains in the right position, because at the beginning, the ramp (42) starts to push the positioner (48) outwards, and then, due to the force of the spring (46), the positioner (48) is forced to be lodged in the dent (43); when someone pulls a working card after being unblocked by the blocking device (B), the positioner (48) is pushed outwards due to the dent (43) being rounded, thus releasing the working card.

12. The Remote Safety System according to claims 1, 3 and 4, **characterized in that** the linker is constituted by a detachable electronic circuit that contains: a unique code that identifies itself and the central unit at which it belongs to, and when it is transferred from a central unit to a remote unit creates a communication link between these two units; a non-volatile read/write memory capable of being loaded by a computer with additional information that minimizes configuration errors, which information is the code of the safety key that will be blocked in the central unit, the code of the remote unit to where the linker will be transferred to, and the name and/or geographical coordinates of the point of the electrical grid needing repairs.
13. The Remote Safety System according to claims 1, 2, 3, 4, 5, 6, 7, 8, and 12, **characterized in that** the central unit, at the phase that there is the intention of turning the switch off and blocking the safety key (31), functions accordingly the following sequence of events: after the switch has been turned off and locked, the safety key (6) is taken out from the lock (5) and inserted into the lodging slot (9) of the current central unit, where it is immediately blocked by the blocking device (A); the safety key (31) actuates the limit-switch (27), which sends a signal to the microcontroller indicating that the safety key is present; the microcontroller orders the code reader of the safety key to read the code; the code is displayed on the display (8) in order to the safety officer verify if the code is the expected one; if the code of the safety key is the expected one, then the safety officer presses the transmission button (11); the transmission button sends a signal to the microcontroller, which in turn deactivates the unblocking button (10) of the safety key; the microcontroller verifies what the codes of the absent linkers are, and sends a message with the code of the safety key (31) to every remote unit through the communication unit.

14. The Remote Safety System according to claims 1, 3, 4, 5, 9, 10, 11, 12 and 13, **characterized in that** the remote unit functions accordingly the following sequence of events: when the current remote unit receives from every central unit a message with the code of the respective safety key, the microcontroller activates the unblocking button (18) of the working cards; the operator verifies on the display (15) if the code of the safety key is the expected one, and if so, he presses the unblocking button (18) of the working cards, which actuates the electromagnet (35) that pulls the blocking bar (32), thus unblocking all the working cards (49); while the unblocking button (18) is pressed, each worker takes out one working card (17) from the current remote unit, and executes the repairs on the electrical grid; after having done the due repairs on the electrical grid, each worker puts back his working card (17) into a lodging slot (16) of the respective remote unit; each working card (49) inserted into a lodging slot (16) is immediately blocked due to the action of the blocking device (B); at the time in which each working card (49) is blocked, the respective limit-switch (39) is actuated; when all the working cards have already been inserted back into the current remote unit, the operator presses the transmission button (19); the microcontroller verifies through the limit-switches (39) if all the working cards are present, and if so, the microcontroller deactivates the unblocking button (18) of the working cards; the microcontroller reads the codes of the connected linkers, and sends a message with the code of the current remote unit to every central unit through the communication unit.
15. The Remote Safety System according to claims 1, 2, 3, 4, 5, 6, 7, 8, 12, 13 and 14, **characterized in that** the central unit, at the phase that there is the intention of unblocking the safety key (31) and turning the switch on, functions accordingly the following sequence of events: when the current central unit receives from every remote unit a message with the code of the respective remote unit, the microcontroller displays the code of the remote unit on the display (8), and at the same time ac-

tivates the unblocking button (10) of the safety key; the operator verifies on the display if the code is the expected one, and if so, he presses the unblocking button (10) of the safety key, which actuates the electromagnet (25) that pulls the blocker (22), thus unblocking the safety key (31); the operator takes the safety key out of the lodging slot (9) of the current central unit, insert it into the lock (5), unlocks the switch and turns it on, and consequently the electrical power is connected.

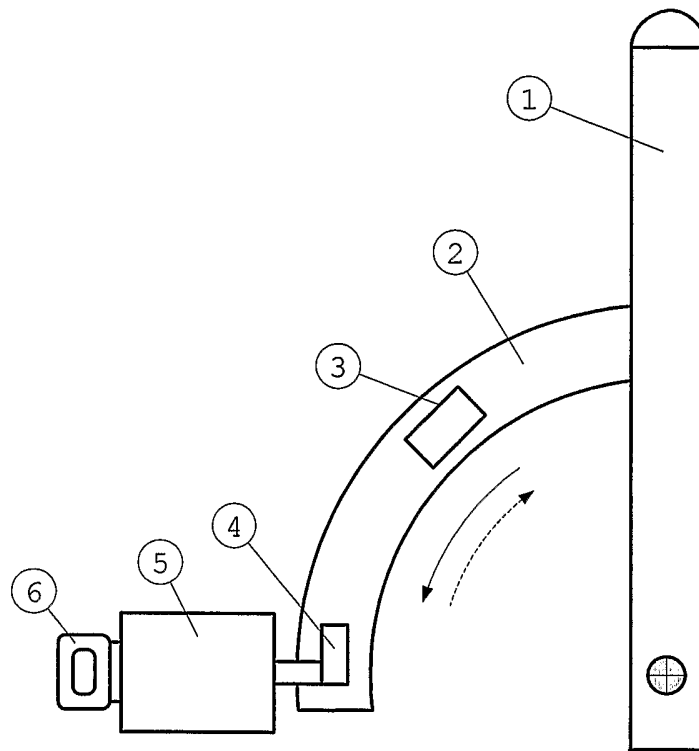


Fig. 1

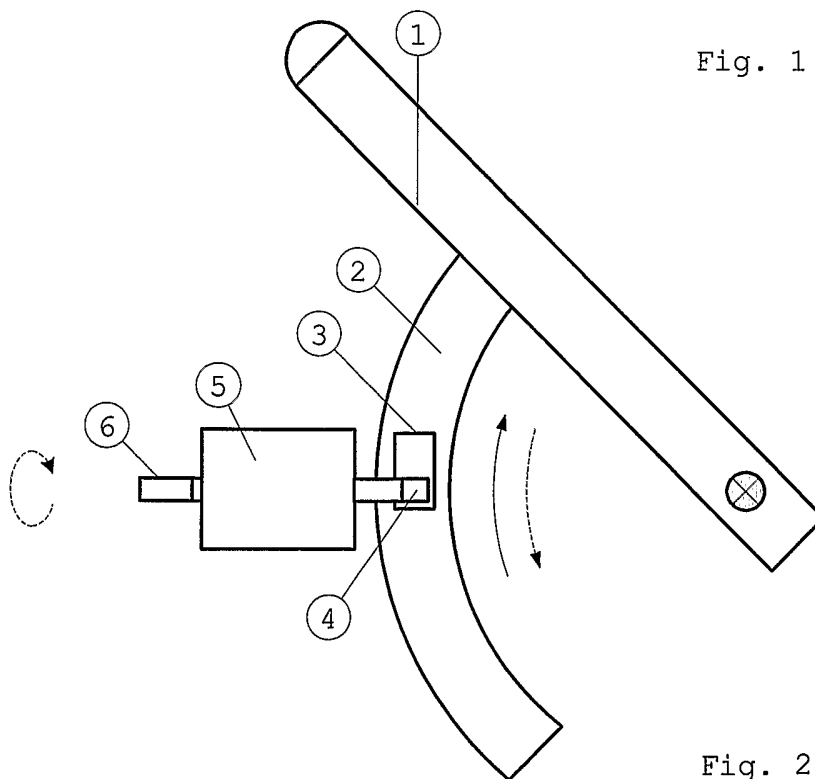


Fig. 2

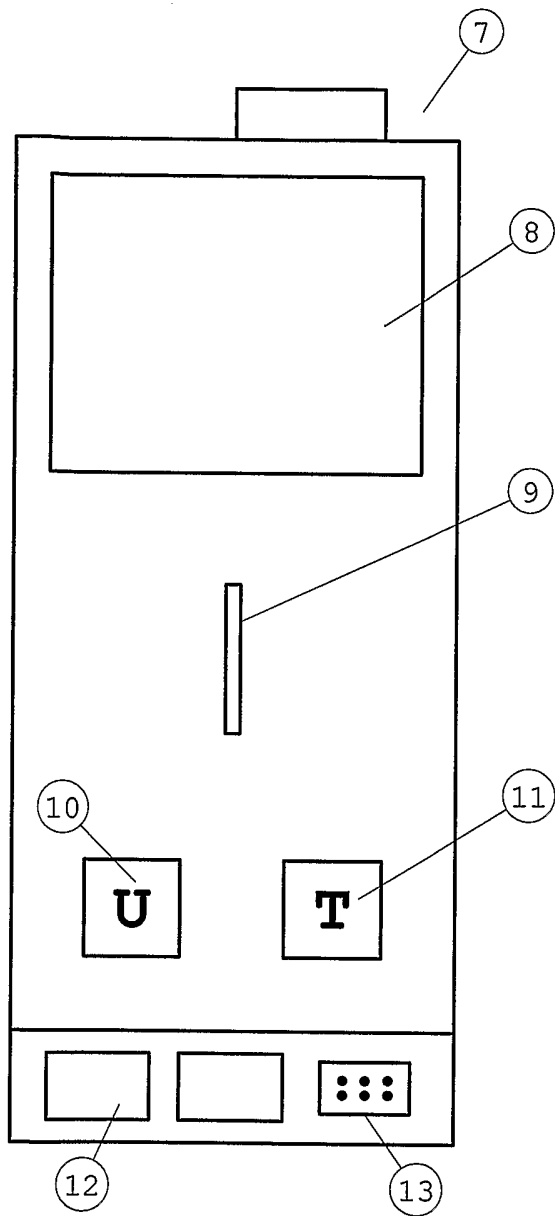


Fig. 3

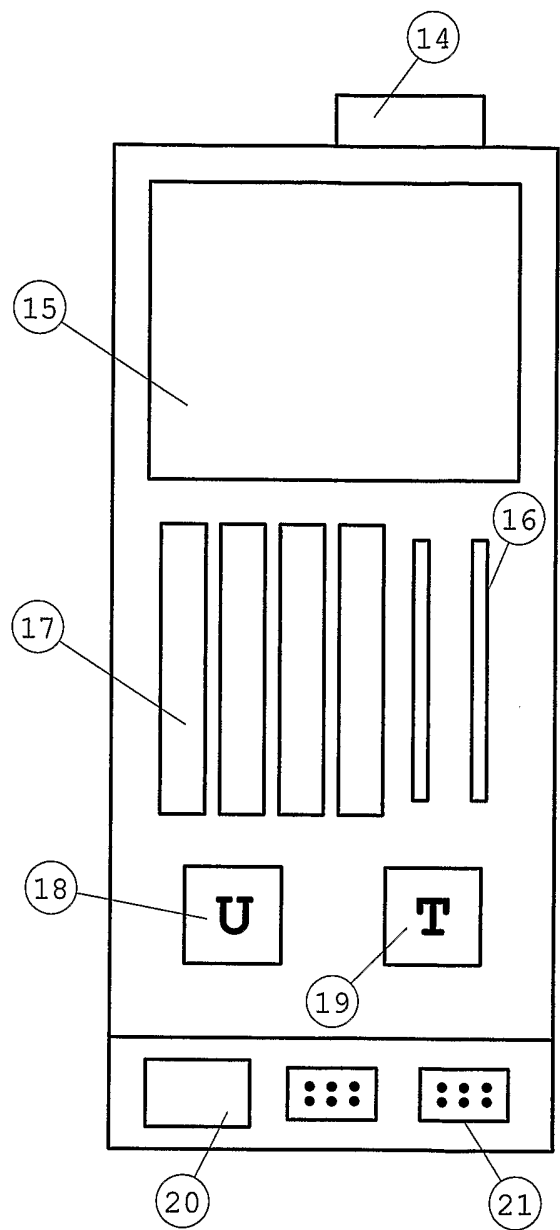


Fig. 4

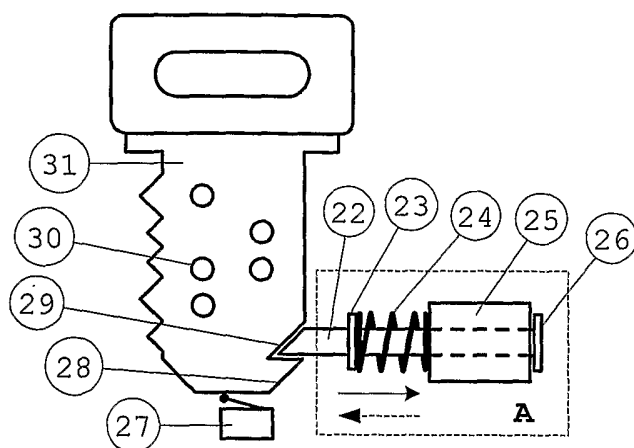


Fig. 5

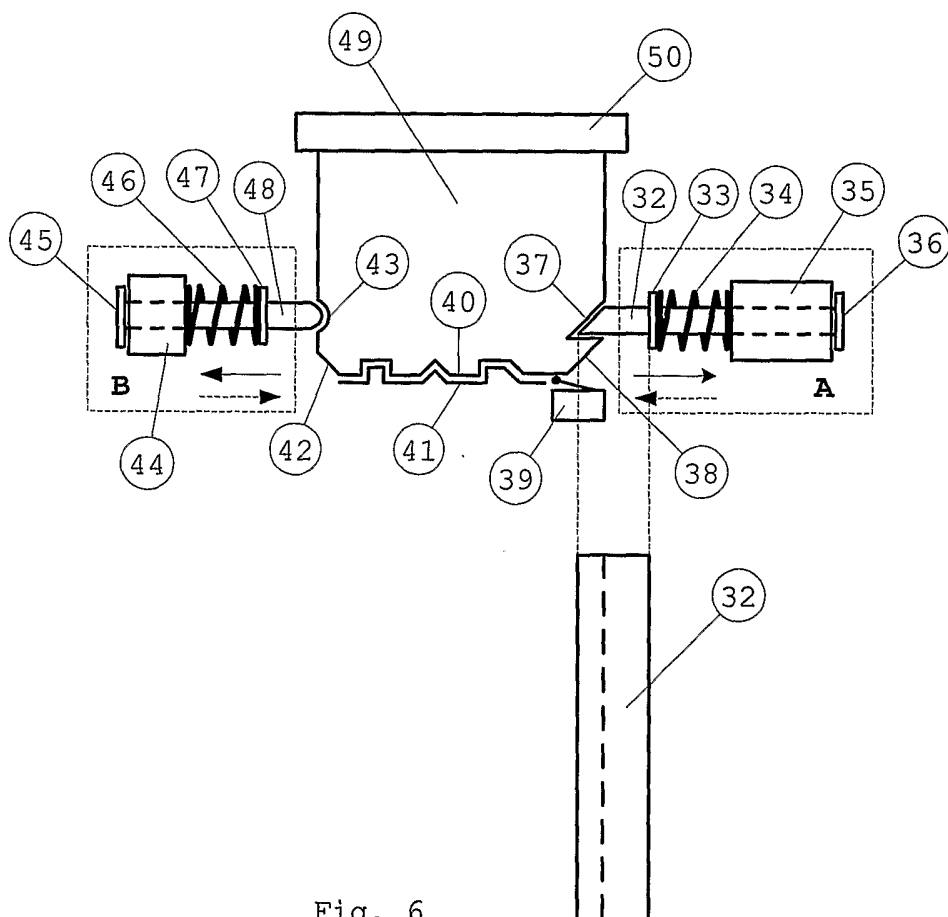


Fig. 6



Fig. 7

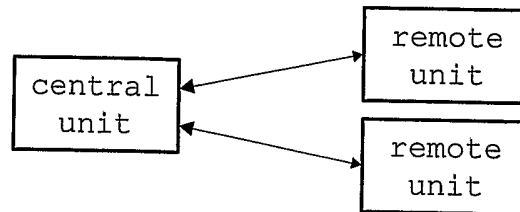


Fig. 8

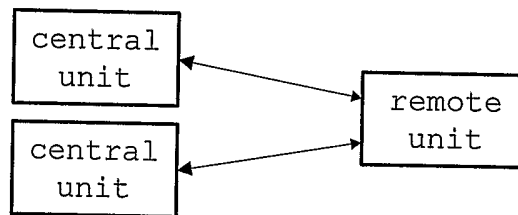


Fig. 9

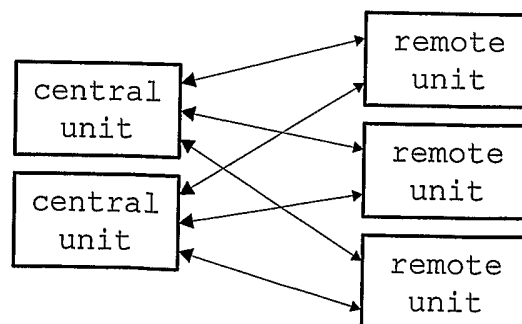


Fig. 10