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

(11) Publication number : **0 494 715 A1**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : **92200021.1**

(22) Date of filing : **07.01.92**

(51) Int. Cl.[5] : **G08B 13/14,** G08B 29/18

(30) Priority : **11.01.91 NL 9100035**

(43) Date of publication of application :
15.07.92 Bulletin 92/29

(84) Designated Contracting States :
DE FR GB NL

(71) Applicant : **Smit, Jacob**
Andoorn 65
NL-7577 AX Oldenzaal (NL)

(72) Inventor : **Smit, Jacob**
Andoorn 65
NL-7577 AX Oldenzaal (NL)

(54) A theft protection system.

(57) The invention concerns a theft protection system with special facilities to suppress electrical noise very well. The preferred embodiment of the system provides a very high integrity. Compatible with the provisions to suppress noise and to increase the integrity is a feature which signals missing merchandise even when functional modules have been disconnected from the controlling system. Several modulation/demodulation techniques are given to make the system immune to external conditions and to increase its functionality.

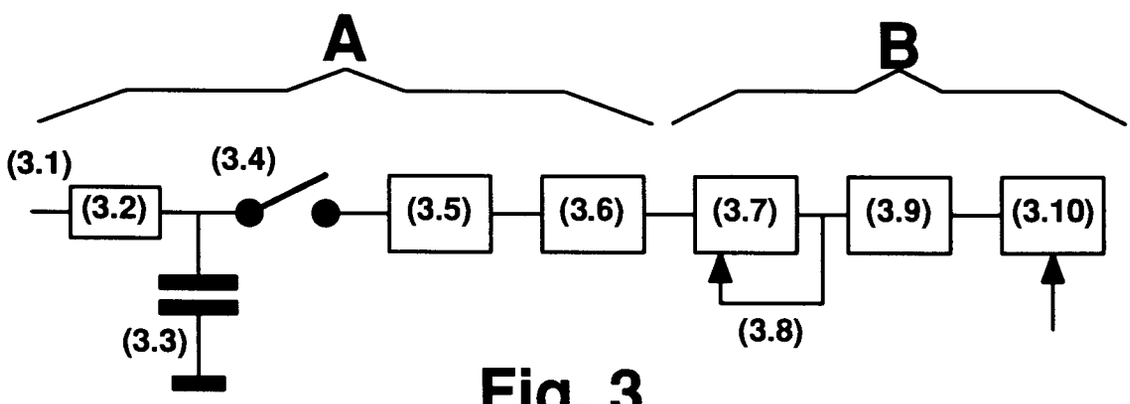

Fig. 3

EP 0 494 715 A1

Application area

The subject of the invention is a theft protection system for merchandise, in accordance with claim 1 and a protection cable, to be used in conjunction with said apparatus, in accordance with claim 2.

Background Art

A theft protection system for merchandise, based on the use of resistance networks, operational amplifiers and several RC networks, used to observe the current in an external sensor, has been described in EP 0 116 701. Special resistor combinations are used to to decode events on the input of the system. The analog nature of this system makes it extremely sensitive for environmental noise, c.q. interference. The sensors used in conjunction with this systems are all based on the presence of a switch of any kind, which is either part of the cable or built into the sensor. Such protection cables are hard to manufacture and hence more expensive than cables without switches. This known theft protection system can enter the false alarm state with relative ease due to environmental noise (of considerable magnitude). Such noise, c.q. interference is however induced by the inherent capacitive crosstalk associated with the cable system proposed in this patent. It is not known whether the circuits in said patent can be extended by suitable RC-circuits, such that ease with which the false alarm state is entered, can be greatly reduced, while preserving the functionality. It should be noted however, that the economic value of such changes is minimal in the light of the current invention.

Three other aspects, of importance for the art, are not covered by the patent EP 0 116 701: 1 The removal of merchandise cannot be signaled in the alarm state. This fact can be traced back to the general construction of the system, 2. Changes in the configuration of the theft protection system can only be made when the system is out of order, 3 The system in EP 0 116 701 is not able to determine the total amount of articles protected.

Another known theft protection system, described in EP 0 052 193, gives the desired protection through the presence of an electrical power supply cable, extending from the apparatus, which has one end integrally attached to the apparatus, which cable in use is anchored to an immovable object, such that the removal of the apparatus cannot occur without damaging the cable. It will be clear from the description of the theft protection system, that the operating conditions for EP 0 052 193, are not applicable for a theft protection system for merchandise.

It will be argued that it is necessary to be able to connect end disconnect existing products (merchandise) in an easy and convenient way, without making scratches, leaving glue residues or causing paint damage. The current invention uses existing connectors, already available on the products to be sold, to simplify in- and out-mutations of merchandise to the utmost extreme. Moreover, the cable construction prevents that the signal transport function of the cables gets lost. The problem of crosstalk in the cables is overcome by the application of digital filters.

Description

Applications of protection systems demand an extremely simple and straightforward method to protect the merchandise. This invention describes an embodiment, based on the usage of cables, attached to existing connectors on the equipment to be protected, like a radio, a compact disk player or a television set. An integral part of the system is an electronic subsystem which (strongly) rejects environmental noise and interference. Another integral part of the system is a subsystem which makes it possible to install the theft protection system, free of interference and noise, without the use of measuring equipment. False alarms cannot be tolerated in a theft protection system. This aspect is frequently avoided by the stringent application of well known installation techniques, like proper grounding, avoidance of ground-loops and adequate shielding. The current invention concerns a design of extreme insensitivity to external noise (interference), crosstalk and/or electromagnetic interference. This property is necessary to detect, with protection cables as shown in figure 1, without error, the presence or absence of merchandise. The application of the proposed protection cables is considered of utmost importance, as they are easily connected and disconnected to or from the Chinch chassis part on the merchandise, using the Chinh connectors (1.I) and (1.II) to protect articles like Radio's, Compact Disk Players and the like. Television sets, video recorders and the like are protected in a similar way using Scart cables. Said cables have as advantage over cables with switches glued onto the surface of the merchandise to be protected, that no residues of the adhesive material are left, nor that paint can be damaged, while offering full protection for all kinds of theft attempts, on the shelf.

Description of the drawings

Figure 1 shows a preferred embodiment of a theft protection cable for connection to an audio installation, consisting of Chinch connectors (1.I, 1.II) and a connection to the theft prevention apparatus (1.III), comprising electrical conductors (1.1), (1.2), (1.3) and (1.4).

Figure 2 shows a preferred embodiment of a theft protection system, consisting of three cables and a multitude of control units.

Figure 3 shows a preferred embodiment of the

signal processing part for a single input, to be connected with a protection cable. The division of the hardware in parts A and B is of essential importance for the construction of an optimally functioning modular system, as indicated in figure 4.

Figure 4 shows a preferred embodiment of a theft protection system, which can protect large amounts of merchandise, by connecting multiple modules to the communication cable (4.S) which in turn is connected to a controller (4.C).

Detailed description

The cable of figure 1 is normally connected to one of the channels of an audio installation. A second audio cable of standard construction is used to make a connection through the other channel. An electrical loop is closed by connecting the wires (1.2) and (1.5). The presence of said loop is detected by the protection system using an adequate input circuit. Attempts to tamper the protection provided by the cable, by bridging the circuit, through intrusion of nails or crocodile clamps, are easily detected with a suitable input circuit, which is connected to cable by means of the connector (1.III). Note that it is impossible to penetrate the cable shielding with a pin or another sharp conducting object, without making electrical contact with the shield. Such attempts to tamper the cable with pins and/or crocodile clamps are observed by the input circuit of the protection system, as the cable shield (1.1) or (1.4) will come into contact with one of the inner wires (1.2), (1.3) or (1.5). The signal wire of the audio system is simply passed through the cable, so the usual audio signals stay available on the connector to provide a live connection. The same principle is applied for the protection of live video installations, which are protected with a pair of Scart connectors. A loop within the TV set is used in this case to detect the presence of the merchandise.

A disadvantage of such cables is the crosstalk between the signal wire (1.3) and the wiring (1.1, 1.2, 1.4, 1.5) of the theft protection system.

A simple theft protection system, based on the usage of the cables described herein, is shown in figure 2. Merchandise (2.MI, 2.MII, ...) is connected to the protection cables using contact sensors and/or Chinch and/or Scart connectors and/or sensors of another type, utilizing an eventual male or female connector on the merchandise. In most cases, the female connector is already present on the merchandise on sale, so male connectors would be part of the protection cables (2.CI, 2.CII, ...). Said protection cables are connected, using another appropriate connector (2.AI, 2.AII, ...), to the controller, further comprising a loudspeaker (2.LS), a keyboard (2.KB) or similar (electromechanical) lock, a display unit (2.DIS).

The system described, will not work without false alarm, if constructed with conventional techniques, as crosstalk between the wires (1.2, 1.3) and (1.3, 1.5) may be substantial. This makes it necessary to use large capacitance and resistance values to reduce the bandwidth of the signals on the connectors (2.AI, 2.AII, ...) to a few Hertz to circumvent the problem indicated. It will be necessary to select an impedance level in the order of one Mega Ohm and capacitances in the order of 2 micro Farad to realize the low cutoff frequency required to make the inputs insensitive to noise. The high impedance level however makes the circuit again sensitive for external interference. The need for capacitors (or inductors) with large values and the related high volume makes such solutions particularly unattractive.

Figure 3 shows an improved block-diagram of a preferred embodiment of the theft protection system. Note that there are various alternatives for the realization of this block-diagram, which are all considered to be equivalent for the purpose of this patent. These alternatives can be derived by application of the laws of Thévenin and/or Norton and/or the application of commutativity/associativity laws on the blocks (3.4, 3.5, 3.6). The input signal (3.1) is passed through a micro-miniature lowpass filter (3.2, 3.3), which may be constructed from an SMD resistor and an SMD capacitor of minimal dimensions. Next to this filter comes a sampler (3.4), a quantizer (3.5) and a hold circuit (3.6). The digital filter (3.7) with feedback circuits (3.8), reduces the bandwidth of the input signal (3.1) to frequencies in the order of 0.4 Hertz. The threshold circuit (3.9) generates a logical signal with value 0 or 1, to represent the presence or absence of an object which should be protected. This value is continuously compared to a reference state (3.10), which can be changed using the signal (3.11) by the control unit, to be able to detect changes in the external configuration, by observing the output signal (3.12).

Large protection circuits quickly give rise to unwieldy wiring problems, which are particularly problematic in shop applications. This situation is improved by a refinement of the setup in figure 2, as shown in figure 4. This figure shows modules (4.I, 4.II, ...), each with input circuits, (4.0, ... 4.7), connected with a serial communication network (4.S) and a controller (4.C).

Said controller generates the signals which control the detection circuit for merchandise, as indicated in figure 3. It is a simple matter to transfer the signals (3.11) and (3.12) over this serial channel (4.S) from and to the controller (4.C). The described embodiment has however serious drawbacks, as status changes, concerning missing merchandise cannot be send to the controller (4.C) when the serial channel (4.S) gets disconnected, for instance due to a tamper attempt, followed by theft.

A refinement of the invention concerns an embodiment in which the parts (3.1, 3.2, 3.3, 3.4, 3.5, 3.6),

indicated as part A in figure 3, are implemented in the modules (4.I, 4.II, ...), and the parts (3.7, 3.8, 3.9, 3.10, 3.11, 3.12), indicated as part B in figure 3 are implemented in the controller (4.C).

The controller can detect the apparent absence of merchandise even when the serial channel has been tampered, for instance bij disconnecting it, or making it inoperable in any other way.

An important consequence of this fact is that the serial connection need not be secured, through the use of screwed connectors or any other fastening system. A simple connector, which may even be accessible to the potential thief, suffices for the accurate and secure operation of the complete system.

A refinement of the invention, comprises a feature which is used to detect the presence of a module (4.I, 4.II, ...). It is not relevant for this feature whether the equipment/merchandise to be protected is connected to any of the input ports (3.1) or not. It will be clear that said refinement is very important during installation of a system with many modules, as this gives rise to a simple method in which the network may be split in order to locate/isolate parts during installation which cause an unwanted alarm state.

This refinement of the invention is based on an extra signal FEED, which is applied to the serial input of all modules (4.I, 4.II, ...), either as an analog or a digital signal, using a high ohmic resistor. This signal is superseded by the outputsignal of the previous module, i.e. the FEED signal of module (4.I), although present, is superseded by the output of module (4.II) etc. Hence there is only one module which receives the FEED signal as input signal, namely the last one on the serial communication line (4.S).

Besides detection on the presence of a module, the hardware described, also monitors the proper operation of the modules (4.I, 4.II, ...), as the sequence present in the FEED signal, sent bij the controller (4.C) comes back to the controller after a delay depending on the number of modules connected. Given a fixed maximum for the number of modules connected, there is however still uncertainty about the number of modules connected, as it may happen that a bit-combination, representing (dis) connected sensor inputs (3.1), has direct correspondence with the sequence of the FEED signal.

This gives, without precautions, raise to ambiguities. This patent claims two possible provisions to overcome this problem. These provisions may be used in conjunction, or separate.

1) Some of the input ports can be used to feed into the system a certain signal, instead of being used as a normal input. The signal may be static, but it may represent a time sequence as well. For instance a 1 bit code applied to the module, which is permanently 1, may be used in conjunction with the FEED signal which is always zero at the corresponding bit-location to detect the presence of the module, by distinguishing a '1' bit received, due to presence of a module, from a '0' bit received due to absence of a module. Note that such an embodiment gives raise to a reduced capacity of the system. An alternate embodiment of this concept uses a bit which rotates over a restricted number of bits, like the bit used to scan the rows or columns of a keyboard. Said detection circuit can now be used to detect the position of an extra keyboard, characterized by a rotating bit sequence in the serial line (4.S). An amount of 3 to 4 subsequent sequences may be used to decode a 3x4 keyboard. It will be clear that extra keyboards may be inserted on the serial line (4.S) at arbitrary positions between modules.

2) A second method, which gives opportunities to detect the presence of modules, without sacrificing input port positions is based on a modulation technique, which changes the FEED signal sequence in subsequent shift cycles, in such a way that the sequence of the feed signal can be uniquely distinguished from the sequence generated on the sequential line (4.S) by an arbitrary sensor signal combination. The relatively low maximum speed with which the sensor signal may change, is caused for one part by the RC filter (3.2, 3.3) and for the other part by the impossibility to perform inand out-mutations of merchandise at high speed. This makes it possible to construct a detector which separates the FEED signal sequence from the sensor signal, by using one modulation/demodulation technique, to be selected from a multitude of possibilities.

Another refinement of the patent concerns a provision to suppress errors in the sensor signals, caused by errors on the serial line. A control circuit recognizes the position of the modules (4.I, 4.II, ...). Each unused module position, is checked on the presence of a correct, delayed copy of the FEED signal. One time slot is be allocated such that at least one delayed copy of the FEED signal, which may or may not be correct, is present. There is a high probability that (almost all) sensor signals read will be mis-interpreted in a sample period which corresponds to the transmission of a disturbed FEED signal. A decision circuit, incorporated in the protection system, plays an important role to filter unreliable sensor data out, in case the FEED signal is found to be disturbed, such that such erroneous signals do not enter the digital filter (3.7).

Any change to the expected value of the FEED signal is an indication that the system is improperly functioning. An error-status signal is used to monitor this fact, which is subject to digital filtering with threshold logic as well, in this case to monitor the proper operation of the serial channel (4.S).

The monitor function built into the controller (4.C) can recognize the following situations, based on the

embodiment just described:

1. Changes in data signals, based on digitally filtered observations, with an extremely low false alarm chance (This is the primary function of the theft protection system).
2. Detection of noise/crosstalk on (to) the serial line (4.S) by inspection of the delayed sequence signal of a FEED signal.
3. Detection of the removal or the addition of a module.
4. Verification of the correct operation of the shift register(s) in each (all) module(s).

Description of the main application:

The embodiment described makes it possible to generate tone sequences, as well as indicator signals on a (LED) display, such that the proper operation of the theft protection system can be monitored without the use of any measurement equipment. It is attractive to make all connections to the modules with connectors. Using normal installation procedures, one connects one module after the other while the controller (4.C) is active. A tone sequence generated by the controller (4.C) is used to signal in- and out-mutations of individual modules (4.I, 4.II, ..) and so on. Similar tone sequences are used as well to signal in- and out-mutations on the ports (4.0, ... 4.7) of the modules. The out-mutations trip the alarm, provided that the system is not in installation mode, or made accessible for the sale of a single article. The tone sequences of the in-mutations are used to provide the user with feedback indicating that the merchandise is properly secured. A count of the total amount of pieces of equipment/merchandise is kept to inform the shop personnel.

Application for large fire alarm installations

Fire alarm installations for large factories are extremely sensitive for external noise, especially when large amounts of motors and/or TL-lamps are switched on or off. The insensitivity of the system described for noise make it especially suitable for application in large fire alarm installations. The installation procedures make the system extremely attractive for large factories and premises. The ability to indicate the exact location of a fire, either directly on a display or indirectly on the alarm equipment of the fire brigade is another important detail of the system described. The correct operation of the equipment can be guaranteed, in the absence of a malfunction alarm, as all important parts of the system are permanently surveyed.

Applicator for medical surveillance for aged and disabled patients

A refinement of the system consist of the addition of a second serial communication line, comparable with (4.S), connect in a similar way with modules. One of the communication lines is used to reach all houses or rooms on the left side of a street or corridor, while the other one reaches all houses or rooms on the right side. A variable allocation of numbers is used to allocate all odd numbers to one side and all even number to the other as appropriate. A start-address is used to let the numbering of the sensor circuits coincide with the numbers of the houses or rooms to be surveyed. The keyboard can now be configured in such a way that just one single alarm, instead of all alarms at once, can be switched of by typing a password.

Special properties of the system

The system can be coupled to an external computer to maintain a sales database or to locate a fire location on a map projected on the screen of a remote computer. These applications are possible as all in- and out-mutations can be transmitted one after the other to the computer, without problems associated due to improper arbitration, which might otherwise occur during an in- or out-mutation during an alarm and/or during simultaneous in- and/or out-mutations.

Claims

1. A surveillance system suitable for theft prevention with a considerably reduced sensitivity for electrical noise and/or crosstalk either caused by parasitic effects in sensor wiring or by external sources, effects which are frequently called electromagnetic interference, characterized by the presence of digital filters used to reduce the bandwidth and hence the effect of unwanted signals, which may trip a false alarm.

2. A cable system protected against tampering, of which a possible configuration is given in figure 1, to be used to protect merchandise from theft at the sales location, characterized by the fact that no switches nor other similar sensors are used in the cable, nor in the connectors.

3. A safe and accurate theft protection system for merchandise, based on a serial link (4.S) from cable sections which may be disconnected, characterized by a division of the system from claim 1, in parts A and B from figure 3, or any equivalent thereof, such that out-mutations of merchandise can even be signaled in the case that the corresponding sensor circuits are

removed together with one or more modules (4.I, 4.II, ...) from the serial communication line (4.S), used for communication between the (removed) modules and the controller (4.C).

4. A refinement of the system of claim 3, to be used to dynamically determine the amount of modules, connected to the serial line (4.S), characterized by the presence of an extra FEED signal sequence, which is applied to all inputs of all modules using a resistor with a high ohmic value, such that the feed signal is superseded by the lower output impedance of a next module (with a higher number in sequence) on the serial channel (4.S).

5. A refinement of the system of claim 4, to be used to detect the presence of a module of a certain type, like a sensor-module, a keyboard-module or a module with another function, connected to the serial channel (4.S), characterized by hardware provisions which feed the parallel inputs of a modules shift section with a pattern of one or more bits, either constant in time, or comprising a sequence, connected to the serial channel (4.S), said provision to be used in conjunction with a demodulation/recognition circuit and the FEED signal described in claim 4.

6. A refinement of the system of claim 4, used to avoid the potential ambiguity of the FEED signal with respect to a sequence of sensor signals, as found during transmission on the serial line, characterized by the introduction of a modulation/demodulation technique of any kind, which separates the delayed FEED signal from sequences produced by sensor data on the serial line.

7. A refinement of the system of claim 1, which delays simultaneous in- and out-mutations, characterized by the fact that alle in- and out-mutations are reported one after the other, while eventual alarm messages are suppressed for the time being.

8. A refinement of the system of claim 1, to be used to suppress sensor observations which are likely to be wrong, characterized by a decision circuit which detects the presence of a corrupted FEED signal indicating poor signal conditions on the serial communication line (4.S), said condition used to inhibit the filterprocess applied to the sensor data.

9. A refinement of the system of claim 4, to be used to detect the malfunctioning of the serial communication line (4.S), characterized by a decision circuit, cascaded with a digital filter and a threshold detector, used to provide a malfunction-alarm.

10. A refinement of the system of claim 1, to be used to display in- and/or out- and/or (multiple-) alarm conditions, characterized by a display unit capable to display the address of said mutations, using either an absolute addressing scheme, or an even/odd addressing scheme, which assigns all even addresses to one serial line and all odd addresses to another serial line.

11. A refinement of the system of claim 1, used to inform the user about in and/or out-mutations and/or multiple alarm messages, characterized by audible tone sequences and/or other audible signals, like for instance spoken messages.

12. A refinement of the system of claim 1, used to update a sales database, or to display a map containing fire locations or to update a comparable external representation of the state of the surveillance system, characterized by a communication link over which all in- and/or out-mutations on the inputs of the system can be transmitted without errors and/or ambiguity.

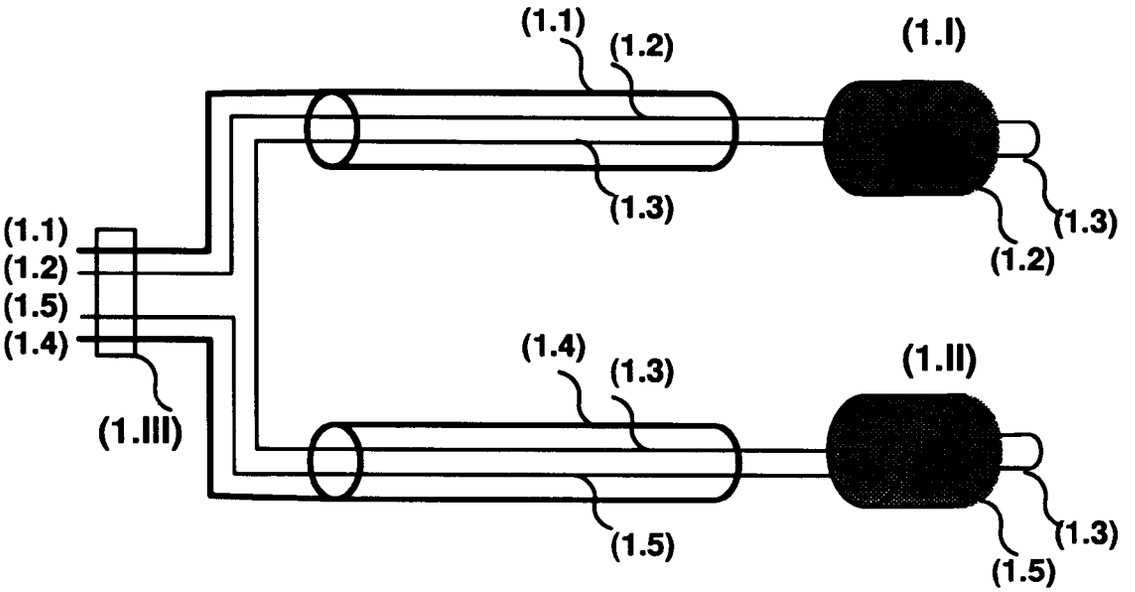

Fig. 1

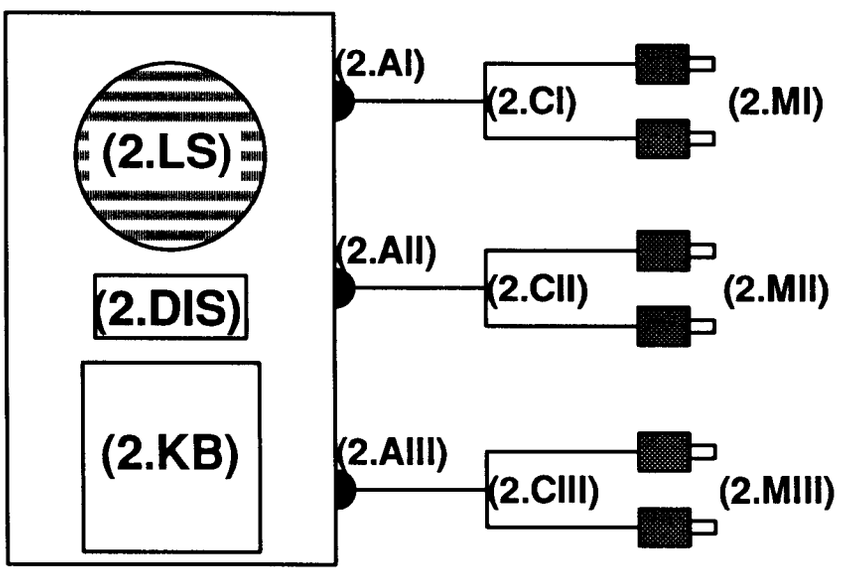

Fig. 2

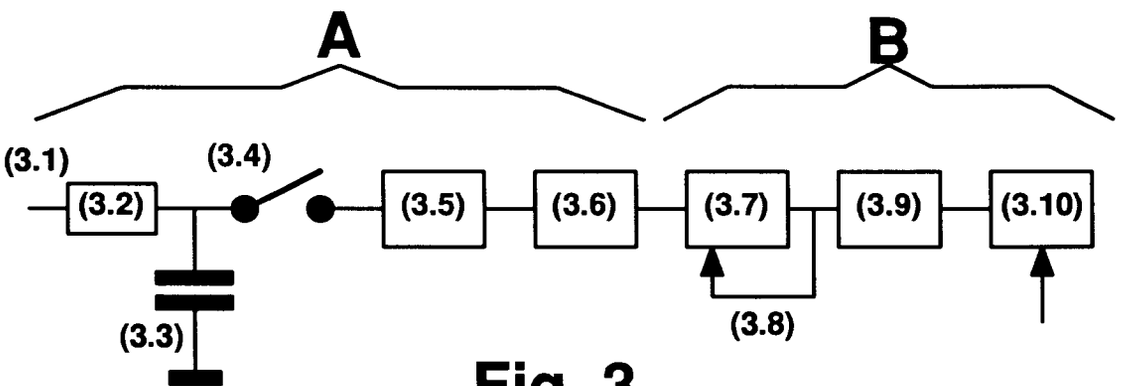

Fig. 3

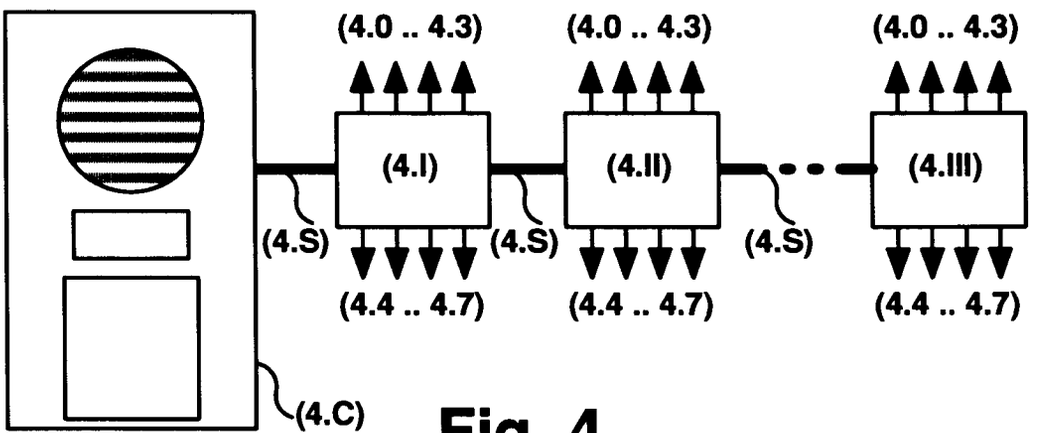

Fig. 4

European Patent Office

EUROPEAN SEARCH REPORT

Application Number

EP 92 20 0021

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
A,D	EP-A-0 116 701 (OTT) * abstract *	1	G08B13/14 G08B29/18
A	FR-A-2 589 609 (FRERE) * page 1, line 1 - page 2, line 11 *	1	
A	EP-A-0 290 413 (DIANTEK) * abstract *	1	
A,D	EP-A-0 052 193 (IBM) * abstract *	1	

TECHNICAL FIELDS SEARCHED (Int. Cl.5)

G08B

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	07 APRIL 1992	SGURA S.

CATEGORY OF CITED DOCUMENTS

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

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

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P0401)