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

(11) EP 1 953 063 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
06.08.2008 Bulletin 2008/32

(51) Int Cl.:
B61L 7/08 *(2006.01)*

(21) Application number: **07425064.8**

(22) Date of filing: **05.02.2007**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK RS

(71) Applicant: **ALSTOM FERROVIARIA S.P.A.**
12038 Savigliano (Cuneo) (IT)

(72) Inventor: **Campedelli, Francesco**
40068 S. Lazzaro di Savena (BO) (IT)

(74) Representative: **Karaghiosoff, Giorgio Alessandro**
Studio Karaghiosoff e Frizzi s.r.l.
Via Pecorile 25
17015 Celle Ligure (SV) (IT)

(54) Field vital output device and system for directly interfacing a control logic unit with at least one or more wayside units

(57) A field vital output device for directly interfacing a central control logic unit with at least one or more wayside units, such as relays, contacts, lamps and the like, which device comprises:
at least one input for the control signals generated by the control logic unit; at least one output port for a wayside unit actuating signal, which port is and/or may be connected to said wayside unit; means for enabling/disabling said output port to transmit the wayside unit actuating signal;
means for generating the wayside unit actuating output signal, which are connected to said output port; which control signals control the means for enabling/disabling the output port of the output device to allow/prevent transmission of the wayside unit actuating signal.

The device further comprises:
a switching element which sets the wayside actuating signal transmission enabled/disabed state of the port; electronics for detecting such state from the control imposed by the control logic unit, said output signal generating means being designed to be vitally disabled when the enabled/disabled state of said port does not correspond to the control condition imposed by the control logic.

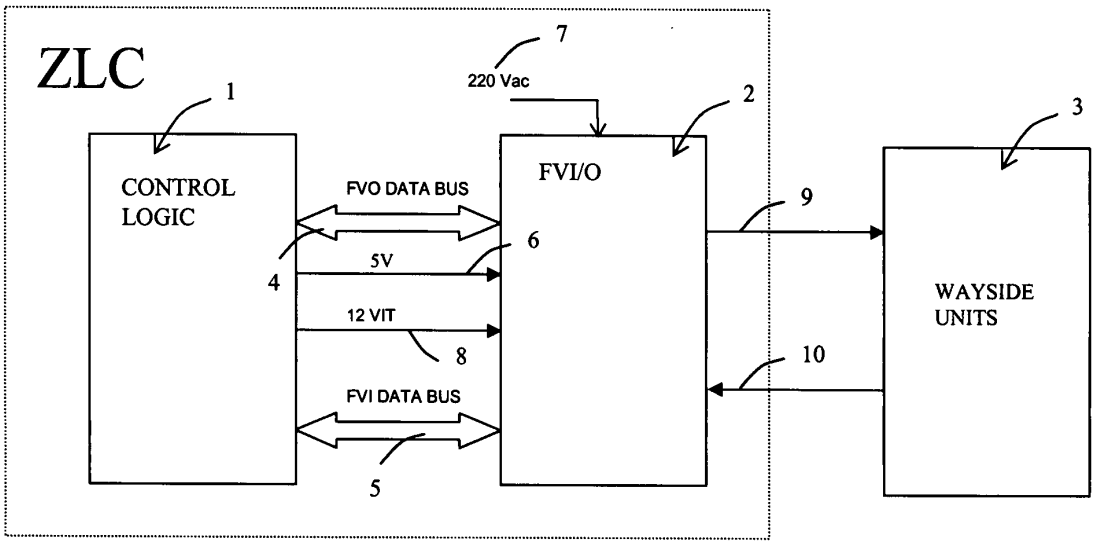

Fig. 1

EP 1 953 063 A1

Description

[0001] The invention relates to a field vital output device for directly interfacing a control logic unit with at least one or more wayside units, such as relays, contacts, lamps and the like, which device comprises:

at least one input for the control signals generated by the control logic unit;
at least one output port for transmission of a wayside unit actuating signal, which output port is and/or may be connected to said wayside unit;
means for enabling/disabling said output port to transmit the wayside unit actuating signal;
means for generating the wayside unit actuating output signal, which are connected to said output port;
which control signals, generated by the control logic unit, control the means for enabling/disabling the output port of the output device to allow/prevent transmission of the wayside unit actuating signal.

[0002] These systems are well known and, in railway applications or the like, consist of railway safety relays. They are used, for instance, for actuating remote safety relays, which are situated at or near the wayside units, such as particularly the relays used for remote parallel information transmission.

[0003] Prior art railway safety relays and thermal cutout circuits have a complex and bulky construction and do not ensure electrical insulation between field devices, i.e. wayside units and electronic devices. Furthermore, prior art railway safety relays require regular maintenance.

[0004] Therefore, the invention is based on the problem of providing a stationary output device for actuating field devices, such as wayside units or the like, which may be used instead of prior art railway safety relays, and provide at least the same or better safety standards as compared with prior art relays.

[0005] The invention fulfils the above objects by providing an output device as described hereinbefore, having:

a switching element that can set the wayside unit actuating signal transmission enabled/disabled state of the output port;
electronics for detecting such state from the control imposed by the control logic unit, the output signal generating means being designed to be vitally disabled when the enabled/disabled state of said port does not correspond to the control condition imposed by the control logic.

[0006] Thanks to this particular configuration, the conventional enabling/disabling means, typically fail-safe railway relays, may be replaced by commercial non-fail-safe electromechanical enabling/disabling means, such as force guided relays, without affecting the required safety standard, thereby reducing the volume for the requested function, and avoiding regular maintenance needs. This is achieved by associating the electromechanical means to electronics that, using an efficient mechanism for vital control of the switching state, allows to disable the output device whenever it comes to an unsafe permissive state.

[0007] Advantageously, the electromechanical switching element comprises at least one input and at least one output. The input-to-output relation is a function of the port enabled/disabled state and is vitally detectable by the electronics by comparison of the output of the switching element with a check code transmitted to its input.

[0008] According to one embodiment, the switching element has at least one pair of relay contacts, also known as auxiliary contacts, which are electrically connected to the input and the output of the switching element respectively. This pair of contacts is mechanically connected to the port enabling/disabling means, which are advantageously a second pair of relay contacts, so-called main contacts, which are electrically connected to the output signal generating means and the output port respectively. The two pairs of contacts are mechanically interconnected so that switching of one pair causes switching of the other, and are typically part of the same relay, which is also known as a force guided relay for its mechanical characteristic of only allowing rigid movements between the contacts. This allows to assess the closed/open state of the main contacts, and of the port, by analyzing the open/closed state of the auxiliary contacts. The auxiliary contacts are not energized by the wayside unit control voltage, thence their state may be easily detected by determining whether or not a control signal transmitted to one contact reaches the other contact of the pair. If the closed/open state of the auxiliary contacts, and therefore the enabled/disabled state of the port, is not consistent with the transmitted actuating control, the vital supply voltage is promptly cut off, and the port output is set to a safe non permissive state, corresponding to a de-energized condition of the wayside unit.

[0009] In a particularly advantageous configuration, the main contacts are normally open when idle (i.e. when no control is transmitted thereto) to ensure a safe non permissive state when the port is not selected/enabled, whereas the auxiliary contacts are normally closed when idle. Furthermore, the mechanical linkage among the contacts prevents them from being simultaneously closed/open. Thus, the logic port enabled state is reversed with respect to the state of the auxiliary contacts, which provides further protection against short-circuit failures.

[0010] When the output signal is a bipolar signal, e.g. when the wayside units are actuated by DC voltage, the device

may also include a signal polarity selection circuit, which may also accomplish the task of the output port enabling/disabling means. The use of multiple relay contacts, belonging either to the same relay or to different relays, allows to separately enable/disable each of the output signal poles and also to exchange polarities by using an antiparallel assembly of multiple relays designed to be controlled in a mutually exclusive manner. This does not affect the safety level, the enabled/disabled state of each contact being repeatedly vitally read.

[0011] The device operates in a safe manner, as the mechanisms for checking the actual port enabled/disabled state are directly operative on the function of vitally enabling output signal generation, and typically consist of DC/DC or DC/AC converters which are pulse-driven under the control of a DC enabling signal.

[0012] The device may advantageously comprise an overcurrent protection circuit, typically between the signal generator and the enabling/disabling relays, which is calibrated to prevent the generated output signal from reaching the output port, typically using a manually or software-wise resetting double break mechanism, as soon as a current absorption above a given trigger value is detected. This provides an additional safety mechanism for the device, particularly against short-circuit failures, such as those caused by cable insulation losses, especially if the output ports of the uncontrolled devices are normally short-circuited, e.g. by means of force guided relays. The combination of the overcurrent protection and short-circuit functions is particularly effective in protecting the wayside units from undue actuation, e.g. caused by double, separate, ordered contact failures, i.e. involving a short-circuit between cables directed to different units. These failures cause an uncontrolled unit to be in parallel with a controlled unit and to be unduly actuated as a result. However, since each uncontrolled unit is short-circuited due to the short circuit on the corresponding vital output device, the port that delivers the required power to actuate the unit is also short-circuited, thereby generating an increase of the delivered current, which causes overcurrent protection to be triggered before any undue actuation.

[0013] The device typically has a local unit interfacing with the central logic unit for controlling the device. The local unit is configured to convert the port enabling/disabling controls from the central logic unit to corresponding relay switching controls and is interfaced with the overcurrent protection circuit to disable the relay switching controls whenever the protection circuit is triggered. The local unit further comprises electronics for vital detection of the wayside unit actuating signal transmission enabled/disabled state of the output port. Advantageously, the port enabled/disabled state is detected by circulation of functional check codes (codewords) from the central logic unit to the local unit. The local unit turns the codewords into input signals for the switching element, reads the output thereof and codes such output into corresponding codewords to be transmitted back to the central logic unit. Thus, the central unit can assess the port state by checking the open/closed states of the contacts of the switching element, i.e. the auxiliary contacts of the enabling/disabling relay. Particularly, in the specific case of auxiliary contacts that are normally open when idle, the port is in the enabled state when the codewords do not circulate through said contacts.

[0014] In a further aspect, the invention relates to a vital input and/or output field system comprising:

a control logic unit for processing data and/or performing other control tasks, which logic unit comprises means for generating unique codes for functional check of the processing and/or receiving and/or transmitting steps being performed (so-called codewords) and a port for the transmission of the codewords generated at each step;
a fail-safe protection unit, with a memory containing a program for checking the functional steps of the logic unit and a program for checking the correctness of functional check codes (codewords) and the time sequence thereof, which protection unit communicates through a transmitting and/or receiving port with the logic unit and generates enabling signals when the codewords are correct;
a vital output device which communicates with the logic unit to receive control signals and/or transmit state/diagnostic signals based on the control codewords and interfaces with the protection unit to receive the vital enabling signal based on the result of codeword correctness and sequence checks.

[0015] The protection unit preferably comprises a power source which is controlled to deliver vital supply voltage to the output device in response to checkword/codewords correctness and sequence checks. The vital supply voltage is cut off when the enabled/disabled state of the output device does not correspond to the control condition imposed by the control logic.

[0016] For increased reliability and safety, the system is preferably of the redundant type, which means that all wayside units or at least some of them are controlled by a pair of parallel equivalent vital output devices. The system comprises a vital redundancy management circuit which is configured to exclusively enable the first or second device respectively, to ensure safe actuation of the wayside unit in case of malfunction of either device.

[0017] According to an embodiment, the system comprises two or more vital output devices for directly interfacing a control logic unit with two or more wayside units, such as relays, contacts, lamps and the like, which devices comprise:

an overcurrent protection circuit, which is calibrated to prevent the generated output signal from reaching the output port of the device if current absorption exceeds a given trigger value;
a relay having at least one pair of normally open contacts, which can short-circuit the output port, when controlled

to do so,
which system is configured to short circuit the output ports of uncontrolled devices so that the overcurrent protection circuit of the controlled port can be triggered to prevent any insulation loss of the cables directed to the unit from causing undue actuation of uncontrolled units.

[0018] Particularly, the system is configured to protect the units from undue actuation caused by double separate ordered contact on multipolar cables and the relays used to short circuit the ports are force guided by auxiliary contacts to allow rereading of the actual enabled state, by codeword circulation.

[0019] In another aspect, the invention relates to a system for safe digital information exchange between a control logic unit and one or more remote wayside units, by means of electrically insulated control conductors, which information is transmitted by the logic unit to the remote unit/s in the form of controls for forcing the presence/absence of voltage corresponding to the type of binary information desired on one or more ports that can be accessed by the remote unit/s. The energized/de-energized state of the port/s is determined by enabling/disabling one or more force guided relays in electric communication with voltage generating means. The enabled/disabled state of said relay/s is reread by the control logic by circulation of codewords for vitally disabling such generating means when the enabled/disabled state of the relay/s does not correspond to the control condition imposed by the control logic due to the presence of failures or undesired potentials possibly induced on control conductors due to degradation of ground and mutual insulation of conductors.

[0020] Particularly, the system is configured to cyclically check the insulation of control conductors by repeated vital reading of the actual enabled state of a remote port after transmission of a predetermined sequence of enabling codewords to the control conductors.

[0021] Further features and improvements will form the subject of the dependent claims.

[0022] The features of the invention and the advantages derived therefrom will be more apparent from the following detailed description of the annexed drawings, in which:

Fig. 1 is a simplified block diagram of a subsystem for safe management of field vital input/output.
Fig. 2 is a diagram of the vital output device of the invention with reference to a single output port.
Fig. 3 is the block diagram of relay-driven actuation and polarity selection stage.
Fig. 4 is the block diagram of the vital power supply stage.
fig. 5A is a block diagram of a first embodiment of the overcurrent protection stage.
Fig. 5B shows a second embodiment of the overcurrent protection stage.
Fig. 6 is the block diagram of central control logic.
Fig. 7 shows an example of a double separate ordered contact between two wayside units.
Fig. 8 is a simplified block diagram of a redundant subsystem for safe management of field vital input/output.

[0023] While the example of the figures mainly relates to the field of railways, and particularly to an output device and the associated control and/or monitoring system, for controlling wayside units of a railway station system, this invention shall not be intended to be limited thereby, as it is applicable to any output device that has to accomplish fail-safe functions and use non fail-safe hardware for accomplishing its remote unit actuation functions.

[0024] Referring to Fig. 1, the subsystem of this block diagram, known as ZLC, i.e. Zone Logic Computer, comprises a control logic unit 1, which interfaces with one or more wayside units 3, such as relays, contacts, lamps or the like, through a Field Vital Input/Output FVIO. The device 2 is designed both to interpret the control signals from the logic 1 and convert them into safe actuation signals 9 for the wayside unit 3 (Field Vital Output function, i.e. FVO 102), and to safely read data 10 from the wayside unit 3 (Field Vital Input function, i.e. FVI 202). The device 2 interfaces with the logic unit 1 by one or more data buses, two data buses being shown in Fig. 1, for output 4 and input 5 respectively. At its input, the device 2 receives power 6 for its internal digital circuits (+5V), AC voltage 7, typically 220 VAC, for generating the actuation signal and a DC voltage 8 (12 VIT) for vitally enabling the generation of such actuation signal.

[0025] Fig. 2 is a block diagram of the vital output device FVO 102 with reference to a single output port. In one embodiment, the device 102 comprises 8 overcurrent-protected output modules which, depending on the control from the logic 1, can provide a positive or negative DC voltage (typically $\pm$48V, $\pm$144V) or an AC voltage (typically 150 Vac), for actuating the wayside unit 3.

[0026] The voltage for actuating the wayside unit connected to the output port 9 is generated by the module 10 which comprises, in a preferred embodiment, switching converters that can convert the input AC voltage 7 into the desired output voltage V when the vital signal 8 is enabled. The generator 10 comprises four converters to provide DC voltages of 24V, 48V and 144V and an AC voltage of 150 V respectively. The circuit 110 selects the appropriate output voltage by actuating the corresponding converter. According to an embodiment, such selection occurs by grouping ports: preferably eight modules, or six and two modules, or four and four modules. Thus, each port may be freely configured as needed. For safety, such configuration is performed manually by the installation and/or testing operator during installation

and/or testing, by using jumpers or connectors on the motherboard of the module 110. Fig. 4 shows the structure of the generator module 10, which is well known in the art, in greater detail. Once the input AC voltage 7 has been high frequency filtered by the filter EMC 210 and has passed the overcurrent protection stage 310, it reaches the rectifier 410, typically a diode bridge, and then the AC/DC or AC/AC conversion stage. Conversion occurs by switching, as is known in the art, and is PWM driven under the control of the DC enabling signal 8. Particularly, the enabling signal is operative on the pulsed-driving stage to prevent generation of driving pulses when vital power +12VIT is not present. The diagram of Fig. 4 is complemented by additional overcurrent protection components 910 and insulation components 710. In a first example, the insulation measurement circuit is the one designated by 103 in Fig. 2.

[0027] Otherwise, a circuit for checking ground insulation 620 may be used, which is interfaced with the local logic through a diagnostic circuit 70. Any ground insulation loss measurement device may also be used, provided that it complies with EEC standard EN 61557-8.

[0028] The output voltage from the generator 10 reaches the overcurrent protection circuit 20 which disables the output whenever current absorption exceeds the trigger value. As described in greater detail hereafter, a solid state double break switch 320' and a double measurement circuit 120', as shown in Figures 5A and 5B, may be possibly provided.

[0029] Two maximum current thresholds are provided, depending on overcurrent time. The first threshold (known as "thermal" threshold) is lower than the second threshold (known as "magnetic" threshold) but may be held for a longer time. The solid state switches 310 and the relays 130 and 230 of Fig. 3 may be disabled under the control of the ZLC control logic software, which may break both phases of the signal (double-break) and directly remove the port enabling control, when the "thermal" current threshold is exceeded: this condition is communicated by the central control logic by corresponding codewords.

[0030] When the "magnetic" current threshold is exceeded it is the local logic (designated as 20 in Fig. 2) that causes the solid state switches 320 and/or 320', referring to the variants of Figures 5A and 5B respectively, and possibly the relays 130 and 230 of Fig. 3, to break both signal phases (double-break). Such condition is indicated by a LED on the front panel 80 and is diagnosed by the module 70 through the local logic 60. For manual reset of overcurrent protection, a button is provided on the panel 80 which enables the modules of the overcurrent device 20 again. Reset may be also controlled remotely, by software means.

[0031] The trigger value of the protection circuit 20 is defined by local configuration, as a function of the output voltage and the type of controlled unit. For example, a default "thermal" value of 0.1 A corresponds to the 48V outputs.

[0032] Referring to the embodiment of Figure 5B, the overcurrent protection function 20 is provided by current measurement (sensing) circuits 120, and a static switch 320, which is set to the open state by the circuit 220, when the sensed current exceeds the trigger threshold.

[0033] In the variant embodiment of Figure 5A, the overcurrent protection function 20 is provided by current measurement (sensing) circuits 120, 120' on both power conductors, and a double static switch 320, 320' which is set to the open state by the circuit 220, when the sensed current exceeds the trigger threshold.

[0034] According to another feature, a test is regularly provided to check overcurrent protection effectiveness, which test is controlled by the central logic SW (software) before ports are enabled. Particularly referring to the variant embodiment of the figure, before enabling any port, the SW closes a dummy load of known value is closed for a short time, to cause the "thermal" current threshold to be exceeded, and checks that the local sensing circuit detects this situation by dedicated codewords, and then the SW opens the switch 320 and checks that the sensed current changes back to zero. If one of these conditions is not fulfilled, the overcurrent protection circuit does not operate properly and the corresponding port is not enabled.

[0035] After appropriate high frequency noise filtering by the filter 50, to meet the electromagnetic compatibility standard EN50121-4, the output voltage from the overcurrent protection module 20 reaches the output of the port 9 through the relay-driven actuation and polarity selection stage 30 which form the core of the device.

[0036] Referring to Fig. 3, the relay-driven actuation and polarity selection stage 30 comprises a pair of force guided relays 130 and 230, each having two pairs of main contacts 133-134, 135-126 and 233-234, 235-236, which are normally open when idle, i.e. are able to break the circuit when no driving signal 137, 237 is detected. Each relay 130, 230 further comprises a pair of auxiliary Drive-Sense contacts (131-132, 231-232), which are normally closed when idle. The components 138 and 238 reverse the output signal with respect to the input to protect against short circuit failures between Drive 131, 231 and Sense 132, 232.

[0037] Force guided relays, such as those compliant with EN 50205 and UIC736e, sold by ELESTA relays GmbH, are so called because they have mechanically linked contacts, so that switching of one pair of contacts causes switching of the other pair/s of contacts. Particularly, normally open and normally closed contacts cannot be closed at the same time. According to the above mentioned standard, if one pair of normally closed contacts does not open when the relay is actuated, e.g. due to contacts being joined together, all the remaining normally open contacts of the relay must not close or must be spaced at least 0.5 mm apart. This allows to reliably assess the closed/open state of the main contacts 133-134, 135-126 and 233-2234, 235-236, by analyzing the open/closed state of the respective Drive/Sense auxiliary contacts 131-132, 231-232. The auxiliary contacts are not energized, thence their state may be easily detected by

determining whether or not a control signal transmitted to the Drive terminal reaches the Sense terminal, particularly with a opposite polarity, due to the reversal 138, 238.

[0038] The pair of force guided relays 130, 230 has the function of actuating the device, i.e. of transmitting the voltage generated by the module 10 to the output port 9, and of reversing the polarity thereof. The two relays 130, 230 are connected with parallel inputs 133/233, 135/235 and antiparallel outputs 134/236, 136/234, to provide a bipolar output signal which is in phase with the input signal, if the relay 130 is actuated, or in counterphase with the input signal, if the relay 230 is actuated.

[0039] The two relays 130, 230 are actuated by a high logic signal "1" on the control terminals 137, 237. The driving logic is configured to actuate the two relays 130, 230 when the ON+ and ON- controls 530, 430 are at the high logic level "1" and in the enabled "overcurrent protection" signal conditions respectively. This signal comes from the block 20, upstream from the stage 30, and is disabled, i.e. assumes the low logic value "0", when overcurrent protection is triggered, whereas the controls 530 and 430 come from the central logic unit 1 through the local logic 60. The driving signals 137, 237 of the relays 130 and 230 come from the AND ports 630 and 730 respectively, which have the "overcurrent protection" signal 330 at their outputs, as well as the ON+ signal 530 and ON- signal 430 respectively. If overcurrent protection is triggered, then the relay drive is disabled whatever the control condition on the terminals 430 and 530. If protection is not triggered, the two relays 130, 230 may be controlled by sending a high logic level signal on ON+ or ON-. The local control logic 60 shall ensure that these controls are mutually exclusive, to prevent both relays 130, 230 from being in a simultaneously actuated condition, which would cause the port to be shorted. Should such short-circuit occur due to a failure, safety would be ensured anyway by overcurrent protection, which causes both relays 130, 230 to be disabled, by disabling the signal 330.

[0040] A third relay NCC 40 provides the "neutral closed circuit" function, when the port is not actuated, i.e. when both ON+ and ON- controls 530, 430 are at the low logic level "0" and the board is operating, as two boards belonging to the systems N and R respectively (see Fig. 8) may be connected in parallel to the same units. This condition ensures that no failure or off condition of one of the systems causes the relay to close (undue NCC). This normally open forced guide relay 40 is driven 140 by a logic port NOR 830 having the ON+ and ON- signals 530, 430 as inputs. Actuation of the relay causes the port to be shorted, thereby ensuring effective protection against cable insulation loss failures, as better shown hereafter. The actuation state of the NCC relay 40 may be diagnosed from its auxiliary contact (not shown).

[0041] Safety of the device is assured by a dynamic mechanism for controlling the actuation state of the relays 130, 230, which is directly operative on the function of vitally enabling 8 the actuation signal generator 10. If the closed/open state of the auxiliary contacts 131-132 and 231-232, and therefore the opened/closed state of the main contacts 133-134, 135-136 and 233-234, 235-236 is not consistent with the transmitted actuating control 530, 430, the vital supply voltage 8 is promptly cut off, and the port output 9 is set to a safe non permissive state, corresponding to a de-energized condition of the wayside unit 3.

[0042] For the purposes of vital check, the two relays 130 and 230 are independently managed by the local logic 60 through the Drive+/Sense+ circuits 131-132 and Drive-/Sense- circuits 231-232, under the control of the central logic 1 of the ZLC subsystem. Checking occurs by circulating a binary check word (codeword), generated by the logic 1 of the ZLC system, through the (normally closed) auxiliary contact, corresponding to the (normally open) main contact of the relevant relay 130, 230. When the port is not controlled, the codeword circulates through the closed contacts and is reread and denied by the logic. Codeword denial protects against short circuit failures between Drive and Sense.

[0043] If the codeword read by the logic 1 does not correspond to the transmitted codeword, the ZLC system disables vital power 7 to the subsystem in use, and the relevant output ports 9 are not powered. The system is set to unpowered port conditions, in a response time of less than 200 ms. The wayside units 3 with which the FVO subsystem 102 interfaces shall ensure they will not be set to a permissive state for a time not shorter than such safe response time.

[0044] The central logic 1, as exemplified in Fig. 6, is a vital computer logic, such as the one disclosed in WO03093999, and is basically composed of two main sections:

- A control section 101, which consists of a microprocessor system, including the required peripherals (program memory, Random Access Memory (RAM), serial interfaces, auxiliary clock and reset signal generating circuits, watchdogs), for interfacing both with the vital output devices 102 through the bus 401 and with other subsystems through the bus 501;
- A vital protection section 201, i.e. a checking and protecting unit which uses hardware blocks and safety code-related software blocks which form a system for certifying the check codes or words being generated by the control section 101 based on the feedback transmitted thereto by the vital output devices 102, controlled by said section 101, to control the compatibility with the received control and the proper execution of the controlled function. The protecting unit has the function of ensuring the achievement of a safety state in case of failures in the control section. The safety architecture of the vital computer module 1 is of the reactive type; the protection section 201 has the task of identifying any behavior susceptible of affecting the safety of the control section 101 and to force the system into a safety state in a given time. The protection section is designed with fail-safe techniques.

[0045] The control section 101 and the protection section 201 are managed by two independent processors, which communicate by a Dual Port RAM 301. More specifically, the control section 101 generates codewords to feed the protection section 201, which cyclically consumes the codewords and detects possible control process errors.

[0046] The protection section 201 vitally generates the voltage 8 required to enable the voltage generators 10 on the vital output device 102. The checks performed by the protection section 201 are both logic and time checks; the protection section periodically receives codewords from the control section 101, which codewords are used to confirm proper performance of all safety-related operations, and checks the validity thereof. If codewords are logically correct, they arrive in well defined time ranges and the self-diagnostic process of the protection section 201 detects no failure, then the protection section 201 provides vital power supply 8, otherwise, it removes such power supply, and prevents any signal transmission to the wayside units.

[0047] Thanks to this vital check mechanism, the output device 102 can safely deliver the power required to actuate the wayside unit 3, without using expensive and bulky fail-safe railway relays.

[0048] The following table summarizes the possible failure types, as well as their effects:

	Control	Failure	Expected port state	Actual port state	Vitally detected failure
1	ON +	RL1 always closed	+V	+V	NO
2	ON +	RL1 always open	+V	Unpowered	NO
3	ON +	RL2 always open	+V	+V	NO
4	ON +	RL2 always closed	+V	0V DC port: Overcurrent protection triggered	YES Detected by vital control on RL2
5	ON +	RL1, RL2 always open	+V	Unpowered	NO
6	ON +	RL1, RL2 always closed	+V	0V DC port: Overcurrent protection triggered	YES Detected by vital control on RL2
7	ON -	RL1 always closed	-V	0V DC port: Overcurrent protection triggered	YES Detected by vital control on RL1
8	ON -	RL1 always open	-V	-V	NO
9	ON -	RL2 always open	-V	Unpowered	NO
10	ON -	RL2 always closed	-V	-V	NO
11	ON -	RL1, RL2 always open	-V	Unpowered	NO
12	ON -	RL1, RL2 always closed	-V	0V DC port: Overcurrent protection triggered	YES Detected by vital control on RL1
13	Uncontrolled port	RL1 always closed	Disabled	+V	YES Detected by vital control on RL1
14	Uncontrolled port	RL1 always open	Disabled	Unpowered	NO
15	Uncontrolled port	RL2 always open	Disabled	Unpowered	NO
16	Uncontrolled port	RL2 always closed	Disabled	-V	YES Detected by vital control on RL2

(continued)

	Control	Failure	Expected port state	Actual port state	Vitally detected failure
17	Uncontrolled port	RL1, RL2 always open	Disabled	Unpowered	NO
18	Uncontrolled port	RL1, RL2 always closed	Disabled	0V DC port: Overcurrent protection triggered	YES Detected by vital control on RL1, RL2

[0049] As shown above, there are two types of failures that cannot be detected by the vital control:

- failures in which the port state is consistent with the expected state as a function of the control;
- failures in which the port state is "unpowered".

[0050] Therefore, in both cases, the undetected failure condition is not inconsistent with safety requirements.

[0051] Insulation is a critical aspect in high safety applications, such as railway applications. Any voltage induced on the cables as a result of an insulation loss may cause undesired actuation of wayside units, which may even have fatal consequences (like those possibly ensuing from the actuation of a switch or a train stop lamp). Therefore, the vital output device 102 of the invention is designed to be interfaced with diagnostic devices 601, 103 for measuring ground insulation losses, pursuant to EEC standard EN 61557-8. Insulation loss checks may be performed either at the supply cables and at wayside cables. In the former case, the measuring device indicates ground insulation losses of the group of ports having the same power source, in the latter, insulation loss is indicated for each port. In both cases, the control unit can promptly disable the relevant port.

[0052] In addition to the above, any undesired control induced by noise on the cables that interface the control unit 1 with the vital output device 102 is prevented by the vital port state control mechanism, whereas the combination of the above discussed overcurrent 20 and short-circuit 40 protection functions is particularly effective in protecting the wayside units from undue actuation, e.g. caused by double separate ordered contact failures (d.s.o.c.), as schematically shown in Fig. 7. These failures involve a short circuit between cables directed to different units and cause an uncontrolled unit (unit2) to be in parallel with a controlled unit (unit1) and to be unduly actuated as a result. However, since each uncontrolled unit is short-circuited due to the short circuit on the corresponding vital output device 40 (NCC), the port (OUT#1) that delivers the required power to actuate the unit is also short-circuited, thereby generating an increase of the delivered current (Imax), which causes overcurrent protection 20 to be triggered before any undue actuation.

[0053] Referring to Fig. 7, to prevent any undue actuation of the unit2, the overcurrent protection 20 trigger value shall be such that the residual voltage at the ends of the unit2 is lower than its minimum actuation threshold. The residual voltage value at the ends of the unit is closely related to the length of the cable section, whose resistance is designated by R.

[0054] For an even safer protection, the NCC relay state is controlled by the ZLC logic SW by circulation of codewords through one of the auxiliary contacts of such relay.

[0055] For increased reliability and safety, the ZLC subystem is preferably of the hot backup redundant type, which means that the wayside unit 3 is driven by a pair of equivalent subsystems as described and shown in Fig. 1. Fig. 8 is a block diagram of this redundant subsystem. N and B designate Normal and Backup respectively. Each of the N and B subsystems can safely provide the same functions. Particularly, they operate in parallel, i.e. they transmit the same controls and perform the same processing, although only the input/output port of one of the two devices 2, 2', typically the N device, is enabled. Should a malfunction occur to one of the two subsystems, a vital redundancy management circuit (not shown) enables the other subsystem to assure safe actuation of the wayside unit 3.

[0056] Redundancy is particularly advantageous in case of failure of the short circuit protection circuit 40 of one of the ports of the vital output device 102. The same function may be thus accomplished by the short circuit protection circuit of the output device of the parallel redundant subsystem associated to the unit, which further increases the safety of the whole ZLC subsystem.

[0057] Obviously, the invention is not limited to the above description and figures, but may be greatly varied, especially as regards construction, without departure from the inventive teaching disclosed above and claimed below.

Claims

1. A field vital output device for directly interfacing a central control logic unit with at least one or more wayside units, such as relays, contacts, lamps and the like, which device comprises:

   at least one input for the control signals generated by the control logic unit;
   at least one output port for transmission of a wayside unit actuating signal, which output port is and/or may be connected to said wayside unit;
   means for enabling/disabling said output port to transmit the wayside unit actuating signal;
   means for generating the wayside unit actuating output signal, which are connected to said output port;
   which control signals, generated by the control logic unit, control the means for enabling/disabling the output port of the output device to allow or prevent transmission of the wayside unit actuating signal,

   characterized in that the device further comprises:

   a switching element that can set the wayside unit actuating signal transmission enabled/disabled state of said port;
   electronics for detecting said state from the control imposed by the control logic unit, said output signal generating means being designed to be vitally disabled when the enabled/disabled state of said port does not correspond to the control condition imposed by the control logic.

2. A device as claimed in claim 1, **characterized in that** the switching element comprises at least one input and at least one output, the input-to-output relation being a function of the port enabled/disabled state, said state being vitally detectable by the electronics by comparison of the output of the switching element with a check code transmitted to its input.

3. A device as claimed in claim 2, **characterized in that** the switching element has at least one pair of relay contacts, which is mechanically linked to the port enabling/disabling means, the contacts of the pair being electrically connected to the input and the output of the switching element respectively.

4. A device as claimed in claim 3, **characterized in that** the port enabling/disabling means comprise at least one relay having at least one pair of contacts, which are electrically connected to the output signal generating means and the output port respectively, said pair of contacts being mechanically linked to the pair of contacts of the switching element, so that switching of one pair causes switching of the other pair.

5. A device as claimed in claim 4, **characterized in that** one pair of contacts is normally closed when idle, and the other is normally open when idle, the contacts being mechanically linked together so that they cannot be closed/open at the same time.

6. A device as claimed in claim 5, **characterized in that** the contacts of the switching element are normally closed when idle, and the contacts of the port enabling/disabling means are normally open when idle.

7. A device as claimed in one or more of the preceding claims 4 to 6, **characterized in that** the contacts of the switching element and the contacts of the port enabling/disabling means are part of a single relay, particularly a so-called force guided relay which, when actuated, switches the contacts to a reversed state with respect to the idle state.

8. A device as claimed in one or more of the preceding claims, **characterized in that** it comprises a circuit for selecting the output signal polarity.

9. A device as claimed in claim 8, **characterized in that** the output port enabling/disabling means include said polarity selection circuit.

10. A device as claimed in one or more of the preceding claims, **characterized in that** the output signal is a bipolar signal and the port enabling/disabling means comprise a first relay having pairs of normally open contacts to enable/disable the first of the two output signal poles.

11. A device as claimed in claim 10, **characterized in that** the port enabling/disabling means comprise a second relay having pairs of normally open contacts to enable/disable the second of the two output signal poles.

12. A device as claimed in claim 10, **characterized in that** the relay comprises at least two pairs of normally open contacts to enable/disable each pole of the output signal.

13. A device as claimed in claim 12, **characterized in that** the port enabling/disabling means comprise a second relay having at least two pairs of normally open contacts, which is mounted in parallel to the first relay, with reversed inputs or outputs to provide, when actuated, a reversed polarity signal to the output port, the two relays being driven in a mutually exclusive manner.

14. A device as claimed in one or more of the preceding claims 10 to 13, **characterized in that** the relay/s comprise at least one pair of normally closed auxiliary contacts, which are mechanically forced to open when the corresponding main contacts close.

15. A device as claimed in one or more of the preceding claims, **characterized in that** the output signal generating means have at least one input for a vital enabling signal for enabling/disabling output signal generation.

16. A device as claimed in claim 15, **characterized in that** the output signal generating means comprise at least one DC/DC or DC/AC converter which is provided in combination with vital enabling/disabling means.

17. A device as claimed in claim 16, **characterized in that** the vital enabling/disabling means generate a vital enabling signal, which is operative on pulsed-driving of said at least one converter, to prevent generation of driving pulses when vital power supply is not present.

18. A device as claimed in one or more of the preceding claims, **characterized in that** it comprises an overcurrent protection circuit, said protection circuit being calibrated to prevent the generated output signal from reaching the output port of the device if current absorption exceeds a given trigger value.

19. A device as claimed in claim 18, **characterized in that** the overcurrent protection circuit is located downstream from the output signal generating means, and is configured to disable the device output by double-break of the circuit that connects the output signal generating means with the output port enabling/disabling means.

20. A device as claimed in claim 18 or 19, **characterized in that** the overcurrent protection circuit comprises at least one static switch having a manual or software-controlled reset arrangement.

21. A device as claimed in one or more of the preceding claims, **characterized in that** it comprises at least one switch element that can short-circuit the output port, when controlled to do so.

22. A device as claimed in claim 21, **characterized in that** said switch element is a relay, particularly a force guided relay having at least one pair of normally open contacts.

23. A device as claimed in one or more of the preceding claims, **characterized in that** it has a local unit interfacing with the central logic unit for controlling the device.

24. A device as claimed in claim 23, **characterized in that** the local unit is configured to convert the port enabling/disabling controls from the central logic unit into corresponding relay switching controls.

25. A device as claimed in claim 24, **characterized in that** the local unit interfaces with the overcurrent protection circuit to disable the relay switching controls whenever the overcurrent protection circuit is triggered due to a local decision and/or to a central logic unit SW decision.

26. A device as claimed in claims 23 to 25, **characterized in that** the local unit comprises electronics for vital detection of the wayside unit actuating signal transmission enabled/disabled state of the output port.

27. A device as claimed in claim 26, **characterized in that** the port enabled/disabled state is detected by circulation of codewords from the central logic unit to the local unit, which local unit turns said codewords into input signals for the switching element, reads the element output and codes said output into corresponding codewords to be transmitted back to the central logic unit.

28. A device as claimed in claim 27, **characterized in that** the port state is detected by checking the open/closed state

of the switching element contacts, the port being in the enabled state when said contacts are open.

29. A field vital input and/or output system comprising:

a control logic unit for processing data and/or performing other control tasks, which logic unit comprises means for generating unique codes for functional check of the processing and/or receiving and/or transmitting steps being performed (so-called codewords) and a port for the transmission of the codewords generated at each step;
a fail-safe protection unit, with a memory containing a program for checking the functional steps of the logic unit and a program for checking the correctness of functional check codes (codewords) and the time sequence thereof, which protection unit communicates through a transmitting and/or receiving port with the logic unit and generates enabling signals when the codewords are correct;
a vital output device as claimed in one or more of the preceding claims, which device communicates with the logic unit to receive control signals and/or transmit state/diagnostic signals based on the control codewords and interfaces with the protection unit to receive the vital enabling signal based on the result of codeword correctness and sequence checks.

30. A system as claimed in claim 29, **characterized in that** the protection unit preferably comprises a power source which is controlled to deliver vital supply voltage to the output device in response to checkword/codewprds correctness and sequence checks.

31. A system as claimed in claim 30, **characterized in that** the vital supply voltage is cut off when the enabled/disabled state of the output device does not correspond to the control condition imposed by the control logic.

32. A system as claimed in one or more of the preceding claims 29 to 31, **characterized in that** it comprises a second vital output device as claimed in one or more of the preceding claims 1 to 28, having its output ports in parallel to the first device, the system comprising a vital redundancy management circuit which is configured to exclusively enable the first or second device respectively, to ensure safe actuation of the wayside unit that is or may be connected to such ports, in case of malfunction of either device.

33. A system as claimed in one or more of the preceding claims 29 to 32, **characterized in that** it comprises two or more vital output devices as claimed in one or more of claims 1 to 28, for directly interfacing a control logic unit with two or more wayside units, such as relays, contacts, lamps and the like, which devices comprise:

an overcurrent protection circuit, which is calibrated to prevent the generated output signal from reaching the output port of the device if current absorption exceeds a given trigger value;
a relay having at least one pair of normally open contacts, which can short-circuit the output port, when controlled to do so,
which system is configured to short circuit the output ports of uncontrolled devices so that the overcurrent protection circuit of the controlled port can be triggered to prevent any insulation loss of the cables directed to the unit from causing undue actuation of uncontrolled units.

34. A system as claimed in claim 33, **characterized in that** it is configured to protect the units from undue actuation caused by double separate ordered contact failures on multipolar cables.

35. A system as claimed in claim 33 or 34, **characterized in that** the relays used to short circuit the ports are force guided relays having auxiliary contacts for reading the actual enabled state by circulation of codewords.

36. A system for safe digital information exchange between a control logic unit and one or more remote wayside units, by means of electrically insulated control conductors, which information is transmitted by the logic unit to the remote unit/s in the form of controls for forcing the presence/absence of voltage corresponding to the type of binary information desired on one or more ports that can be accessed by the remote unit/s, **characterized in that**
the presence/absence of voltage at the port/s is determined by enabling/disabling one or more force guided relays in electric communication with means for generating said voltage, the enabled/disabled state of said relay/s being reread by the control logic by circulation of codewords for vitally disabling the generating means when the enabled/disabled state of the relay/s does not correspond to the control condition imposed by the control logic due to the presence of failures or undesired potentials possibly induced on control conductors due to degradation of ground and mutual insulation of conductors.

37. A system as claimed in claim 35, **characterized in that** it is configured to cyclically check the insulation of control conductors by repeated vital reading of the actual enabled state of a remote port after transmission of a predetermined sequence of enabling codewords to the control conductors.

38. A system as claimed in claim 36 or 37, **characterized in that** it also has one or more of the features as claimed in claims 29 to 35.

39. A system as claimed in one or more of the preceding claims 36 to 38, **characterized in that** it is provided in combination with a vital output device as claimed in claims 1 to 28.

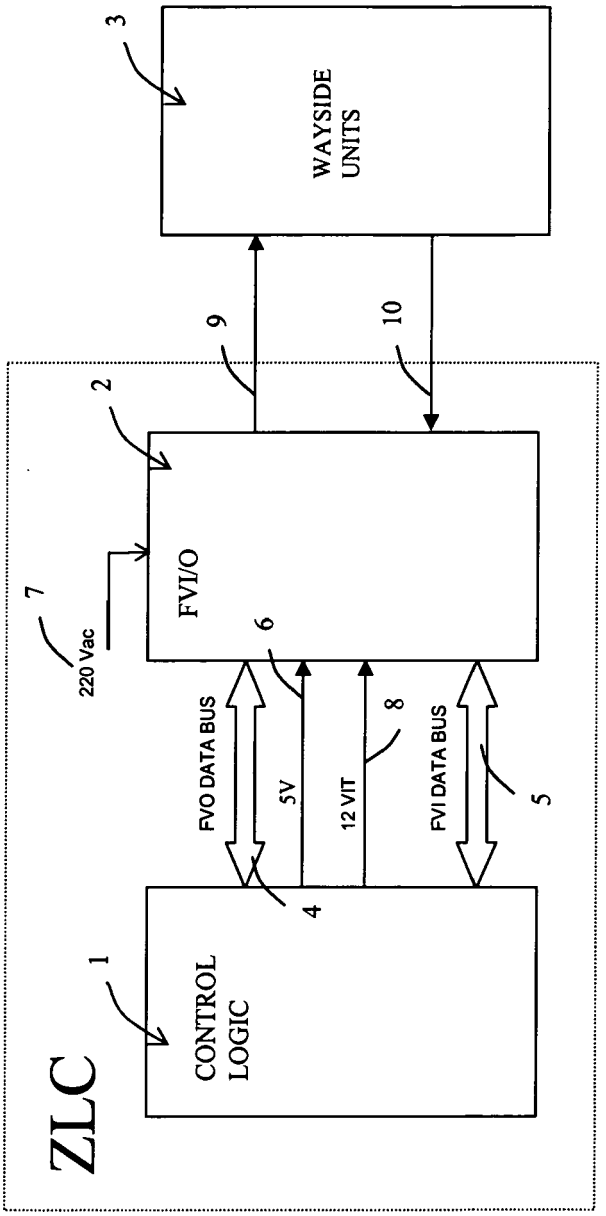
3
WAYSIDE UNITS
9
10
2
FVI/O
7
220 Vac
6
FVO DATA BUS
5V
12 VIT
8
FVI DATA BUS
5
4
1
CONTROL LOGIC
ZLC

Fig. 1

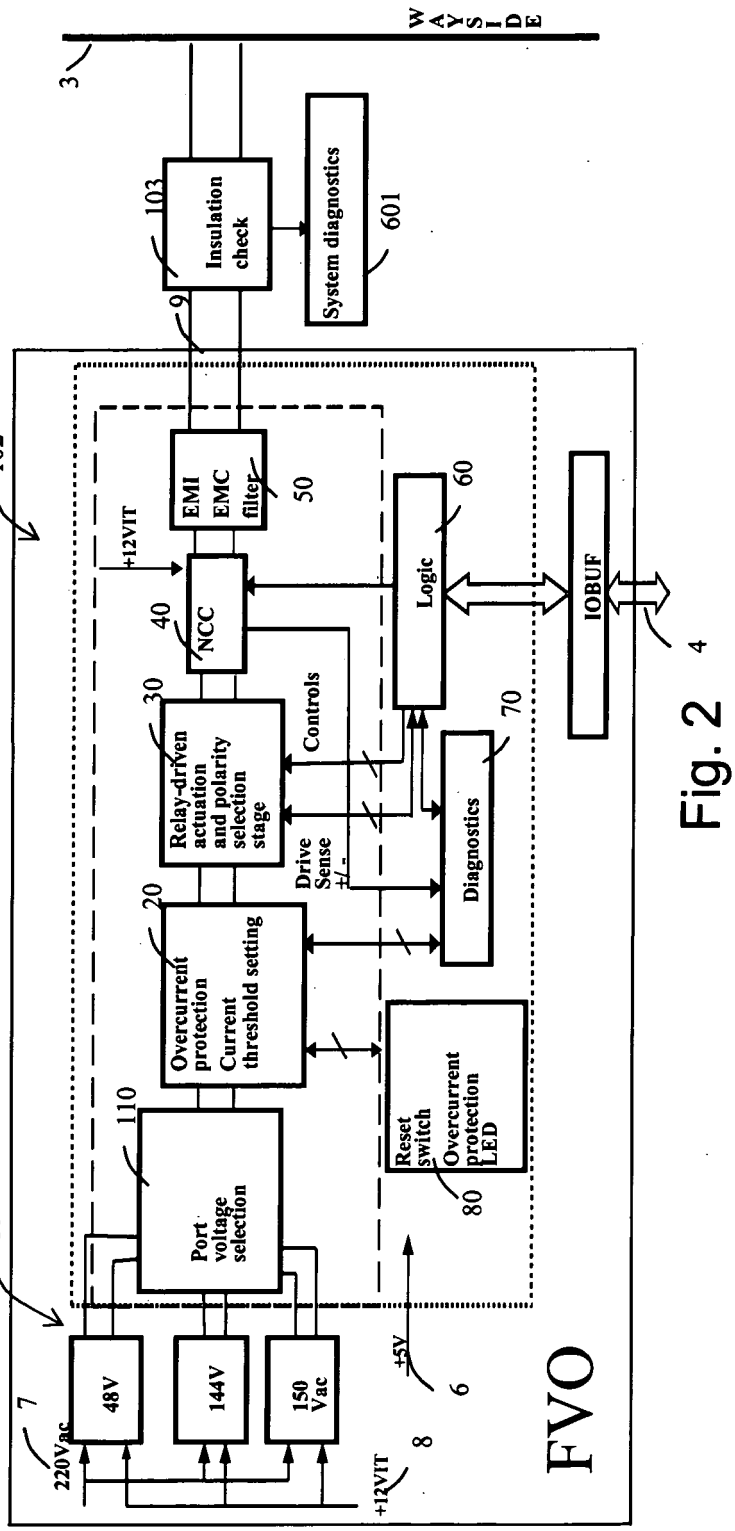
WAYSIDE
3
Insulation check
103
System diagnostics
601
9
102
EMI EMC filter
50
+12VIT
NCC
40
Logic
60
IOBUF
4
Relay-driven actuation and polarity selection stage
30
Controls
Drive Sense +/-
Diagnostics
70
Overcurrent protection Current threshold setting
20
Reset switch
Overcurrent protection LED
80
Port voltage selection
110
10
48V
144V
150 Vac
220Vac
7
+5V
6
+12VIT
8
FVO

Fig. 2

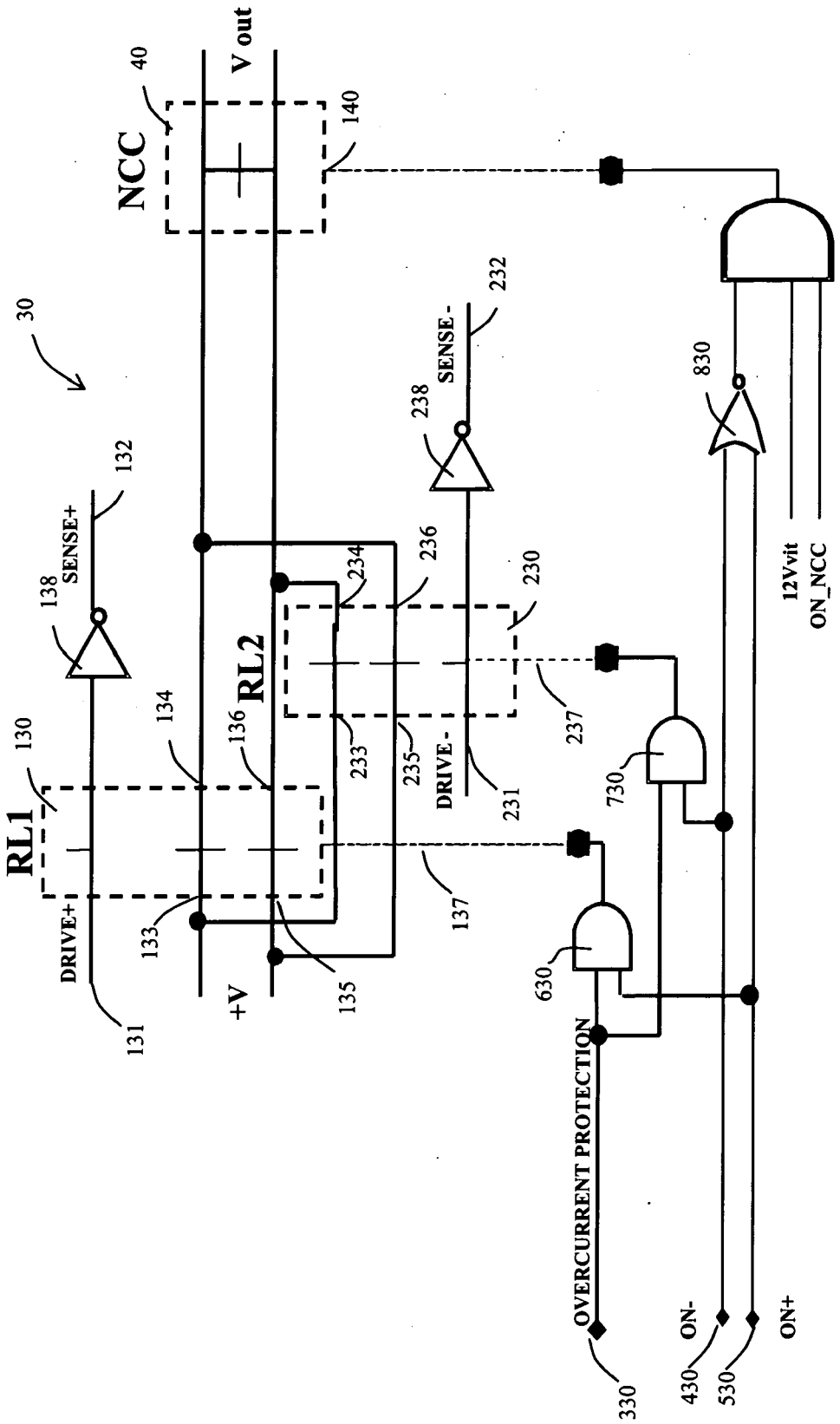
30
NCC
40
V out
140
SENSE+
132
138
SENSE-
232
238
830
12Vit
ON_NCC
RL1
130
RL2
134
136
234
236
230
233
235
237
DRIVE+
DRIVE-
231
730
133
135
137
+V
131
630
OVERCURRENT PROTECTION
330
ON-
430
ON+
530

Fig. 3

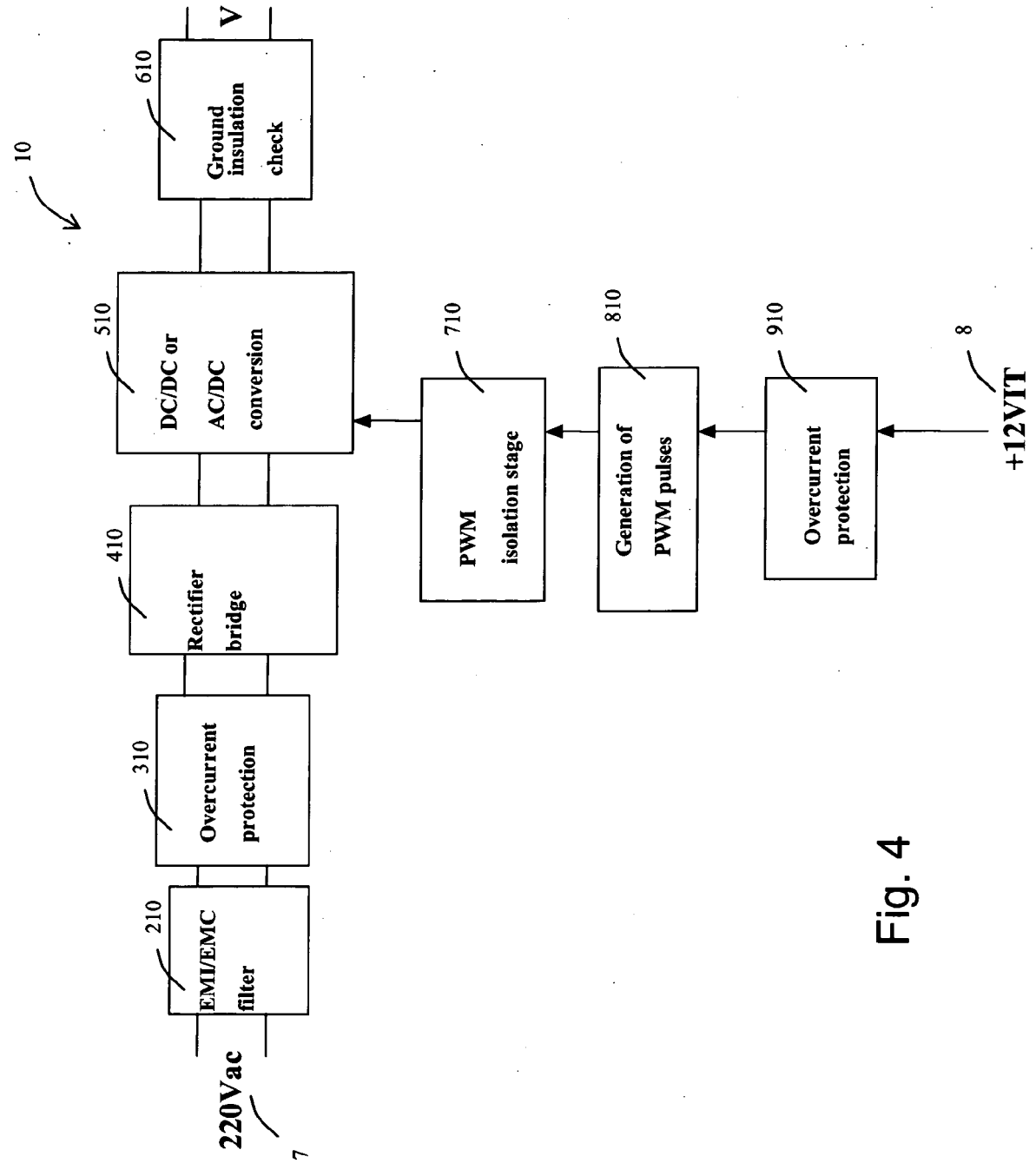
10
610
Ground insulation check
V
510
DC/DC or AC/DC conversion
410
Rectifier bridge
310
Overcurrent protection
210
EMI/EMC filter
220Vac
7
710
PWM isolation stage
810
Generation of PWM pulses
910
Overcurrent protection
8
+12VIT

Fig. 4

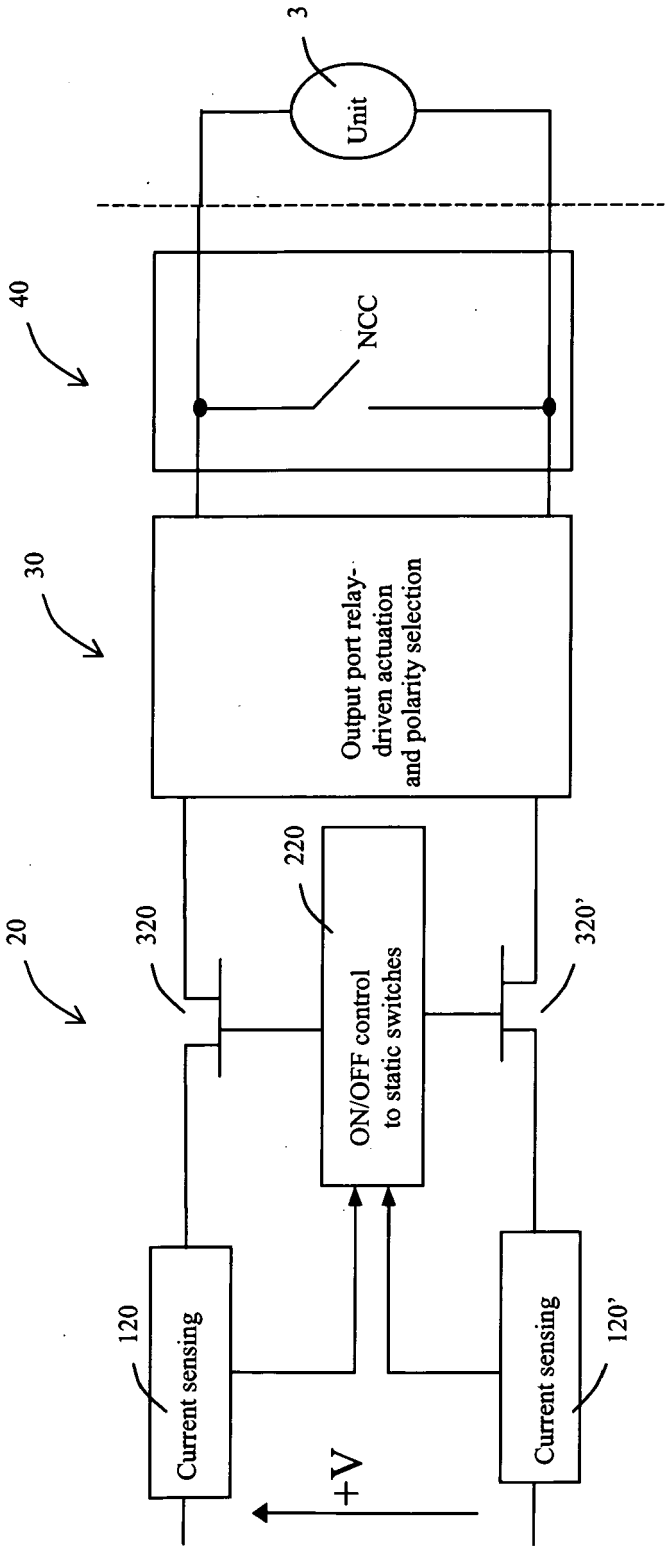
3
Unit
40
NCC
30
Output port relay-driven actuation and polarity selection
220
ON/OFF control to static switches
20
320
320'
120
Current sensing
120'
Current sensing
+V

Fig. 5A

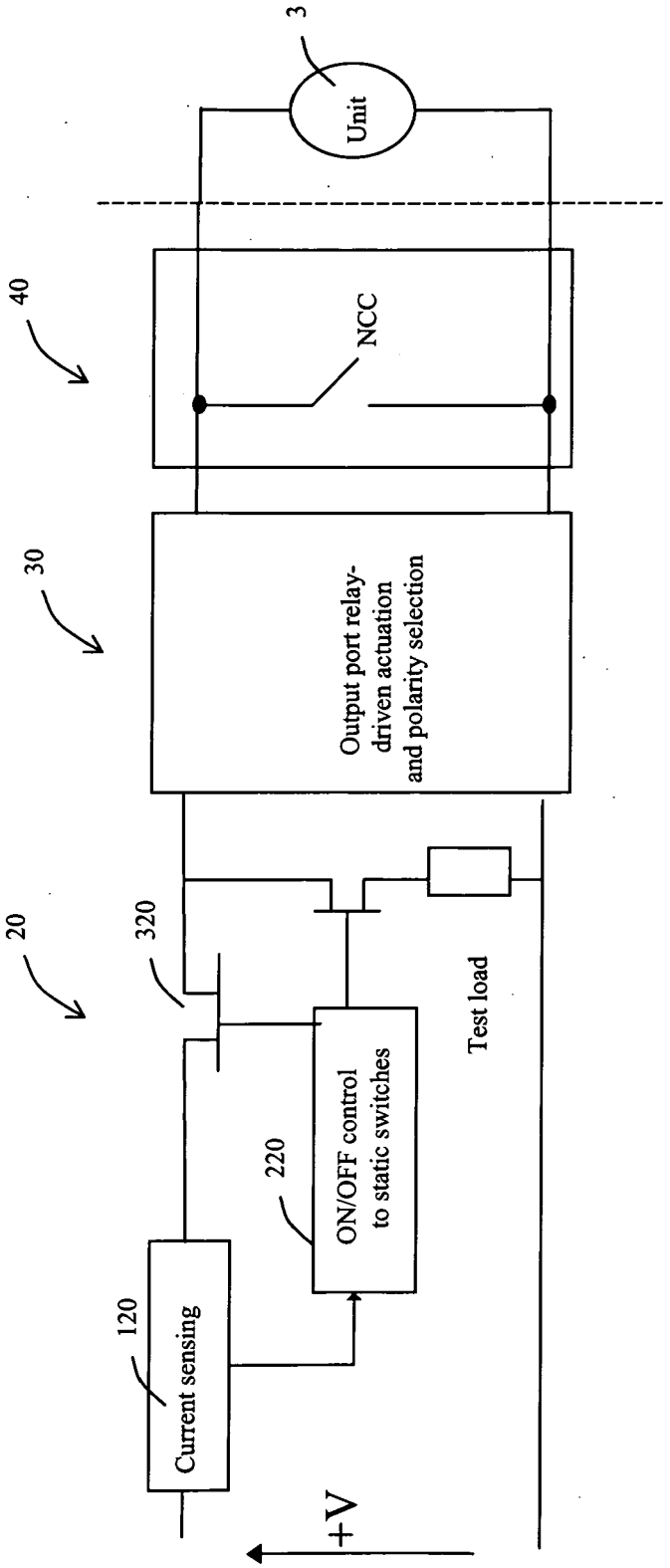
3
Unit
40
NCC
30
Output port relay-driven actuation and polarity selection
20
320
Test load
220
ON/OFF control to static switches
120
Current sensing
+V

Fig. 5B

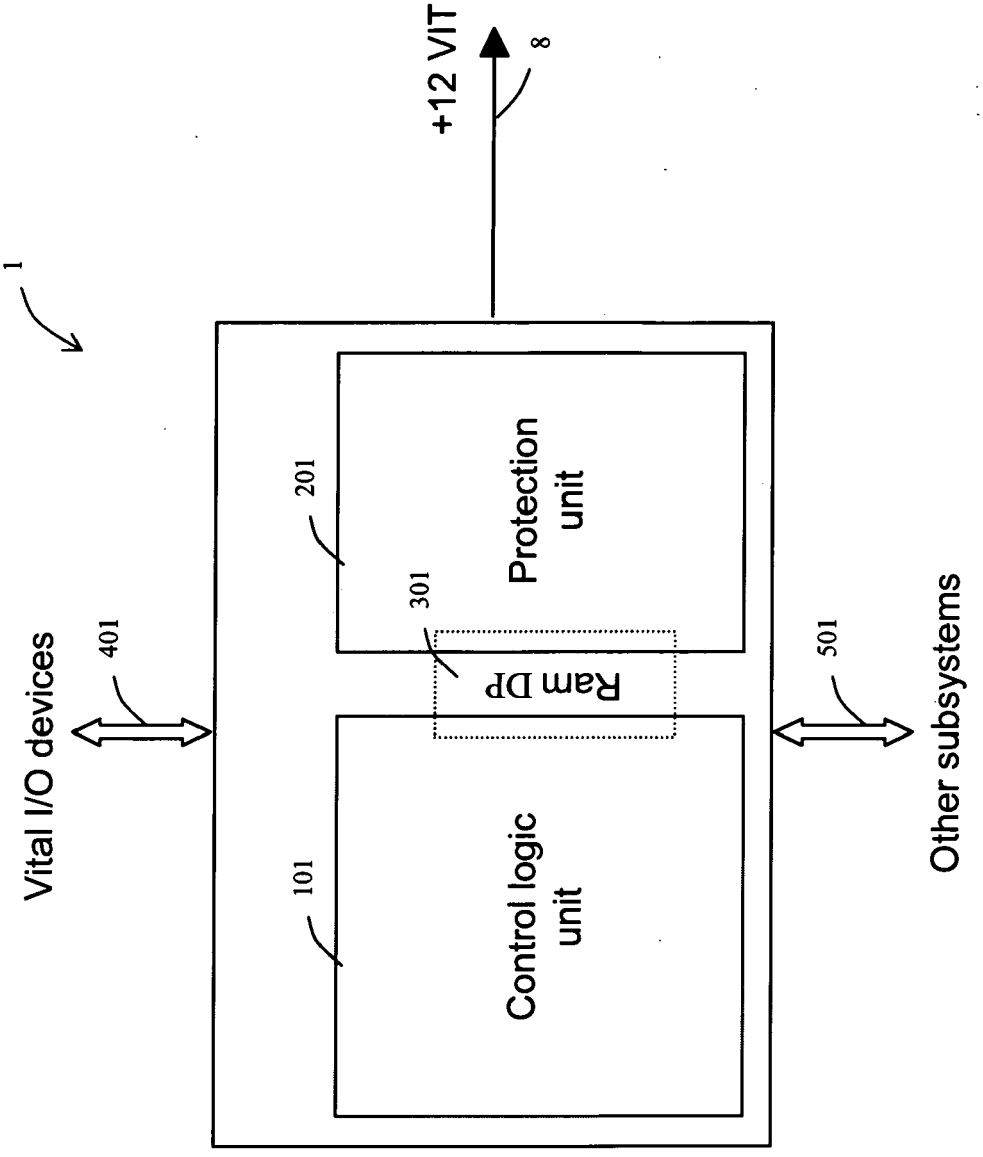
+12 VIT
8
1
201
Protection unit
301
Ram DP
401
Vital I/O devices
501
Other subsystems
101
Control logic unit

Fig. 6

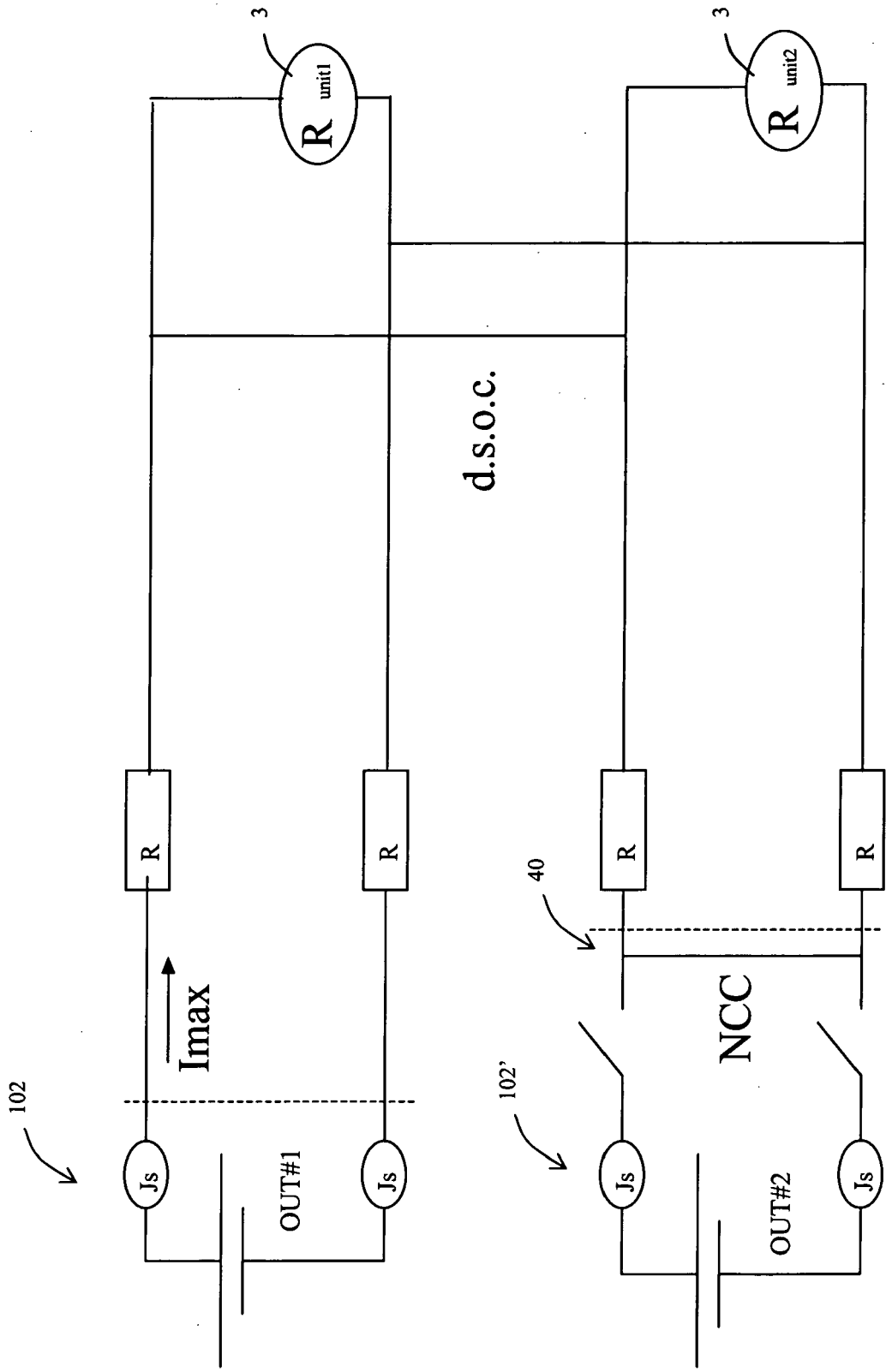
3
R unit1
3
R unit2
d.s.o.c.
R
R
R
R
40
Imax
NCC
102
102'
Js
Js
Js
Js
OUT#1
OUT#2

Fig. 7

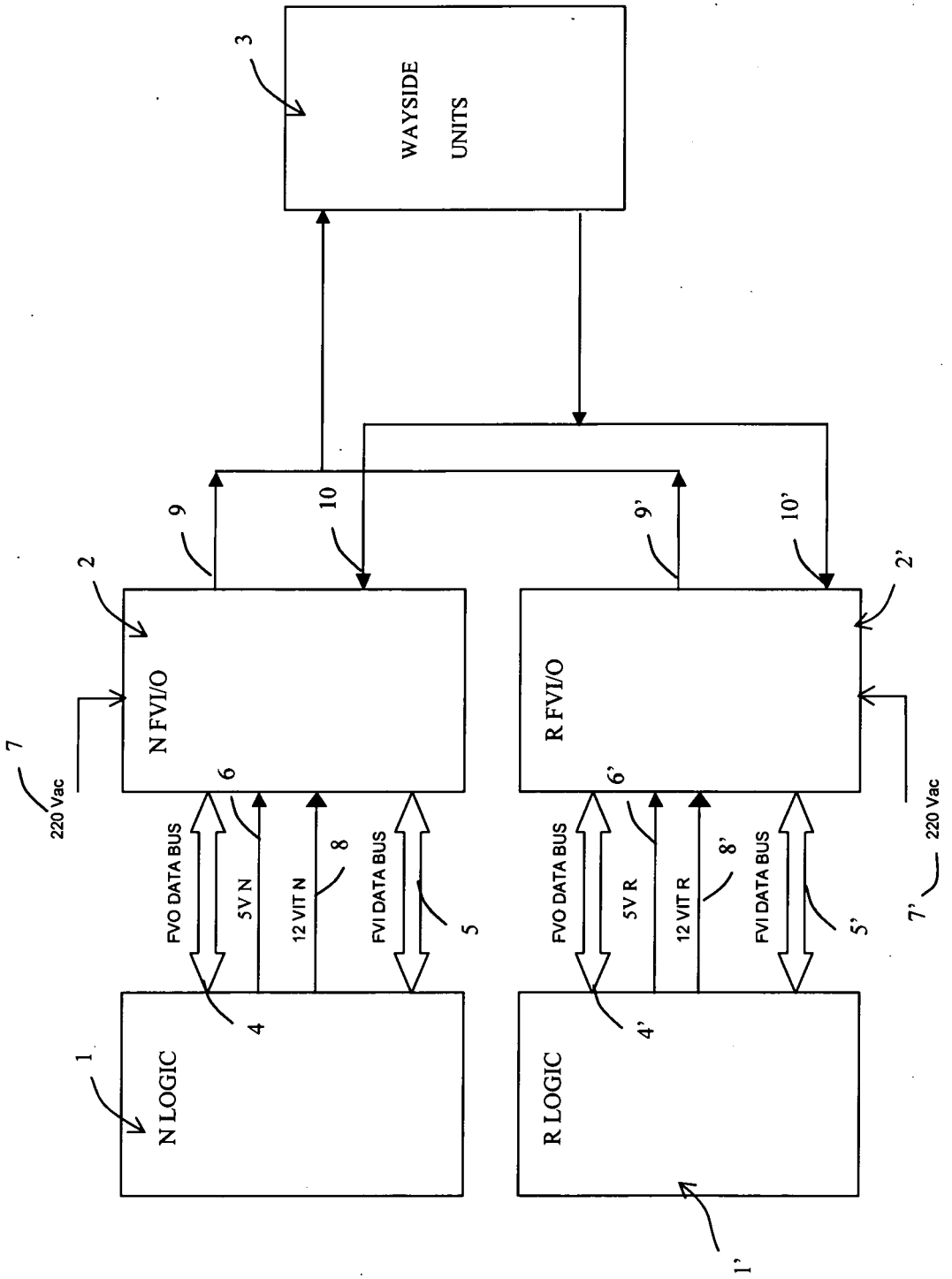
3
WAYSIDE UNITS
9
10
9'
10'
2
2'
N FVI/O
R FVI/O
7
220 Vac
6
6'
FVO DATA BUS
5V N
12 VIT N
8
FVI DATA BUS
5
FVO DATA BUS
5V R
12 VIT R
8'
FVI DATA BUS
5'
7'
220 Vac
4
4'
1
N LOGIC
R LOGIC
1'

Fig. 8

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 07 42 5064

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	US 6 463 337 B1 (WALKER JIM E [US]) 8 October 2002 (2002-10-08) * column 3, line 8 - column 4, line 9 * * figure 1 *	1-39	INV. B61L7/08
A	EP 1 524 167 A (SIEMENS SCHWEIZ AG [CH]) 20 April 2005 (2005-04-20) * paragraphs [0008] - [0011] * * paragraphs [0015] - [0019] * * figure 2 *	1,29,36	
A	EP 1 594 101 A (SIEMENS SCHWEIZ AG [CH]) 9 November 2005 (2005-11-09) * paragraphs [0011], [0023] * * figure 1.2 *	1,29,36	
A	DE 198 36 079 A1 (SIEMENS AG [DE]) 10 February 2000 (2000-02-10) * column 1, line 3 - column 1, line 14 * * column 2, line 44 - column 2, line 58 * * column 3, line 42 - column 4, line 46 * * figure 1 *	1,29,36	TECHNICAL FIELDS SEARCHED (IPC) B61L
A	US 5 922 034 A (FEELY BENNETT R [US]) 13 July 1999 (1999-07-13) * column 4, line 35 - column 6, line 60 * * figures 2-5 *	1,29,36	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	23 July 2007	Massalski, Matthias

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 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 07 42 5064

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

23-07-2007

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6463337 B1	08-10-2002	NONE	
EP 1524167 A	20-04-2005	NONE	
EP 1594101 A	09-11-2005	NONE	
DE 19836079 A1	10-02-2000	AT 410987 B	25-09-2003
		AT 127999 A	15-01-2003
		CN 1243974 A	09-02-2000
		HK 1024310 A1	11-06-2004
		ZA 9904845 A	31-01-2000
US 5922034 A	13-07-1999	US 6259978 B1	10-07-2001

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- WO 03093999 A **[0044]**