

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
11 January 2007 (11.01.2007)

PCT

(10) International Publication Number  
**WO 2007/005629 A2**

(51) International Patent Classification: Not classified

(21) International Application Number:  
PCT/US2006/025627

(22) International Filing Date: 29 June 2006 (29.06.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
60/695,829 30 June 2005 (30.06.2005) US

(71) Applicant (for all designated States except US): **BALLARD POWER SYSTEMS CORPORATION** [US/US]; 15001 Commerce Drive North, Dearborn, Michigan 48120 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **SOUDIER, Christophe** [FR/US]; 9538 Glenhill Dr., Ypsilanti, Michigan 48198 (US). **CHENG, Bing** [US/US]; 5073 Forestdale Dr., West Bloomfield, Michigan 48322 (US).

**KOWALEC, Steven, J.** [US/US]; 16460 Homer, Plymouth, Michigan 48170 (US). **NALLAPA, Venkatapathi, R.** [US/US]; 7006 Carlyle Crossing, West Bloomfield, Michigan 48322 (US). **HAMPO, Richard, J.** [US/US]; 13745 Embers Court, Plymouth, Michigan 48170 (US).

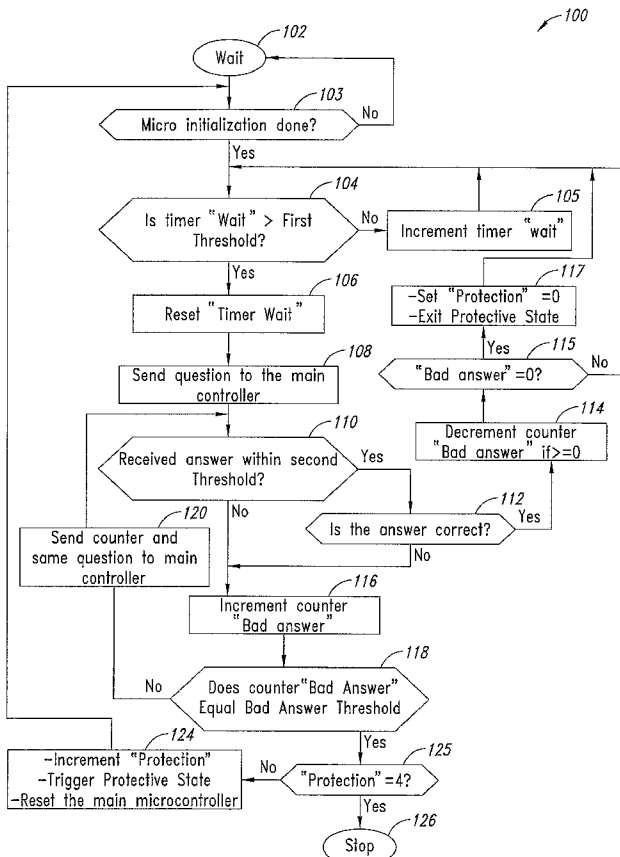
(74) Agents: **ABRAMONTE, Frank** et al.; Seed Intellectual Property Law Group PLLC, Suite 6300, 701 Fifth Avenue, Seattle, Washington 98104-7092 (US).

(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, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, 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, RS, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Continued on next page]

(54) Title: CONTROLLER METHOD, APPARATUS AND ARTICLE SUITABLE FOR ELECTRIC DRIVE



(57) Abstract: A control system, method and article allows a monitoring module to monitor operation of a main controller in an electric drive, by providing questions and evaluating the accuracy and/or timeliness of responses from the main controller. Upon detection of an excessive number of incorrect or late responses, the monitoring module can shutdown operation, and may provide an alternative communications path, thereby preventing corrupt data from reaching a vehicle network, while providing communications for diagnostic and recovery such as by provision of new software or firmware instructions. The main controller may monitor the operation of the monitoring module, taking appropriate action if a fault is detected. Disabling a supply of power to a traction motor may be based on current operating conditions, such as speed.

WO 2007/005629 A2



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).

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

**Published:**

- *without international search report and to be republished upon receipt of that report*

## CONTROLLER METHOD, APPARATUS AND ARTICLE SUITABLE FOR ELECTRIC DRIVE

### CROSS-REFERENCE TO RELATED APPLICATION

This application claims the benefit under 35 U.S.C. § 119(e) of  
5 U.S. Provisional Patent Application No. 60/695,829, filed June 30, 2005.

### BACKGROUND OF THE INVENTION

#### Field of the Invention

This disclosure generally relates to electrical power systems, and  
more particularly to a controller for controlling operation of electric drives, for  
10 example electric drives associated with electric and/or hybrid vehicles.

#### Description of the Related Art

Power conversion systems transform and/or condition power from  
one or more power sources for supplying power to one or more loads. A power  
conversion system component commonly referred to as an "inverter" transforms  
15 direct current (DC) to alternating current (AC) for use in supplying power to an  
AC load. A power conversion system component commonly referred to as a  
"rectifier" transforms AC to DC. A power conversion system component  
commonly referred to as a "DC/DC converter" steps-up or steps-down DC  
voltage. In some embodiments, these components may be bi-directionally  
20 operable to perform two or more functions. These functions may, in some  
cases be inverse functions. For example, a switch mode inverter may be  
operable to invert DC to AC in one direction, while also operable to rectify AC to  
DC in another direction. An appropriately configured and operated power  
conversion system may include any one or more of these components to  
25 perform any one or more of these functions.

In common usage, the term "converter" applies generically to all  
power conversion components whether inverters, rectifiers and/or DC/DC

converters and is used herein and in the claims in that generic sense. Power converters typically employ power semiconductor devices, such as insulated gate bipolar transistors (IGBTs), metal oxide semiconductor field effect transistors (MOSFETs), and/or semiconductor diodes. One or more power  
5 conversion system components may be provided as a self-contained unit, commonly referred to as a power module, which comprises an electrically insulative housing that houses at least a portion of the power conversion system component, and appropriate connectors such as phase terminals or bus bars.

10 Many applications employ the delivery of high power, high current and/or high voltage from a power source to a load. For example, it may be desirable in transportation applications to provide a relatively high DC voltage to an inverter to supply AC power for driving a load such as a traction motor for propelling an electric or hybrid electric vehicle. It may also be desirable at the  
15 same time to provide relatively low voltage AC or DC power for driving accessory or peripheral loads. Such applications may employ one or more of a variety of power sources. Applications may, for example, employ energy producing power sources such as internal combustion engines or arrays of fuel cells and/or photovoltaic cells. Applications may additionally, or alternatively,  
20 employ power sources such as energy storage devices, for example, arrays of battery cells, super- or ultra-capacitors, and/or flywheels. Often, such applications employ a power converter to transform and/or condition the power, for example, stepping down the voltage at which the power is supplied to the load.

25 Operation of electric drives, particular those employing permanent magnet motors must address a number of issues not presented by other types of drives, such as drives employing internal combustion engines. Additionally, it may be desirable to provide some limited ability to continue operating an electric drive after a fault has occurred. Such capability may be referred to as  
30 "limp home" capability, which may, for example, allow operation of the electric drive at reduced power for a time sufficient to move a vehicle to a point of

safety. Addressing such problems may be commercially beneficial to the acceptance of electric and/or hybrid vehicles. Thus, new approaches to accurately detect, handle and/or remedy fault conditions in electric drives are desirable.

## 5 BRIEF SUMMARY OF THE INVENTION

In at least one embodiment, a control system and method or article provides a main controller to control operation of an electric drive such as an electric drive for a vehicle, and an independent monitoring module that monitors the operation of the main controller. The monitoring module, for  
10 example monitoring logic configured in a field programmable gate array or the like, may from time-to-time provide questions or queries to the main controller. The monitoring logic verifies the accuracy and/or timeliness of responses by the main controller to the questions or queries, and maintains one or more counters reflecting such.

15 In at least one embodiment, a control system and method or article provides a main controller to control operation of an electric drive such as an electric drive for a vehicle, and an independent monitoring module that monitors the operation of the main controller. The monitoring module, for  
20 example monitoring logic configured in a field programmable gate array or the like, may from time-to-time provide questions or queries to the main controller. The monitoring logic verifies the accuracy and/or timeliness of responses by the main controller to the questions or queries, and maintains one or more counters reflecting such. Additionally, the main controller monitors the operation of the monitoring logic. From time-to-time, the main controller provides an  
25 intentionally incorrect answer to a question or query from the monitoring logic. The main controller also verifies the timeliness of questions or queries from the monitoring module, and maintains one or more counters reflecting such.

30 In at least one embodiment, a control system and method or article provides the ability to load new instructions and/or perform diagnostics and analysis after a shutdown occurs in response to detection of a fault

condition. The control system and method or article may disable a regular communications path between a vehicle and a main controller such as a microprocessor to prevent the communications of corrupted data. The control system and method or article may provide an alternative communications path  
5 allowing diagnostics, analysis and the reconfiguring of instructions, for example, via loading of new software and/or firmware instructions. Such may allow the resetting of the main controller after appropriate troubleshooting and corrective action.

In at least one embodiment, a control system and method or  
10 article employs fault and monitoring logic to determine an appropriate way to disable an electric drive in response to a fault condition. The control system and method or article may determine the appropriate response based on a speed, for example an angular velocity, of a traction motor controlled by the control system. The control system and method or article may disable a gate  
15 drive placing all power semiconductor switches in a DC/AC converter supplying power to the traction motor in an open, non-conducting state, for example where the speed is below a speed threshold. The control system and method or article may disable a gate drive placing some of the power semiconductor switches in an open, non-conducting state, and other of the power  
20 semiconductor switches in a closed, conducting state to electrically short the traction motor, for example where the speed is above a speed threshold.

#### BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S)

In the drawings, identical reference numbers identify similar elements or acts. The sizes and relative positions of elements in the drawings  
25 are not necessarily drawn to scale. For example, the shapes of various elements and angles are not drawn to scale, and some of these elements are arbitrarily enlarged and positioned to improve drawing legibility. Further, the particular shapes of the elements as drawn, are not intended to convey any information regarding the actual shape of the particular elements, and have  
30 been solely selected for ease of recognition in the drawings.

Figures 1A-1C are a functional block diagram of a portion of an electric drive system employing a microprocessor as a main controller and a field programmable gate array implementing monitoring logic to monitor the main controller, according to one illustrated embodiment.

5           Figure 2 is a flow diagram showing a method of operating a monitoring module such as the monitoring logic of the field programmable gate array to monitor the operation of a main controller such as the microprocessor, according to one illustrated embodiment.

10           Figure 3 is a flow diagram showing a method of operating the main controller to monitor the operation of a monitoring module such as the field programmable gate array, according to one illustrated embodiment.

Figure 4A is a schematic diagram showing a switch mechanism operable to switch CAN ports of a main controller between two CAN channels via a pair of CAN transceivers, according to one illustrated embodiment.

15           Figure 4B is a logic diagram for implementing the switch mechanism of Figure 4A with respect to transmit lines or ports of the CAN transceivers, according to one illustrated embodiment.

20           Figure 4C is a logic diagram for implementing the switch mechanism of Figure 4A with respect to receive lines or ports of the CAN transceivers, according to one illustrated embodiment.

## DETAILED DESCRIPTION OF THE INVENTION

In the following description, certain specific details are set forth in order to provide a thorough understanding of various embodiments. However, one skilled in the art will understand that the invention may be practiced without these details. In other instances, well-known structures associated with power converters, controllers and/or gate drives have not been shown or described in detail to avoid unnecessarily obscuring descriptions of the embodiments.

Unless the context requires otherwise, throughout the specification and claims which follow, the word "comprise" and variations

thereof, such as, "comprises" and "comprising" are to be construed in an open sense, that is as "including, but not limited to."

Reference throughout this specification to "one embodiment" or "an embodiment" means that a particular feature, structure or characteristic  
5 described in connection with the embodiment is included in at least one embodiment. Thus, the appearances of the phrases "in one embodiment" or "in an embodiment" in various places throughout this specification are not necessarily all referring to the same embodiment. Further more, the particular features, structures, or characteristics may be combined in any suitable manner  
10 in one or more embodiments.

The headings provided herein are for convenience only and do not interpret the scope or meaning of the claimed invention.

Figures 1A-1C show a portion of an electric drive system 10 according to one illustrated embodiment.

15 The electric drive system 10 may include, or may be coupled to drive, various components of an electric or hybrid electric vehicle, for example, a permanent magnet traction motor 12. The electric drive system 10 may comprise a control subsystem 14 and one or more power converters, for example a DC/DC power converter 16 and/or DC/AC power converter 18,  
20 operable to modify, transform and/or otherwise transfer electrical power between one or more power sources (not shown) and one or more loads. The power sources may, for example, take the form of one or more energy producing power sources such as internal combustion engines or arrays of fuel cells or photovoltaic cells, and/or may take the form of one or more energy  
25 storage power sources such as arrays of chemical battery cells and/or super- or ultra-capacitors. The loads may, for example, take the form of one or more power supplies, compressors, fans, pumps and/or a traction motor, such as the permanent magnet traction motor 12. While typically identified as a load, in  
30 some embodiments the traction motor 12 may at times function as a power source, for example when operating in a regenerative braking mode.



The DC/DC power converter 16 may be operable to step-up and/or step-down a DC voltage. The DC/AC power converter 18 may be operable to invert DC power to AC power, for example, to drive the traction motor 12. In some embodiments, the DC/AC power converter 18 may also be operable to rectify AC power to DC power, for example, to recharge a battery using power generated by the traction motor 12 during regenerative braking. Each of the power converters 16, 18 generally comprises a number of power semiconductor switches and a number of power semiconductor diodes electrically coupled in anti-parallel across respective ones of the power semiconductor switches, arranged to form at least a portion of a bridge circuit. The power semiconductor switches, may, for example, take the form of metal oxide semiconductor field effect transistors (MOSFETs), insulated gate bipolar transistors (IGBTs) and/or other switches suitable for high power operation. In some embodiments, the power semiconductor diodes may be formed as part of the power semiconductor switches, for example as body diodes, while in other embodiments the power semiconductor diodes may take the form of discrete semiconductor devices.

The control subsystem 14 may comprise one or more microprocessors 20 and one or more updatable components, such as one or more field programmable gate arrays (FPGA) 22, or random access memory (RAM) or read only memory (ROM). The FPGA 22 is physically independent from the microprocessor 20, and communicates therewith via an appropriate interface. The control subsystem 14 may also include a resolver-to-digital (R/D) converter 24 and/or DC/DC pulse width modulation (PWM) controller 26. The control subsystem 14 may further include dedicated output signal processor 28 and digital input signal processor 29, both communicatively coupled to the DC/AC power converter 18 via a gate drive board 30. The control subsystem 14 may further include a communications subsystem 31, as well as a power supply 32 and signal processor 34 communicatively coupled to supply wake up signals 27 to the power supply 32, and analog and digital signals 33 to the microprocessor 20.

The microprocessor 20 is operable to execute instructions which may be stored in a memory such as a read only memory (ROM) and/or random access memory (RAM) (not shown), to produce a variety of outputs based on a variety of inputs in order to control operation of the electric drive system 10 in conjunction with the FPGA 22. For example, the microprocessor 20 may receive a clock signal from an off-chip clock 35, or an on-chip clock. Also for example, with respect to operation of the DC/DC power converter 16, the microprocessor 20 may receive DC/DC fault on data bus signals on data bus line 36, and may provide PWM signals on PWM for DC/DC Vref (reference voltage) line 37 and enable DC/DC signals on an enable DC/DC line 38. With respect to operation of the DC/AC power converter 18, the microprocessor 20 may receive gate drive (GD) fault signals indicative of a fault on a gate drive board via a GD fault data bus line 39, and backup power feedback signals on a backup power feedback line 40. The microprocessor 20 may provide emergency power off (EPO) type signals on an EPO type line 41, DC/AC converter reset signals on an Inverter Reset line 42, enable signals for the DC/AC power converter 18 on Inverter Enable line 43, protection type signals on Protection Type line 44, PWM clock signals on PWM Clock line 45, and PWM signals on PWM signals line 46, as well as signals commanding backup power command via a backup power command line 47.

The FPGA 22 is configurable to implement a number of functions to produce a variety of outputs based on a variety of inputs in order to control operation of the electric drive system 10 in conjunction with the microprocessor 20. The functions include monitoring logic 50, gate signal generation 52, and DC/DC function 54. The FPGA 22 is reprogrammed via flash 56, and may receive a clock signal 58 from an on-chip or off-chip clock. The logic is programmed into the FPGA 22, and may be reprogrammed as necessary or desirable. Certain portions of the FPGA 22, for example the monitoring logic 50, may be protected or isolated from reprogramming of other portions of the FPGA 22. The programming for the FPGA 22 may be via a dedicated interface port.

The monitoring logic 50 receives a variety of inputs and produces a variety of outputs in implementing monitoring of the operation of the microprocessor 20. For example, as explained in more detail below, the monitoring logic 50 may exchange questions and answers 60 with the  
5 microprocessor 20. The monitoring logic may also receive direction signals via a direction line 61 and speed signals via a North Mark line 62 from the R/D converter 24. The R/D converter 24 operates to provide digitized signals indicative of angular position of the permanent magnet traction motor 12. The monitoring logic 50 may also receive a download or power-up check signals via  
10 a download or power-up check line 63 from the microprocessor 20. The monitoring logic 50 is capable of providing a reset signal to a reset pin of the microprocessor 20 via a reset line 64, as well as a disable drive and CAN2 signal to the gate signal generation function 52 and communications subsystem  
31 via a Disable Drive and CAN2 line 65. In one embodiment the  
15 microprocessor 20 cannot modify or stop the operation of the monitoring logic 50.

The gate signal generation function 52 receives a variety of inputs and produces a variety of outputs in implementing control of the DC/AC power converter 18, including the production of power and the handling of faults. For  
20 example, the gate signal generation function 52 receives signals via lines 41-47 from the microprocessor 20. Additionally, the gate signal generation function 52 receives the backup power feed back on line 40 from the gate drive board 30 via the digital input signal processor 29. The gate signal generation function 52 also receives over voltage fault signals via HV OV faults line 66 and  
25 desaturation fault signals via desat faults line 67 which are indicative of a problem with one of the power transistors, from the gate drive board 30 via the digital input signal processor 29. The gate signal generation function 52 provides gate signals via gate signal line 68 (e.g., six gate signals) and a DC/AC reset signal via inverter reset line 69 to the gate drive board 30 via a  
30 digital output signal processor 28a of the output signal processor 28. Additionally, the gate signal generation function 52 may receive an emergency

power off (EPO) signal via an EPO line 70 and exchange an interlock signal on interlock line 71 with a vehicle control system via a vehicle harness 72.

The DC/DC function 54 receives a variety of inputs and produces a variety of outputs in implementing control of the DC/DC power converter 16 in conjunction with the DC/DC PWM controller 26 and a DC/DC driver 28b of the output signal processor 28. For example, the DC/DC function 54 may receive the PWM for DC/DC reference voltage signals via the PWM for DC/DC Vref line 37 and the enable DC/DC signal via the Enable DC/DC line 38 from the microprocessor 20. The DC/DC function 54 may also, for example, receive faults signals via faults line 73 and high voltage PWM signals from the DC/DC PWM controller 26 via HV PWM line 74. The DC/DC function 54 may provide PWM drive signals (e.g., four high voltage PWM and two low voltage PWM signals) to the DC/DC driver 28b of the output signal processor 28 via HV PWM and LV PWM lines 75 for driving the DC/DC power converter 16. The DC/DC function 54 may also provide the DC/DC faults signals via a DC/DC fault on data bus line 36 to the microprocessor 20, and may provide enable signals via an Enable line 76 and voltage reference signals via a Vref line 77 to the DC/DC PWM controller 26.

The DC/DC PWM controller 26 is operable to provide PWM drive signals to the DC/DC driver 28b via the DC/DC function 54 of the FPGA 22. In addition to above discussed signals received and provided by the DC/DC PWM controller 26, the DC/DC PWM controller 26 may receive temperature, voltage and current signals on one or more lines (collectively) 79 and may also provide analog signals on an analog signal line 81 to the signal processor 34 for use in operating the power supply 32.

The communications subsystem 31 provides communications between the microprocessor 20 and other elements of the vehicle as well as with programming, testing and/or diagnostic equipment via a first controller area network (CAN) channel 78a and a second CAN channel 78b. The second CAN channel 78b is for normal vehicle communications while the first CAN channel 78a is reserved for program download and/or diagnostics. The two CAN

channels 78a, 78b will not work at the same time over the vehicle CAN bus. Rather, the second CAN channel 78b may be disabled by the monitoring logic 50 of the FPGA 22 in response to a detection or determination of the existence of a fault condition, and the first CAN channel 78a made functional for  
5 downloading programs and/or diagnostics.

To implement such, the communications subsystem 31 comprises a first CAN transceiver 80a and second CAN transceiver 80b and switch mechanism 82 operable to selectively switch CAN ports 84a, 84b of the microprocessor 20 between the CAN channels 78a, 78b. The switch  
10 mechanism 82 may comprise a first switch 82a, second switch 82b, and third switch 82c. The first switch 82a is selectively operable to provide and to remove a communications path between the first CAN transceiver 80a and the first CAN port 84a. The second switch 82b is selectively operable to provide and to remove a communications path between the second CAN transceiver  
15 80b and the second CAN port 84b. The third switch 82c is selectively operable to provide and to remove a communications path between the second CAN transceiver 80b and the first CAN port 84a. The switch mechanism 82 may be responsive to the disable drive and CAN 2 signal provided by the monitoring logic 50 of the FPGA 22 via the Disable Drive and CAN2 line 65, as described  
20 in more detail below with reference to Figures 4A-4C.

In the case of a failure of the microprocessor 20, the monitoring logic 50 of the FPGA 22 may enter a protective state. The monitoring logic 50 may also issue a reset signal to the microprocessor 20. After a set number of attempts (*e.g.*, five) by the monitoring logic 50 to reset the microprocessor 20,  
25 the monitoring logic 50 may maintain the microprocessor 20 in a persistent shutdown state if the microprocessor 20 still exhibits a fault, for example, by providing incorrect answers to questions or queries by the monitoring logic 50. The microprocessor 20 remains in the persistent shutdown state until a new power cycle occurs. Such monitoring of the operation of the microprocessor  
30 20, as well as monitoring of the operation of the monitoring logic 50 is explained more fully below with reference to Figures 2 and 3.

The protective state may include removing a communications path between the second CAN port 84b and the second CAN transceiver 80b, without regard to the outputs of the microprocessor 20, to prevent possibly corrupted data from being transmitted. The protective state may additionally  
5 include removing a communications path between the first CAN port 84a and the first CAN transceiver 80a. The protective state may additionally include providing a communications path between the first CAN port 84a and the second CAN transceiver 80b to provide communications for diagnostic and recovery such as by provision of new software or firmware instructions. The  
10 protective state may additionally disable one or more of the power converters 16, 18. The protective state may additionally disable the gate drive board 30.

In the protective state, the state of the power semiconductor switches in the DC/AC power converter 18 are dependent on the speed and a fault history. If the speed is below a speed threshold, then all of the power  
15 semiconductor switches will be placed in an open (*i.e.*, non-conducting) state. If the speed is above the speed threshold, some of the power semiconductor switches are placed into the closed (*i.e.* conducting) state and some in the open (*i.e.* non-conducting) state to electrically short the traction motor 12. For example, where the DC/AC power converter 18 includes three pairs of power  
20 semiconductor switches (*i.e.*, upper and lower power semiconductor switches for each of three phases A, B, C), the three upper or the three lower power semiconductor switches will be closed (*i.e.*, conducting) depending on the fault history (for example, if a fault was previously detected in one of the three upper semiconductor switches, then the three lower semiconductor switches will be  
25 closed). The speed may be read continuously, and therefore the state may change continuously even if the monitoring is in the persistent shutdown state awaiting a power cycle.

The communications subsystem 31 may further comprise an RS232 port driver 86 to provide serial communications between the  
30 microprocessor 20, FPGA 22 and an interface 88 suitable for running diagnostics and reconfiguring the software and/or firmware with new

instructions. In particular, the RS232 port may transfer a boot strap download of new instructions or programming from the interface 88 to the microprocessor 20 and/or FPGA 22 via a bootstrap download line 89a, 89b. The RS232 port may provide a communications path 90a, 90b between the microprocessor 20 and an interface 88 useful in performing software development. The RS232 port may further provide wake up signals 91 to the power supply 32.

The electric drive system 10 employs three levels of monitoring. A first or functional level includes monitoring motor management functions, for example converting requested motor torque, component monitoring, input/output variable diagnosis, and controlling reactions of the electric drive system 10 when an error or fault is detected. A second or function monitoring level includes detecting a defective sequence of the level 1 functional software, for example by monitoring the calculated torque values, and triggering specific reactions of the electric drive system 10 if a fault or error is detected. A third or controller monitoring level includes a monitoring module (*i.e.*, monitoring logic 50 of FPGA 22) that is independent of the main controller (*i.e.*, microprocessor 20), which tests that the main controller is operating correctly. As explained in detail below, this may include a question and answer process. The monitoring module may trigger or cause specific reactions by the electric drive system 10 independent of the main controller when an error or fault is detected.

As an overview, the monitoring logic 50 provides questions or queries to the main controller from time-to-time (*e.g.*, one every 40ms). The questions may be randomly selected from a set of defined questions. To reduce communications overhead, the questions may be stored in, or at the microprocessor 20, with the monitoring logic simply providing a pointer to the appropriate question or questions. The monitoring logic 50 expects to receive an answer within a defined period. For example, where the main controller processes the monitoring function queries every 10ms, an answer is expected within approximately 15ms after the question is provided. A received response may take the form of a correct answer, an incorrect answer, or an answer at a wrong time. An answer received within a defined interval (*e.g.*, between 15ms

and 40ms) is classified as an answer at the wrong time, and the monitoring logic 50 may treat such in a similar fashion as wrong answers.

When a correct answer is received, the monitoring logic 50 decrements a wrong answer counter if such counter is greater than zero, and provides the next question at the next interval. When a received answer is either wrong or an answer at a wrong time, or where no answer is received in a defined period of time (e.g., 15ms), the monitoring logic 50 increments the wrong answer counter. The monitoring logic 50 then provides the same question again to the microprocessor 20, which may occur also immediately rather than waiting for a next defined interval, if defined intervals are employed.

If additional incorrect answers or answers at a wrong time are received, the wrong answer counter is incremented until the wrong answer counter equals or exceeds a defined value (e.g., 3) at which point the monitoring logic 50 enters a protective state (described above), as well as provides a reset signal to the microprocessor 20 via reset line 64 (Figure 1B).

If the microprocessor 20 persists in sending incorrect answers after a threshold number of reset attempts (e.g., 3), the monitoring logic stops trying to reset the microprocessor 20, and remains in a persistent shutdown state until a power cycle occurs. The protective state is active while in the persistent shutdown state.

Figure 2 shows a method 100 of monitoring operation of the microprocessor 20 using the monitoring logic 50 of the FPGA 22, according to one illustrated embodiment. The method 100 involves providing questions or queries from time-to-time to the microprocessor 20 from the monitoring logic 50 of the FPGA 22, and evaluating the answers received from the microprocessor 20.

The monitoring logic executes a wait loop, waiting at 102, determining at 103 whether the microprocessor initialization has been performed, and determining at 104 whether a wait timer is greater than a threshold (e.g., 10ms). If the wait timer has not exceeded the threshold, the



wait timer is incremented at 105 and control returns to 104 to repeat the wait loop. Otherwise control passes to 106.

At 106, the monitor logic resets the wait timer. At 108, the monitoring logic 50 provides a question to the microprocessor 20. For example, 5 the monitoring logic 50 may provide a speed and torque, for example from a lookup table, to the microprocessor 20. As noted above, to reduce communications overhead the questions or queries may be stored at the microprocessor 20 and the monitoring logic provides a pointer to a randomly selected one of the stored questions or queries. At 110, the monitoring logic 50 10 determines whether an answer to the question is received from the microprocessor 20 within a threshold time (e.g., 15ms). At 112, the monitoring logic 50 determines whether the received answer is correct. For example, the microprocessor 20 may return a power value calculated based on the provided speed and torque values, and the monitoring logic 50 may compare the 15 returned power value to a correct power value for the previously provided speed and torque values.

If the monitoring logic 50 determines at 112 that the received answer is correct, the monitoring logic 50 decrements a bad answer counter at 114 if the bad answer counter is at least equal to zero. The monitoring logic 50 20 then determines whether the bad answer counter is equal to zero at 115. The monitoring logic 50 returns control directly to 104 if the bad answer counter is not equal to zero. Alternatively, if the bad answer counter is equal to zero, the monitoring logic 50 sets a protection flag to zero and exits the protective state at 117, if the protective state was active, before returning control to 104. If the 25 received answer is incorrect, the monitoring logic 50 increments the bad answer counter at 116 and passes control to 118.

At 118, the monitoring logic 50 determines if the bad answer counter exceeds a bad answer threshold (e.g., 3). If the bad answer counter does not exceed the threshold, the monitoring logic 50 sends the value of the 30 counter and the same question to the microprocessor 20 at 120, and returns control to 110. If the bad answer counter does exceed the bad answer

threshold, the monitoring logic 50 checks whether the protection counter value exceeds a threshold value (e.g., 4) at 125. If the protection counter does exceed the threshold, control is passed to 126 where the persistent shutdown state is triggered.. If the protection counter does not exceed the threshold, then  
5 control is passed to 124. At 124, the monitoring logic 50 increments the protection counter, triggers the protective state, and sends a reset signal to the microprocessor 20 before returning control to 103. As an overview, the microprocessor 20 not only answers questions or queries posed by the monitoring logic 50, but may also verify the operation of the monitoring logic 50.  
10 When a computed answer is sent back to the monitoring logic 50, a wrong answer counter is decremented if the wrong answer counter is greater than one (1) or maintained if the wrong answer counter is equal to zero (0). From time-to-time (e.g., after every 5 computed answers), the microprocessor 20 intentionally provides an incorrect answer to the monitoring logic 50.

15           The microprocessor 20 also monitors the timing of the questions or queries posed by the monitoring logic 50. If no question is received for more than a defined period (e.g. 50ms) after receipt of a previous question or query, the microprocessor 20 treats such lack of question or query the same as receiving a wrong answer counter.

20           Upon receipt of a wrong answer counter from the monitoring logic 50, the microprocessor 20 does not wait for a next question or query, but rather sends an intentionally incorrect answer to the monitoring logic 50 and waits for a response. The response time (e.g., 20ms) from the monitoring logic 50 in such a situation should be less than the typical response time (e.g., 50ms).

25           The microprocessor 20 keeps track of a monitoring error counter, which is incremented when the wrong answer counter is incorrect and decremented if the wrong answer counter is correct and greater than 1.

          If the monitor error counter exceeds a threshold value (e.g., 3), such is taken as indicative that the monitoring logic 50 is not operating properly,  
30 and the microprocessor 20 disables the drive, entering a protective state and setting a flag to indicate the suspect error or fault is in the monitoring logic 50.

The microprocessor 20 continues communicating with the monitoring logic 50 in the protective state, in a fashion similar to the communications in a normal state. The microprocessor 20 remains in the protective state even if the monitoring logic 50 starts working properly after shutdown, until the occurrence  
5 of a power cycle.

Figure 3 shows a method 200 of monitoring the operation of the monitoring logic 50 of the FPGA 22 using the microprocessor 20, according to one illustrated embodiment. The method 200 involves the microprocessor 20 from time-to-time intentionally providing an incorrect answer to a question or  
10 query from the monitoring logic 50.

The microprocessor 20 executes waits at 202, and at 204 determines whether the microprocessor 20 has intentionally sent an incorrect answer in response to a question or query from the monitoring logic 50 of the FPGA 22. For example, the microprocessor 20 may check the value of a wrong  
15 answer flag. The microprocessor 20 sets a time out value equal to a first value (e.g. 20ms) and clears the wrong answer sent flag at 206 if an incorrect answer has been intentionally sent, or sets the time out value equal to a second longer value (e.g., 55ms) at 208 if an incorrect answer has not been intentionally sent.

At 210, microprocessor 20 determines whether a next question is  
20 received within the time out value previously set at either 206 or 208. If a next question is not received within the time out value previously set at either 206 or 208, the microprocessor 20 increments a monitor error counter at 212, and determines whether the monitor error counter exceeds a threshold (e.g., three) at 214. If the monitor error counter exceeds the threshold, the microprocessor  
25 20 at 216 triggers a protective state and informs the vehicle. Otherwise, the microprocessor 20 sends an intentionally incorrect answer to the monitoring logic 50 at 218, sets a wrong answer sent flag at 220 and returns control to 202. In sending an intentionally incorrect answer, the microprocessor 20 may, for example, provide a power value that is incorrect for the speed and torque  
30 values identified by the question or query.

If the microprocessor 20 determines at 210 that a next question is received within the time out value previously set at either 206 or 208, the microprocessor 20 determines whether the wrong answer counter is correct at 222. If the wrong answer counter is not correct, control passes to 212 where  
5 the monitor error counter is incremented. If on the other hand the wrong answer counter is correct, the microprocessor 20 determines whether the test monitor counter equals or exceeds a threshold value (e.g., 5) at 224.

If the test monitor counter equals or exceeds the threshold value, the microprocessor 20 resets the test monitor counter at 228, and control  
10 passes to 218. If the test monitor counter does not equal or exceeds the threshold value, the microprocessor 20 increments the test monitor counter at 230. The microprocessor 20 then decrements the monitor error counter at 232 if the monitor error counter is greater than zero, sends a computed answer at 234 and returns to 202 where the microprocessor 20 waits. As noted above,  
15 the computed answer may take the form of a power value calculated based on speed and torque values provided as the question. The computed answer sent at 234 should be a correct answer to the question or query if the microprocessor 20 is operating correctly, and not sending an intentionally incorrect answer.

20 Figure 4A is a schematic diagram showing the switch mechanism 82 operable to switch CAN ports CAN1, CAN2 of a main controller such as the microprocessor 20, between two CAN channels 78a, 78b, according to one illustrated embodiment. The switch mechanism is responsive to a disable signal supplied from the monitoring logic 50 via the Disable Drive and CAN2  
25 line 65.

Figure 4B is a logic diagram for implementing the switch mechanism 82 of Figure 4A with respect to transmit lines or ports of the CAN transceivers, collectively referenced as 80, according to one illustrated embodiment.

30 The microprocessor 20 has first and second transmission ports 300a, 300b, while the CAN transceiver 80 has first and second transmission

ports 302a, 302b. The first transmission port 300a of the microprocessor 20 is coupled to the first transmission port 302a of the CAN transceiver 80 by a first AND gate 304. The second transmission port 300b of the microprocessor 20 is coupled to the second transmission port 302b of the CAN transceiver 80 by a second AND gate 306 and an OR gate 308. A third AND gate 310 couples the first transmission port 300a of the microprocessor 20 to the second transmission port 302b of the CAN transceiver 80 via the OR gate 308. A NOT gate 312 receives the disable signal, which may take the form of a binary signal (e.g., 0/1, Low/High, Open/Closed), and supplies the NOT of the binary signal to the first, second and third AND gates 304, 306, 310.

Figure 4C is a logic diagram for implementing the switch mechanism 82 of Figure 4A with respect to receive lines or ports of the CAN transceivers, collectively referenced as 80, according to one illustrated embodiment.

The microprocessor 20 has first and second receive ports 300c, 300d, while the CAN transceiver 80 has first and second receive ports 302c, 302d. The first receive port 302c of the CAN transceiver 80 is coupled to the first receive port 300c of the microprocessor 20 by a first AND gate 314 and an OR gate 316. The second receive port 302d of the CAN transceiver 80 is coupled to the second receive port 300d of the microprocessor 20 by a second AND gate 318. A third AND gate 320 couples the second receive port 302d of the CAN transceiver 80 to the first receive port 300c of the microprocessor 20 via the OR gate 316. A NOT gate 322 receives the disable signal and supplies the NOT of the binary disable signal to the first, second and third AND gates 314, 318, 320.

The foregoing detailed description has set forth various embodiments of the devices and/or processes via the use of block diagrams, schematics, and examples. Insofar as such block diagrams, schematics, and examples contain one or more functions and/or operations, it will be understood by those skilled in the art that each function and/or operation within such block diagrams, flowcharts, or examples can be implemented, individually and/or

collectively, by a wide range of hardware, software, firmware, or virtually any combination thereof. In one embodiment, the present subject matter may be implemented via Application Specific Integrated Circuits (ASICs). However, those skilled in the art will recognize that the embodiments disclosed herein, in whole or in part, can be equivalently implemented in standard integrated circuits, as one or more computer programs running on one or more computers (e.g., as one or more programs running on one or more computer systems), as one or more programs running on one or more controllers (e.g., microcontrollers) as one or more programs running on one or more processors (e.g., microprocessors), as firmware, or as virtually any combination thereof, and that designing the circuitry and/or writing the code for the software and or firmware would be well within the skill of one of ordinary skill in the art in light of this disclosure. In some embodiments, control may be coordinated among the control subsystem 14 and a fuel cell system controller (not shown) and/or an integrated power train controller (not shown), for example via the CAN.

In addition, those skilled in the art will appreciate that the control mechanisms taught herein are capable of being distributed as a program product in a variety of forms, and that an illustrative embodiment applies equally regardless of the particular type of signal bearing media used to actually carry out the distribution. Examples of signal bearing media include, but are not limited to, the following: recordable type media such as floppy disks, hard disk drives, CD ROMs, digital tape, and computer memory; and transmission type media such as digital and analog communication links using TDM or IP based communication links (e.g., packet links).

Although specific embodiments of and examples for the electric drive system and methods are described herein for illustrative purposes, various equivalent modifications can be made without departing from the spirit and scope of the disclosure, as will be recognized by those skilled in the relevant art. The teachings provided herein can be applied to other power system, not necessarily the electric drive system employing the DC/DC power converter 16 and a DC/AC power converter 18 generally described above.

Portions of the electric drive system 10 may be integrated into a housing to form a power module (not shown). For example, the control subsystem and power converters 16, 18 may be integrated into a housing. In particular, the power module may include an electrically insulative lead frame, an integrated base plate heat sink and an electrically insulative cover,  
5 collectively forming the housing.

The various embodiments described above can be combined to provide further embodiments. All of the U.S. patents, U.S. patent application publications, U.S. patent applications, foreign patents, foreign patent  
10 applications and non-patent publications referred to in this specification and/or listed in the Application Data Sheet, including but not limited to commonly assigned U.S. patent application Serial No. 10/738,926 filed December 16, 2003, and entitled "Power Module With Heat Exchange"; and U.S. patent application Serial No. 10/688,834, filed October 16, 2003 and entitled "Power  
15 Converter Employing A Planar Transformer" ; and U.S. patent application Serial Nos. 60/560,755, filed June 4, 2004, and 10/964,000, filed October 12, 2004, both entitled "Integration of Planar Transformer and Power Switches in Power Converter" are incorporated herein by reference, in their entirety. Aspects of the invention can be modified, if necessary, to employ systems, circuits and  
20 concepts of the various patents, applications and publications to provide yet further embodiments of the invention.

These and other changes can be made to the invention in light of the above-detailed description. In general, in the following claims, the terms used should not be construed to limit the invention to the specific embodiments  
25 disclosed in the specification and the claims, but should be construed to include all power converters. Accordingly, the invention is not limited by the disclosure, but instead its scope is to be determined entirely by the following claims.

## CLAIMS

1. A control system to control an electric drive, the control system comprising:
  - a main controller operable to execute instructions including the computation of a value based on at least one parameter; and
  - a monitoring module operable to provide queries from time-to-time to the main controller, operable to evaluate an accuracy of an answer to a query returned to the monitoring module by the main controller, and operable to execute a protective state entry procedure in response to a determination that a number of answers returned by the main controller that are determined to be incorrect exceeds a threshold value.
2. The control system of claim 1 wherein executing the protective state entry procedure comprises disabling a first communications path between the main controller and a vehicle.
3. The control system of claim 2 wherein executing the protective state entry procedure further comprises disabling a gate drive providing drive control signals to a power converter supplying power to a traction motor.
4. The control system of claim 3 wherein executing the protective state entry procedure further comprises disabling the gate drive providing drive control signals to the power converter such that the traction motor is electrically shorted.
5. The control system of claim 3 wherein executing the protective state entry procedure further comprises disabling the gate drive providing drive control signals to the power converter such that all the semiconductor switches are placed in a non-conducting state.



6. The control system of claim 1 wherein the main controller comprises a microprocessor and the monitoring module comprises monitoring logic configured in a reconfigurable electronic circuit device.

7. The control system of claim 1 wherein the monitoring module is further operable to determine whether a response to the answer to the query is timely received from the main controller.

8. The control system of claim 1 wherein the monitoring module provides queries comprising a speed value and a torque value, and receives answers in the form of a power value computed based on the speed and torque values.

9. A control system to control an electric drive, comprising:  
a main controller operable to execute instructions including the computation of a value based on at least one parameter; and  
a monitoring module operable to provide queries from time-to-time to the main controller, to evaluate an accuracy of an answer to the query returned to the monitoring module by the main controller, and to enter a protective state in response to a determination that a number of answers returned by the main controller that are determined to be incorrect exceeds a threshold value, wherein the main controller is further operable to, from time-to-time provide an intentionally incorrect answer to a query from the monitoring module and to evaluate an operation of the monitoring module based on a handling of the intentionally incorrect answer by the monitoring module.

10. The control system of claim 9 wherein the main controller evaluates the operation of the monitoring module by evaluating a wrong answer counter returned to the main controller by the monitoring logic.

11. The control system of claim 9 wherein the main controller is further operable to shutdown operation of the monitoring module in response to an evaluation that the monitoring logic is not operating correctly.

12. A control system to control an electric drive, comprising:  
a main controller operable to execute instructions including the computation of a value based on at least one parameter;  
a communications subsystem selectively operable to provide a first communications path between the main controller and a vehicle network in a first state, and a second communications path between the main controller and an interface suitable for downloading new instructions to the main controller in a second state; and

a monitoring module operable to provide queries from time-to-time to the main controller, to evaluate an accuracy of an answer to the query returned to the monitoring module by the main controller, and to cause the communications system to enter the second state from the first state in response to a determination of an existence of a fault condition in an operation of the main controller.

13. The control system of claim 12 wherein the interface is suitable for performing diagnostic queries of the main controller via the second communications path.

14. The control system of claim 12 wherein the monitoring module is further operable to enter a protective state in response to a determination that a number of answers returned by the main controller that are determined to be incorrect exceeds a threshold value, wherein the main controller is further operable to, from time-to-time provide an intentionally incorrect answer to a query from the monitoring module and to evaluate an operation of the monitoring module based on a handling of the intentionally incorrect answer by the monitoring module.

15. A control system to control an electric drive, comprising:  
a main controller operable to execute instructions including the computation of a value based on at least one parameter; and  
a fault logic module operable to determine an appropriate procedure for discontinuing a supply of electrical power to a traction motor by a power converter based on a speed of the traction motor and/or a fault history.

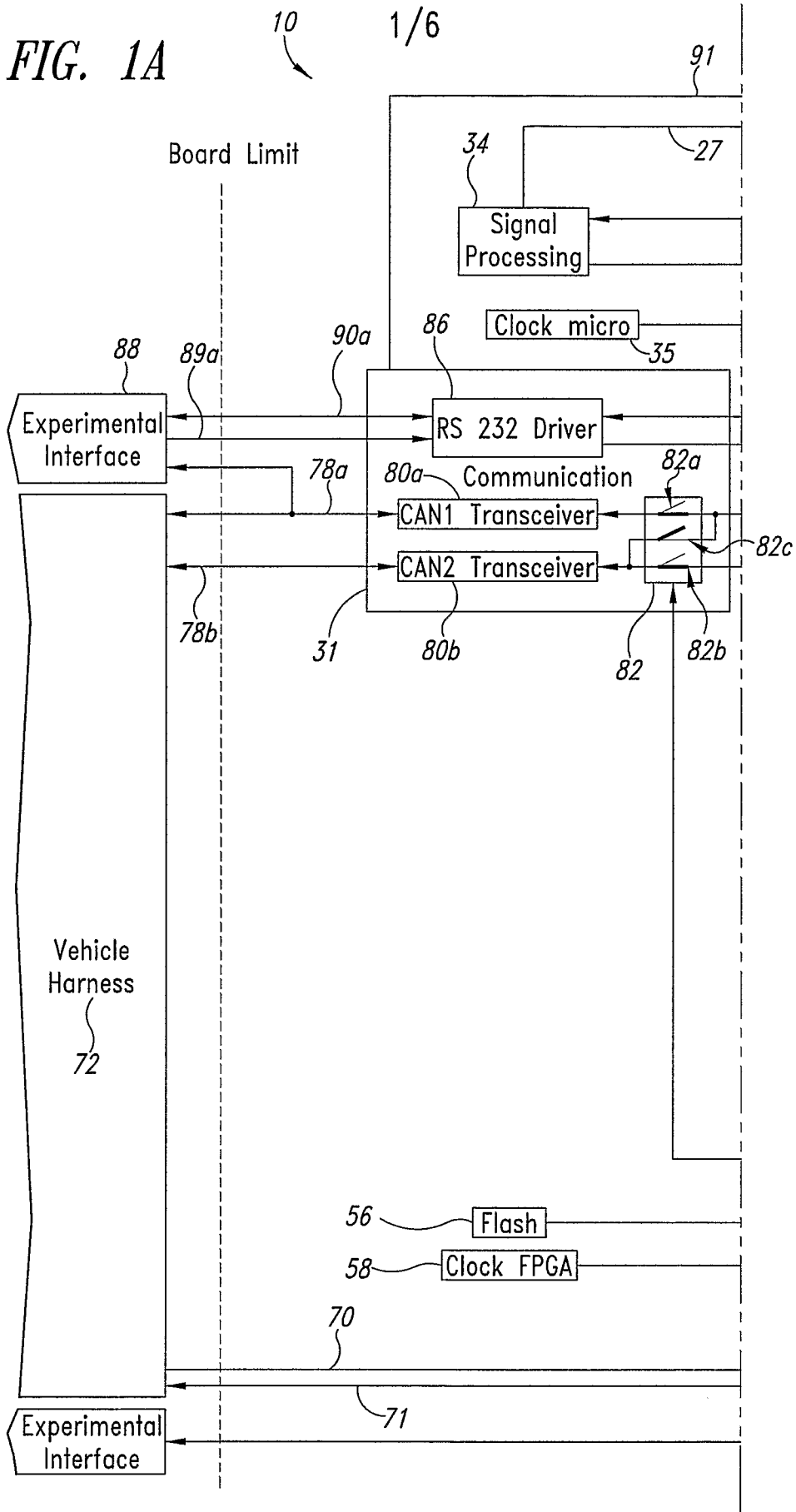
16. The control system of claim 15 wherein the power converter is a DC/AC power converter comprising a plurality of power semiconductor switches in a bridge configuration and the fault logic module places all of the power semiconductor switches in a non-conducting state if the speed of the traction motor is below a threshold speed.

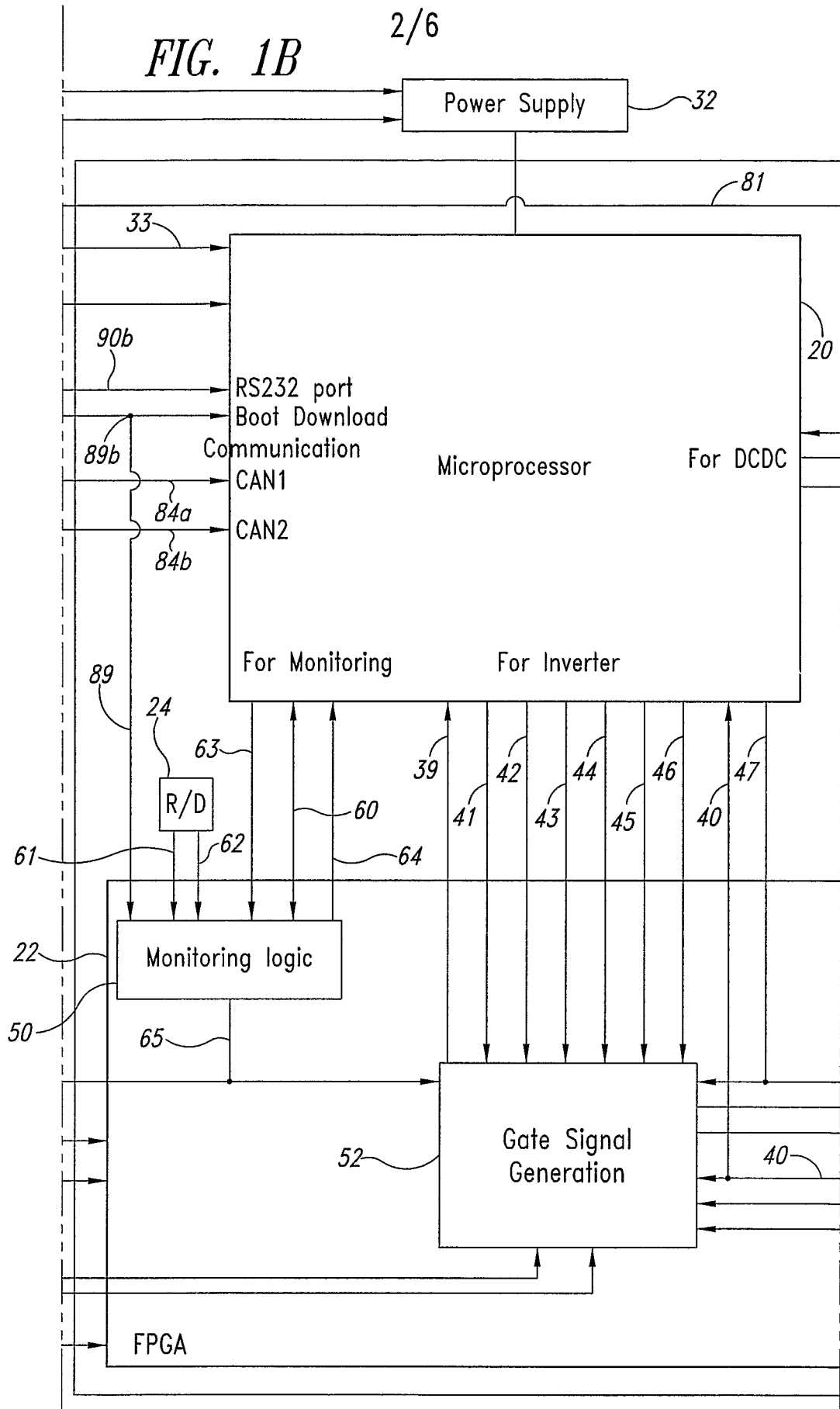
17. The control system of claim 15 wherein the power converter is a DC/AC power converter comprising a plurality of power semiconductor switches in a bridge configuration and the fault logic module places some of the power semiconductor switches in a non-conducting state, and some of the power semiconductor switches in a conducting state to electrically short the traction motor if the speed of the traction motor is above a threshold speed.

18. The control system of claim 15, further comprising:  
a monitoring module operable to provide queries from time-to-time to the main controller, to evaluate an accuracy of an answer to the query returned to the monitoring module by the main controller, and to cause the communications system to enter the second state from the first state in response to a determination of an existence of a fault condition in an operation of the main controller.

19. The control system of claim 18, further comprising:  
a communications subsystem selectively operable to provide a first communications path between the main controller and a vehicle network in a first state, and a second communications path between the main controller and an interface suitable for downloading new instructions to the main controller in a second state.

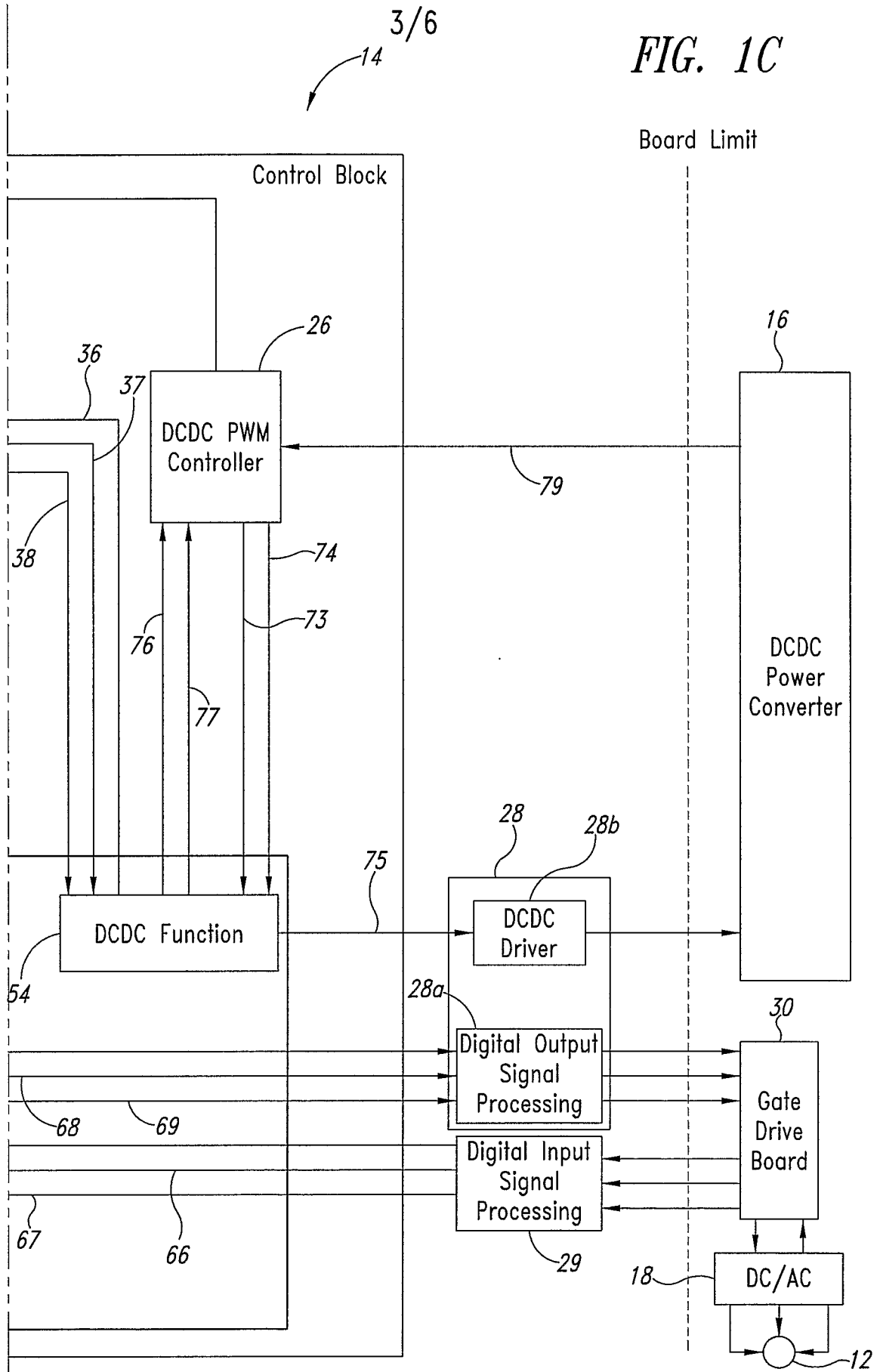
FIG. 1A





3/6

FIG. 1C



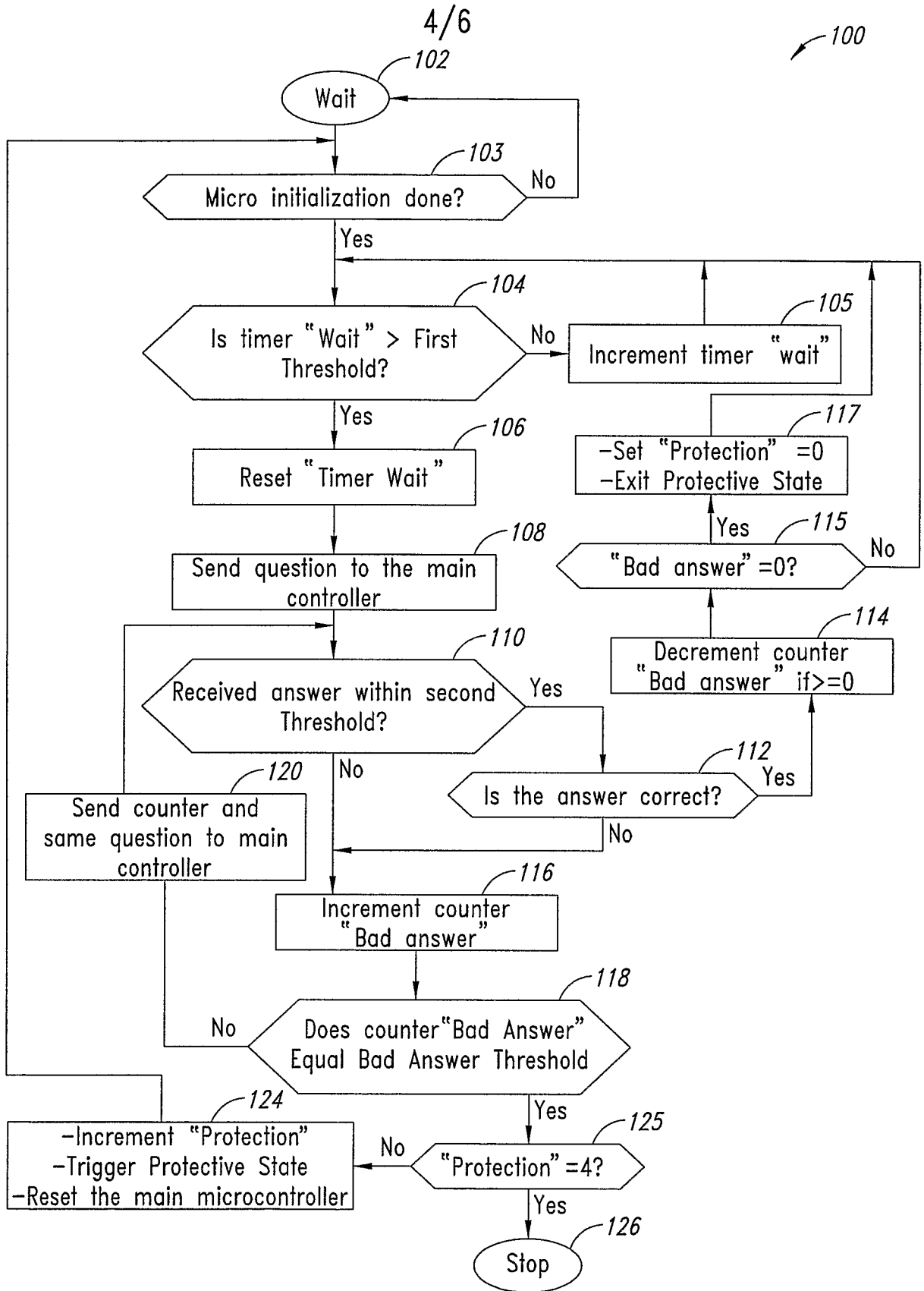


FIG. 2



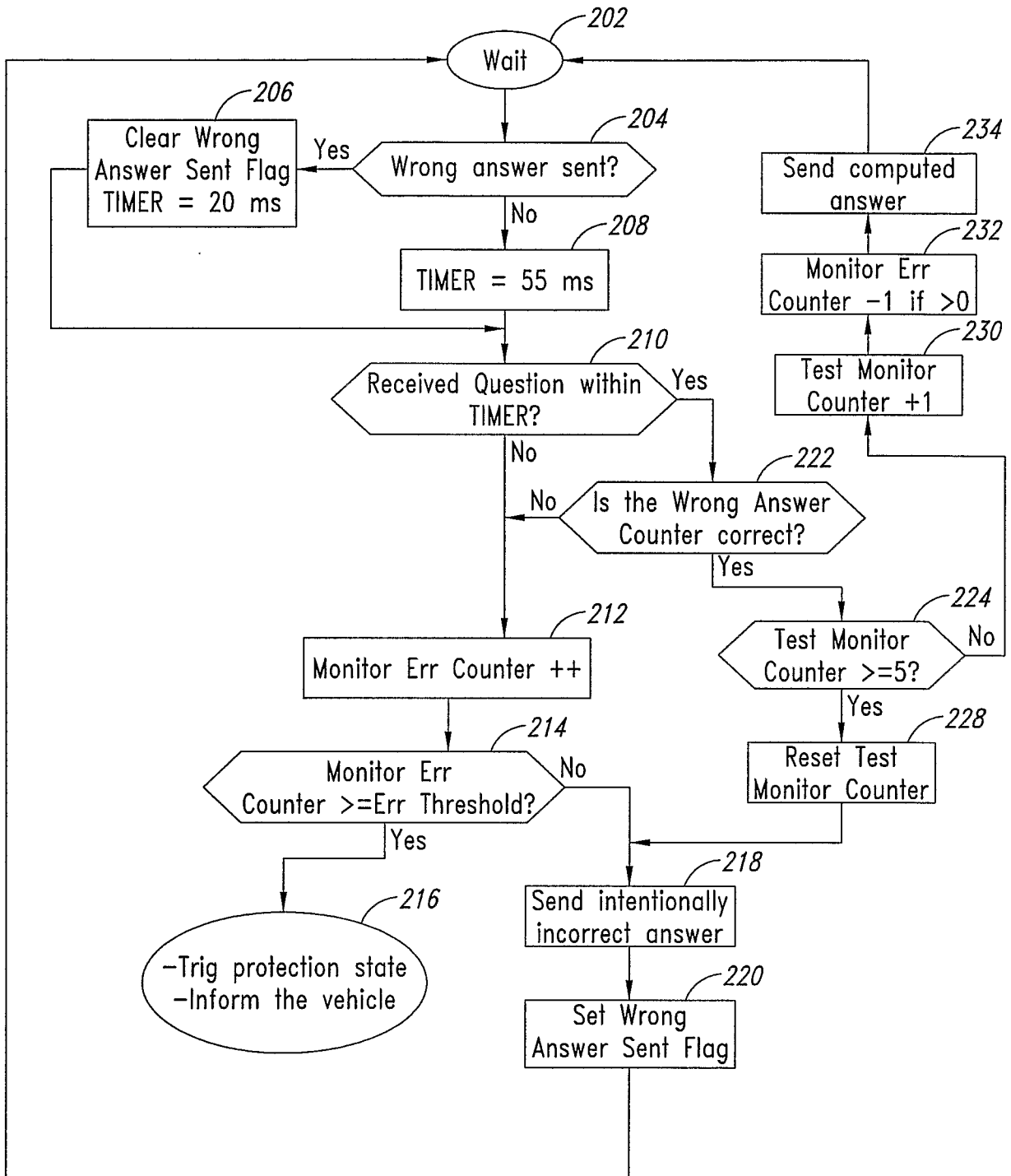


FIG. 3

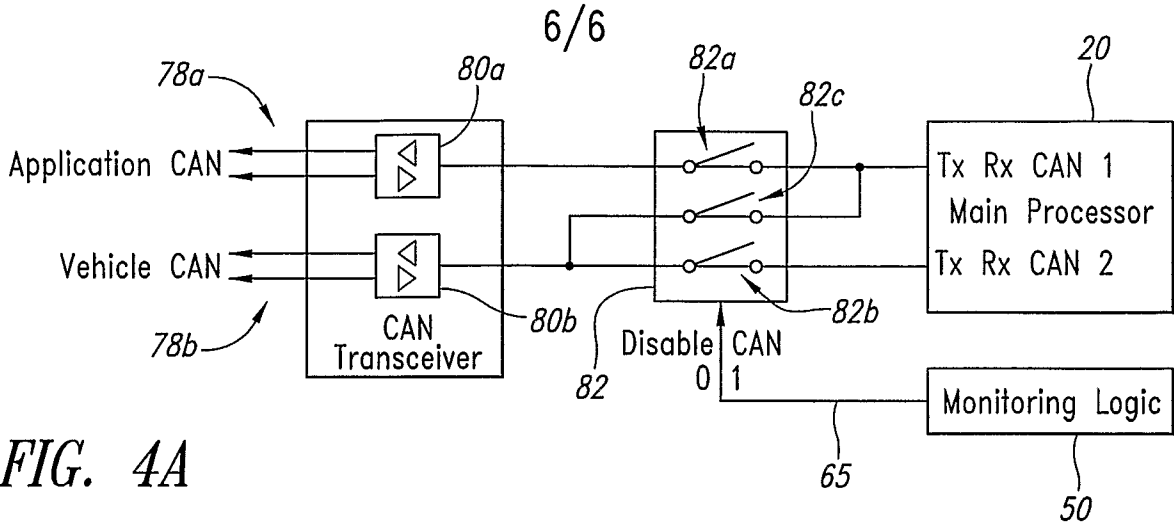


FIG. 4A

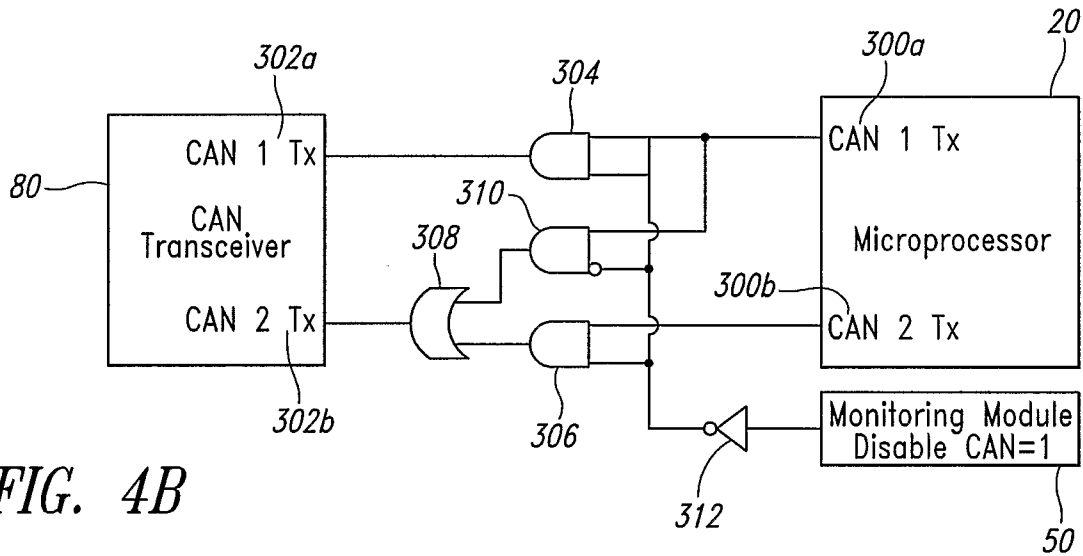


FIG. 4B

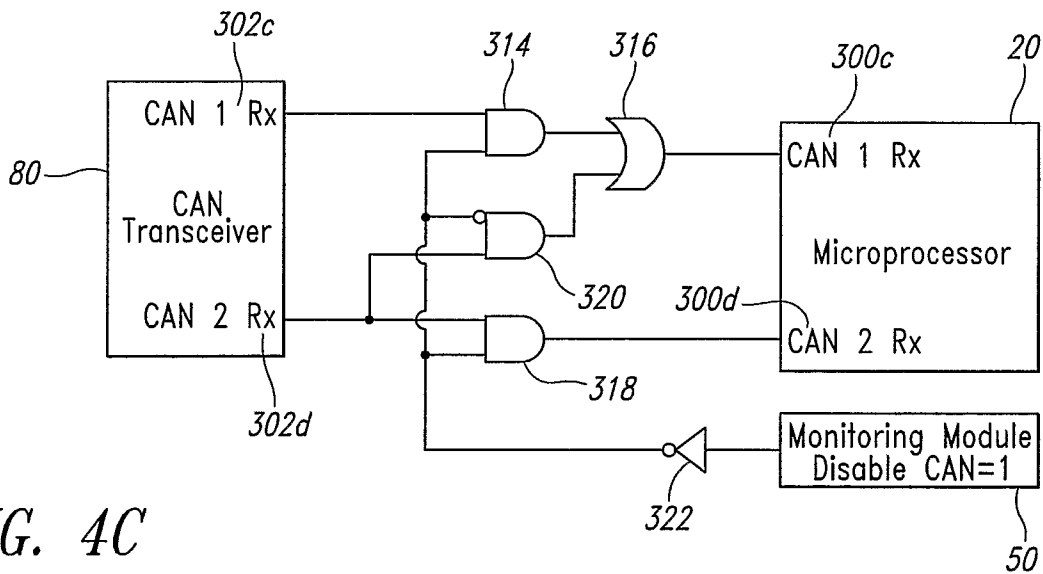


FIG. 4C