

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
23 March 2006 (23.03.2006)

PCT

(10) International Publication Number
WO 2006/031675 A2

(51) International Patent Classification:
G05B 11/01 (2006.01) **G05B 9/02** (2006.01)

(21) International Application Number:
PCT/US2005/032281

(22) International Filing Date:
9 September 2005 (09.09.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/608,684 10 September 2004 (10.09.2004) US

(71) Applicant (for all designated States except US): **GENERAL MOTORS CORPORATION** [US/US]; Legal Staff-Mail Code 482-C23-B21, P.O. Box 300, Detroit, MI 48265-3000 (US).

(72) Inventors: **NAIK, Sanjeev, M.**; 2701 Springtime Drive, Troy, MI 48083 (US). **MISHRA, Pradyumna, K.**; 22202 Solomon Boulevard, Apt. 240, Novi, MI 48375 (US). **PERTET, Soila, M.**; 420 S. Graham Street, Apt. 9, Pittsburgh, PA 15232 (US).

(74) Agent: **MARRA, Kathryn, A.**; General Motors Corporation, Legal Staff-Mail Code 482-C23-B21, P.O. Box 300, Detroit, MI 48265-3000 (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, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

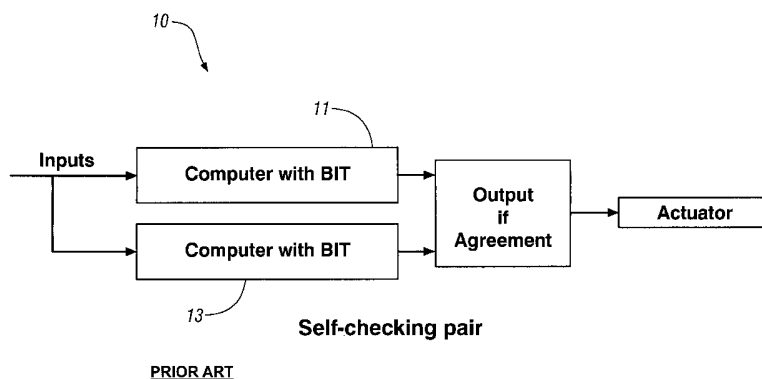
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

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

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

(54) Title: FAULT TOLERANT CONTROL SYSTEM



(57) Abstract: A dual-redundant propulsion-by-wire control architecture with robust monitoring is presented to increase system availability without compromising safety. The dual-redundant controllers are able to cross-monitor and self-monitor. Self monitoring is effected at the application level and built-in system tests are performed. The monitor functions are set as high priority tasks. The first controller controls operation of a first propulsion system, monitors operation of a second controller, and, self-monitors. The second controller controls operation of a second propulsion system, monitors operation of the first controller, and, self-monitors. Each controller is operable to identify faults occurring in the first and the second controller, and implement an alternate operating control scheme for the respective propulsion system when a fault is identified. The first controller is signally connected to the second controller by substantially redundant communications buses.

FAULT TOLERANT CONTROL SYSTEM

TECHNICAL FIELD

[0001] This invention generally relates to vehicle control systems. More particularly, this invention relates to fault-tolerant by-wire vehicle control systems.

BACKGROUND OF THE INVENTION

[0002] Vehicle systems designers are developing numerous propulsion systems to improve energy-efficiency and reduce need for consumption of fossil fuels, including fuel/electric hybrid systems having batteries and individual wheel motors, and fuel-cell systems. Each system uses one or more electronic controllers to control ongoing operation of all or part of one or more systems related to vehicle operation and propulsion. Such vehicle systems include various by-wire control systems, each consisting of an operator-controlled input device which is connected via electric wiring harness and a controller to one or more actuators. Such systems include, for example, propulsion-by-wire and brake-by-wire systems.

[0003] By-wire control systems provide a number of advantages with regard to system packaging. The associated electronic control systems and the implementation of advanced computer control algorithms facilitate numerous new control features. Much attention has been given to designing by-wire control systems and control architectures that ensure robust operation. General design techniques which have been employed in such systems are

redundancy, fault tolerance to undesired events (e.g., events affecting control signals, data, hardware, software or other elements of such systems), and, fault monitoring and recovery to determine if and when such an event has occurred. A typical fault detection scheme takes or recommends action to ensure desired response and control of the vehicle. One approach to providing fault tolerance utilized in by-wire control systems is to design control systems and control architectures which ensure that no single event occurring in the system causes a complete loss of the desired control of the system.

[0004] The prior art often uses a control architecture comprising dual-redundant control systems to overcome the aforementioned concerns. FIG. 1 schematically illustrates a general dual-redundant by-wire control system 10, which comprises a fail-silent control system. The control system 10 generally comprises a pair of substantially identical controllers 11, 13 which implement substantially identical software algorithms. Each of controllers 11, 13 is adapted to provide a control signal for agreement comparison with the other. When the controller outputs agree, a control signal is provided to an actuator, smart actuator or controller for implementation of the control signal. Unless and until the controllers agree, the actuator assumes a predetermined state. Therefore, the system shown in FIG. 1 fails silent after the first fault in either controller. This behavior may be acceptable from a risk management standpoint but undesirably reduces the availability of the system.

Additionally, such architecture does not address software anomalies that may manifest in systems having identity of algorithms among controllers.

[0005] Increased dependability in performance-critical by-wire systems, e.g., propulsion-by-wire ('PBW'), is typically achieved by increasing the level

of hardware redundancy. However, increased levels of hardware redundancy lead to increased system cost and complexity. A single fault in a traditional dual-redundant PBW system (i.e., system with lowest level of redundancy) has the potential to lead to the loss of both the front and the rear (or other distribution) propulsion systems.

[0006] In addition, such systems typically make certain assumptions regarding occurrence of system faults, including there being a single, independent fault per communication cycle (arbitrary or fail-silent); there being no masquerading faults on a controller area network (CAN); and there being no integration of a disabled propulsion system until system reset or successful built-in-self test.

SUMMARY OF THE INVENTION

[0007] The present invention uses a novel dual-redundant propulsion-by-wire architecture with robust monitor that increase system availability without compromising safety. Dual-redundant controllers are characterized by monitors effecting cross-monitoring and self-monitoring. Self monitoring is effected at the application level and built-in system tests are performed. The monitor functions are set as high priority tasks, further increasing the level of security in the system.

[0008] In accordance with the present invention, a fault-tolerant control system for a vehicle propulsion system is provided, comprising a first controller, adapted to: control operation of a first propulsion system, monitor operation of a second controller, and, self-monitor. The second controller is adapted to control operation of a second propulsion system, monitor operation

of the first controller, and, self-monitor. Each said controller operable to identify a plurality of faults occurring in the first and the second controller. The first controller operable to implement an alternate control scheme for operating the first propulsion system when a fault is identified therein. The second controller operable to implement an alternate control scheme for operating the second propulsion system when a fault is identified therein.

[0009] Another aspect of the invention is the fault-tolerant control system having the first controller signally connected to the second controller by substantially redundant communications buses.

[0010] Another aspect of the invention comprises each controller operable to execute a built-in-test capable to identify faults as a highest priority task when the controller self-monitors.

[0011] Another aspect of the invention comprises each controller operable to determine when a plurality of outputs of the alternate controller is each within a desired range when the said controller monitors operation of the alternate controller.

[0012] Another aspect of the invention comprises notifying an operator when a fault is identified by the first controller or the second controller.

[0013] Another aspect of the invention comprises the second controller operable to substantially disable operation of the second propulsion system.

[0014] A further aspect of the invention comprises the first controller operable to operate the first propulsion system when operation of the second propulsion system is substantially disabled.

[0015] Another aspect of the invention comprises the first controller operable to substantially disable operation of the first propulsion system.

[0016] A further aspect of the invention comprises the second controller operable to operate the second propulsion system when operation of the first propulsion system is substantially disabled.

[0017] Another aspect of the invention comprises the first propulsion system being a fuel-cell power system.

[0018] Another aspect of the invention comprises the first propulsion system being an internal combustion engine and driveline.

[0019] Another aspect of the invention comprises the second propulsion system being independent electric wheel motors powered by a high-voltage battery system.

[0020] The exemplary system provides benefits resulting from low levels of hardware redundancy. The diverse and robust monitors improve fault-isolation capabilities and guard against many hardware and software anomalies. The monitors combine self-check of traditional dual-redundant systems with application-specific tests and built-in-tests. Furthermore, a single fault does not result in the loss of both the front and rear propulsion systems. If the monitor on the rear controller fails silent, the front propulsion system is disabled to prevent run-away situations by a subsequent failure in the front controller. Similarly, if the monitor on the front controller fails silent, the rear propulsion system is disabled to prevent run-away situations by a subsequent failure in the rear controller. The minimal amendment of redundancy effects lower system cost, compared to the prior art.

[0021] These and other aspects of the invention will become apparent to those skilled in the art upon reading and understanding the following detailed description of the embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022] The invention may take physical form in certain parts and arrangement of parts, the preferred embodiment of which will be described in detail and illustrated in the accompanying drawings which form a part hereof, and wherein:

[0023] Fig. 1 is a schematic diagram of a prior art fault-tolerant control system;

[0024] Fig. 2 is a schematic diagram of a fault-tolerant control system, in accordance with the present invention;

[0025] Fig. 3 is a schematic diagram of an embodiment of a fault-tolerant control system, in accordance with the present invention; and,

[0026] Fig. 4 is an exemplary monitoring system, in accordance with the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0027] Referring now to the drawings, wherein the showings are for the purpose of illustrating the invention only and not for the purpose of limiting the same, Fig. 2 shows a schematic of an exemplary fault-tolerant control scheme which has been constructed in accordance with the present invention.

The system includes a first system 101 including a first system control unit 103, and a second system 105 including a second system control unit 107.

There is a first supervisory control module 109 including a first control 111 and a second system monitor 113 operable to monitor the second system 105.

A second supervisory control unit 115 includes a second control 117 and a

first system monitor 119 operable to monitor the first system 101. A first system control bus 121 is operatively coupled to the first control 111, the first system control unit 103 and the first system monitor 119. A second system control bus 123 is operatively coupled to the second control 117, the second system control unit 107 and the second system monitor 113. The first control 111 provides a first system command to the first system control unit 103 and the first system monitor 119, and provides a virtual second system command to the second system monitor 113. The second control 117 provides a second system command to the second system control unit 107 and the second system monitor 113, and provides a virtual first system command to the first system monitor 119. The first and second system monitors are characterized by cross-monitoring, and, by self-monitoring, i.e. some form of built-in testing.

[0028] Referring now to FIG. 3, a specific embodiment of the system described hereinabove, and having two associated or alternate controllers, is shown. The first system 101 is preferably a front propulsion and power system for propelling front wheels of a vehicle (not shown). The first propulsion system 101 preferably comprises a single motor front electric traction system ('FETS') 131, which is powered by a fuel-cell power system ('FCPS') 125 and includes a power distribution system ('DCDU') 127. The first propulsion system 101 is controlled by first controller 109, which includes front controller 111 and second system monitor 113. The front controller 111 is signally operably connected to the front propulsion and power system 101 via a FETS controller area network ('CAN') 121.

[0029] The second system 105 is preferably a rear propulsion and power system for propelling rear wheels of the vehicle (not shown). The second

system preferably comprises a pair of rear independent electrical wheel motors 133, 135 powered by an electric energy storage system, e.g. a high voltage ('HV') battery 129. The second system 105 is controlled by second controller 115 which includes rear propulsion controller 117 and first system monitor 119. The rear propulsion controller 117 is signally operably connected to the rear propulsion system 105 via rear, or wheel motor, CAN 123. The fuel-cell power system ('FCPS') 125 and power distribution system ('DCDU') 127 are preferably operably linked to the HV battery 129 as shown by connection 137. The first system monitor 119 is signally connected to the front controller 111 of the first controller 109 via the FETS CAN 121. The second system monitor 113 is signally connected to the rear controller 117 of the second controller 115 via the rear CAN 123. The FETS CAN 121 and the rear CAN 123 preferably comprise effectively redundant bus systems by which various controllers and electronic systems are networked, permitting communications between the controllers and systems, and thus facilitating operation of each controller and system. The redundant CAN bus feature allows the system to tolerate a single communications failure without disabling the vehicle unnecessarily. Controller area networks ('CAN') are known to one skilled in the art and not discussed in detail hereinafter.

[0030] In operation, the front and rear controllers 111, 117 conduct built-in testing to identify faults that may have occurred internal to the individual controller 111, 117. Built-in testing typically comprises one or more algorithms which monitor the controller hardware, inputs/outputs of the controller, and communications buses for faults. Monitored faults typically include corrupted memory locations, overflow or corruption of memory

stacks, overrun of a processor, over/under temperature conditions in the controller, over/under power supply voltage conditions, and failure of a watchdog timer. The built-in-test may include a stimulus engine, whereby the controller proactively stimulates a portion of the controller and expects a specific predetermined result to occur. If the specific predetermined result does not occur, it may indicate presence of a fault. A built-in-test monitoring algorithm typically runs on a 10 millisecond loop, and is treated as a high-priority task in the controller. A high-priority task is a task that preferably continues to execute to completion, and suspends actions of other tasks, regardless of other actions in the controller, e.g. interrupts.

[0031] Additionally, each monitor 113, 119 runs a simple and robust software monitor, which is executed in conjunction with the associated or alternate controller 117, 111. Fault coverage typically includes checking specific controller outputs to assure each output is within a desired range, i.e. rationality checks of the outputs of the monitored controller. The out-of-range check typically identifies defects resulting from defective or corrupted software. Typical fault coverage includes application divergence, i.e. run-time errors or input sensor faults, division by zero, infinity subtracted from infinity, infinity added to infinity, zero divided by zero, invalid compare operation, invalid square root calculation, or invalid integer conversion.

[0032] With additional reference now to Fig. 4, an exemplary software monitor is described, comprising monitoring of torque generated in the rear propulsion system 105. The front controller 109 includes the front propulsion system controller 111 and second system monitor 113, with torque control output to the front propulsion system 101. The second system monitor 113

determines rear torque, as described below. The rear controller 117 sends a signal comprising its determination of torque generated by the rear propulsion system 105 to the front monitor 113 over rear CAN bus 123. The front controller 111 provides a signal comprising its determination of rear propulsion system torque for comparison purposes, i.e. a virtual signal, determined by the second system monitor 113, as follows. The front controller 111 monitors operator input to an accelerator pedal 201 of the vehicle, and determines a fault-tolerant accelerator pedal sensor value 203, in first step 210. A maximum torque value is determined, based upon the fault-tolerant accelerator pedal sensor value 203, in second step 220. The maximum torque value is preferably based upon the position of the accelerator pedal 203 using a precalibrated table contained in software of the second system monitor 113. In the event of substantial disagreement of the torque for the rear system between the front controller 111 and rear controller 117, a decision is made to disable the rear propulsion system when the rear torque value determined by the front controller 111 is less than the maximum torque determined in step 220, as shown in step 230. This action is true, if the built-in test of the front controller 109 succeeds. Alternatively, when the torque determination from the monitor 113 of the front controller 109 substantially agrees with the torque determination from the rear controller 117, the rear propulsion system continues operation. When the determined values for rear torque disagree, as above, the second system monitor 113 indicates a fault, communicates the fault to the rear controller 117 via rear CAN bus 123, which is responsible for controlling the rear propulsion system 105 and acts to implement an alternate control scheme of the rear propulsion system 105, including disabling the rear

propulsion system 105. Other such algorithms for cross-controller monitoring typically comprise other signal input-based rationality checks similar to that described hereinabove.

[0033] Combining built-in test functions with associated or alternate controller test functions provides a more complete monitoring of each controller 111, 117 for detection of faults that may occur therein. When the monitor detects a fault in the associated or alternate controller, it disables the appropriate propulsion motors and power supply.

[0034] The controllers 117, 119 may be programmed to take specific actions in the event of a single fault, and in the event of a second fault. A fault is preferably detectable in the first control module 109 including the first control 111 and second system monitor 113, the second control module 115 including the second control 117 and first system monitor 119, FETS CAN 121 and rear CAN 123. The front propulsion and power system 101 comprising the single motor front electric traction system (FETS), including the fuel-cell power system (FCPS) and power distribution system (DCDU), and the rear system 105 comprising the wheel motors and HV battery are also monitored. When a single, or first, fault, is identified, the system having the identified fault is preferably disabled. A fault may be identified by the built-in-test of the respective controller 109, 115, or by the monitor 113, 119 of the other controller 115, 109. In the event one of the controllers 111, 117 or monitors 113, 119 identifies a second fault, the respective controller may continue to operate and disable the system having the identified fault. Alternatively, occurrence of a second fault may result in a controller commanding operation in a fail-safe mode. A fail-safe operating mode may

include controller-induced actions such as braking compensation during operation. Other situations are readily discernible to a skilled practitioner, and not described in further detail herein.

[0035] The present invention has been described with respect to certain exemplary embodiments. However, these embodiments are intended as non-limiting examples of the invention, it being recognized that alternative implementations are within the scope of the invention. For example, while front and rear propulsion systems have been described, each wheel of a vehicle may have its own associated electric machine for practicing the present invention. Furthermore, one of the propulsion systems may comprise an internal combustion engine with a driveline to one or more of the wheels. Accordingly, it is intended that the invention not be limited to the disclosed embodiments. It is intended that the invention includes all such modifications and alterations insofar as they come within the scope of the invention, as described in the language of the following claims.

[0036] Having thus described the invention, it is claimed:

1. Fault-tolerant control system, comprising:
 - a first controller, adapted to: control operation of a first system, monitor operation of a second controller, and, self-monitor;
 - the second controller, adapted to: control operation of a second system, monitor operation of the first controller, and, self-monitor;
 - each said controller operable to identify faults occurring in the first and the second controller;
 - the first controller operable to implement an alternate control scheme for operating the first propulsion system when a fault is identified therein; and,
 - the second controller operable to implement an alternate control scheme for operating the second propulsion system when a fault is identified therein.
2. The fault-tolerant control system of claim 1, further comprising: the first controller signally connected to the second controller by substantially redundant communications buses.
3. The fault-tolerant control system of claim 2, wherein each said controller operable to identify faults occurring in the first and the second controller comprises: each controller operable to self-monitor by executing a built-in-test capable to identify faults.
4. The fault-tolerant control system of claim 3, wherein each said controller operable to identify faults occurring in the first and the second controller

comprises: each controller operable to monitor operation of the other controller and determine when an output of the other controller is within a desired range.

5. The fault-tolerant control system of claim 4, further comprising: notifying an operator when a fault is identified by the first controller or the second controller.

6. The fault-tolerant control system of claim 1, wherein the second controller operable to implement an alternate control scheme for operating the second propulsion system when a fault is identified therein comprises: the second controller operable to substantially disable operation of the second propulsion system.

7. The fault-tolerant control system of claim 6, comprising the first controller operable to operate the first system when operation of the second system is substantially disabled.

8. The fault-tolerant control system of claim 1, wherein the first controller operable to implement an alternate control scheme for operating the first system when a fault is identified therein comprises the first controller operable to substantially disable operation of the first system.

9. The fault-tolerant control system of claim 8, further comprising the second controller operable to operate the second system when operation of the first system is substantially disabled.

10. The fault-tolerant control system of claim 1, wherein the first system comprises a fuel-cell powered propulsion system.

11. The fault-tolerant control system of claim 1, wherein the first system comprises an internal combustion engine powered propulsion system.

12. The fault-tolerant control system of claim 11, wherein the second system comprises an electric energy storage system powered propulsion system including independent electric wheel motors.

13. The fault-tolerant control system of claim 1, wherein the second system comprises an electric energy storage system powered propulsion system including independent electric wheel motors.

14. The fault-tolerant control system of claim 1, wherein the second system comprises an electric energy storage system powered propulsion system including independent electric wheel motors.

15. Fault tolerant control system comprising:

a first system including a first system control unit;

a second system including a second system control unit;

a first supervisory control module including a first control and a second system monitor;

a second supervisory control module including a second control and a first system monitor;

a first system control bus operatively coupled to said first control, said first system control unit and said first system monitor;

a second system control bus operatively coupled to said second control, said second system control unit and said second system monitor;

said first control providing a first system command to said first system control unit and said first system monitor, and providing a virtual second system command to said second system monitor;

said second control providing a second system command to said second system control unit and said second system monitor, and providing a virtual first system command to said first system monitor; and,

said first and second supervisory control modules characterized by cross-monitoring and self-monitoring.

16. The fault-tolerant control system of claim 15, wherein the first system comprises a fuel-cell powered propulsion system.

17. The fault-tolerant control system of claim 15, wherein the first system comprises an internal combustion engine powered propulsion system.

18. The fault-tolerant control system of claim 15, wherein the second system comprises an electric energy storage system powered propulsion system including independent electric wheel motors.

19. The fault-tolerant control system of claim 15, wherein the second system comprises an electric energy storage system powered propulsion system including independent electric wheel motors.

20. The fault-tolerant control system of claim 15, wherein the second system comprises an electric energy storage system powered propulsion system including independent electric wheel motors.

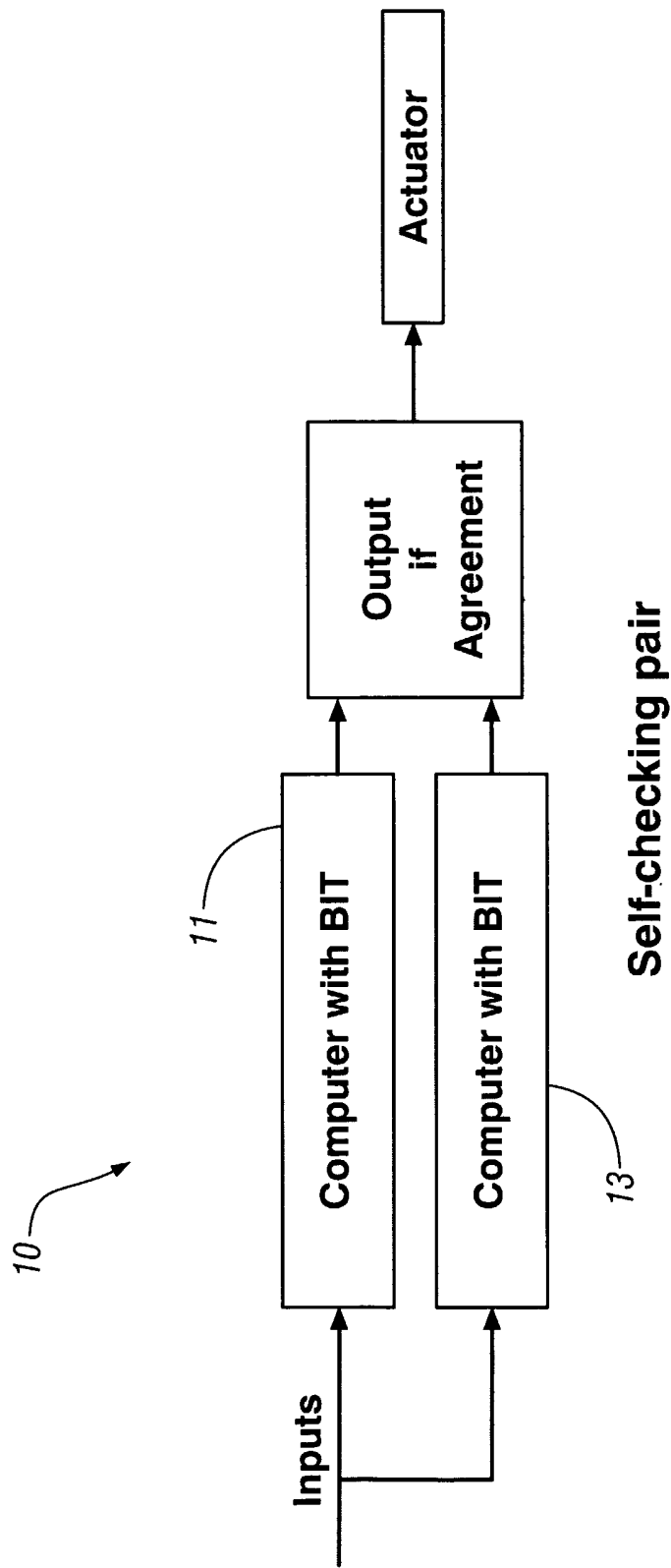
21. Fault tolerant control system for a vehicle having first and second propulsion systems comprising:

a first control module including a) a first control for providing the first propulsion system with a primary first propulsion system command and b) a first monitor;

a second control module including a) a second control for providing the second propulsion system with a primary second propulsion system command and b) a second monitor;

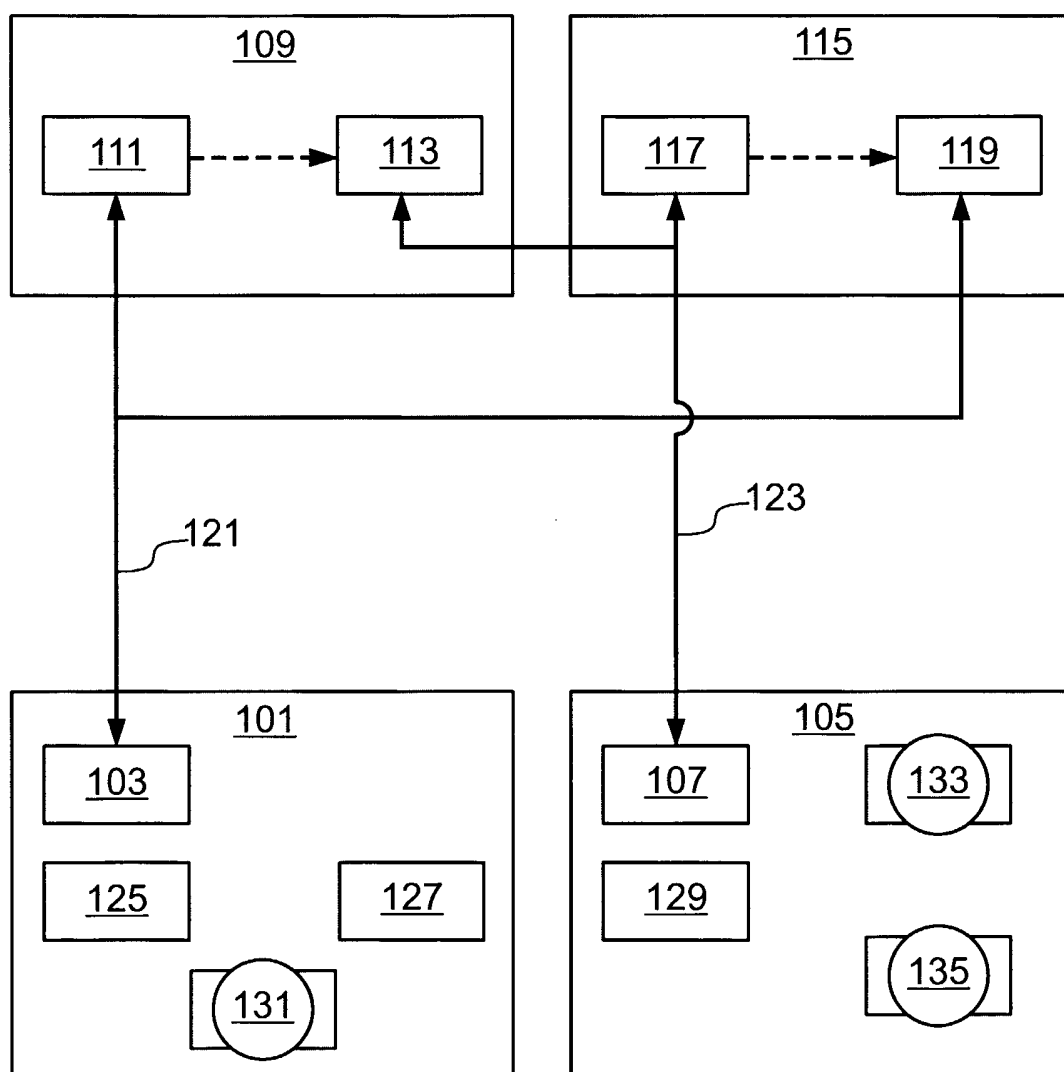
said first monitor adapted to receive said primary second propulsion system command and perform rationality checks thereon to detect faults of the second control module; and,

said second monitor adapted to receive said primary first propulsion system command and perform rationality checks thereon to detect faults of the first control module.



PRIOR ART
FIG. 1

2/4

*FIG. 2*

3/4

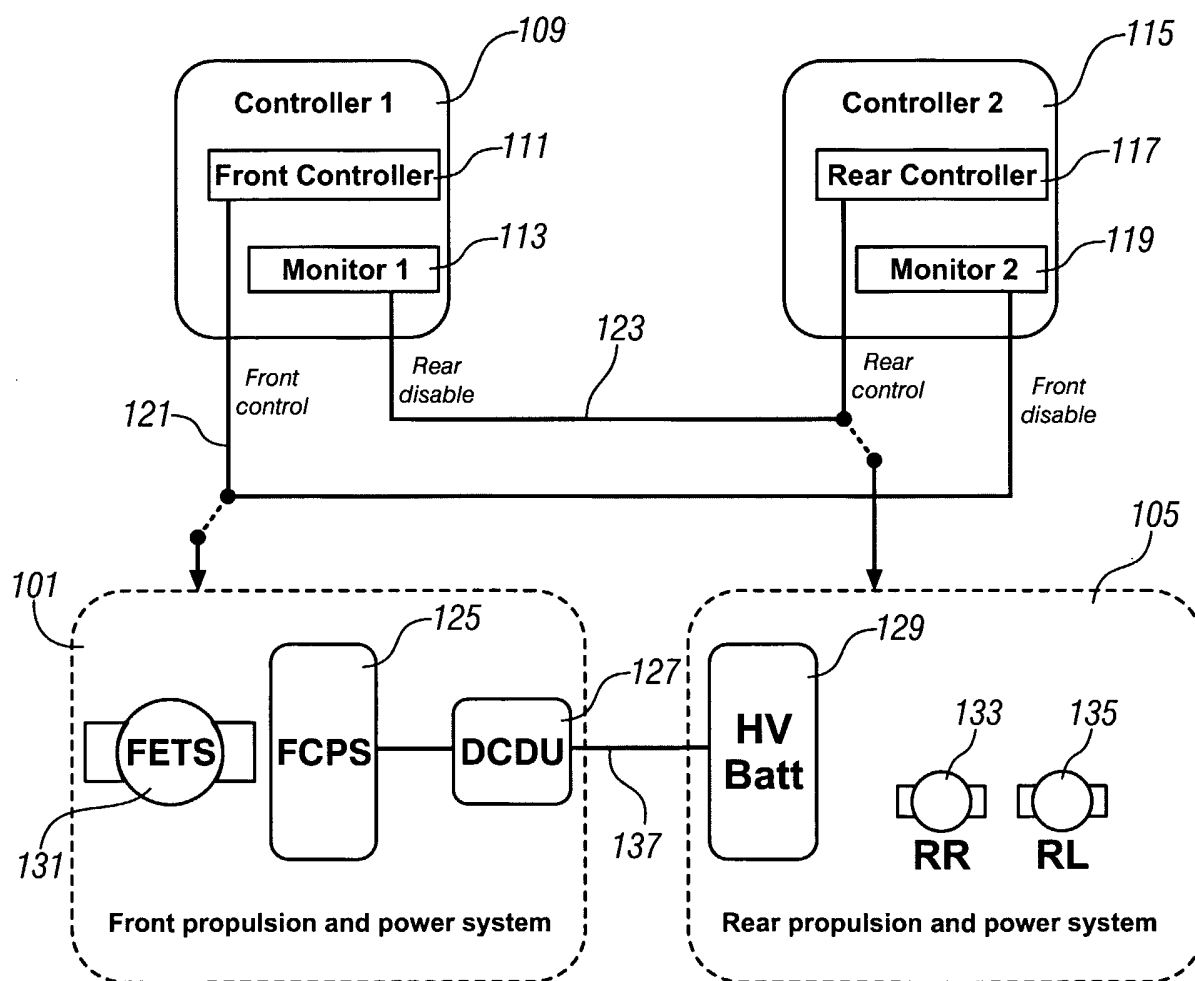


FIG. 3

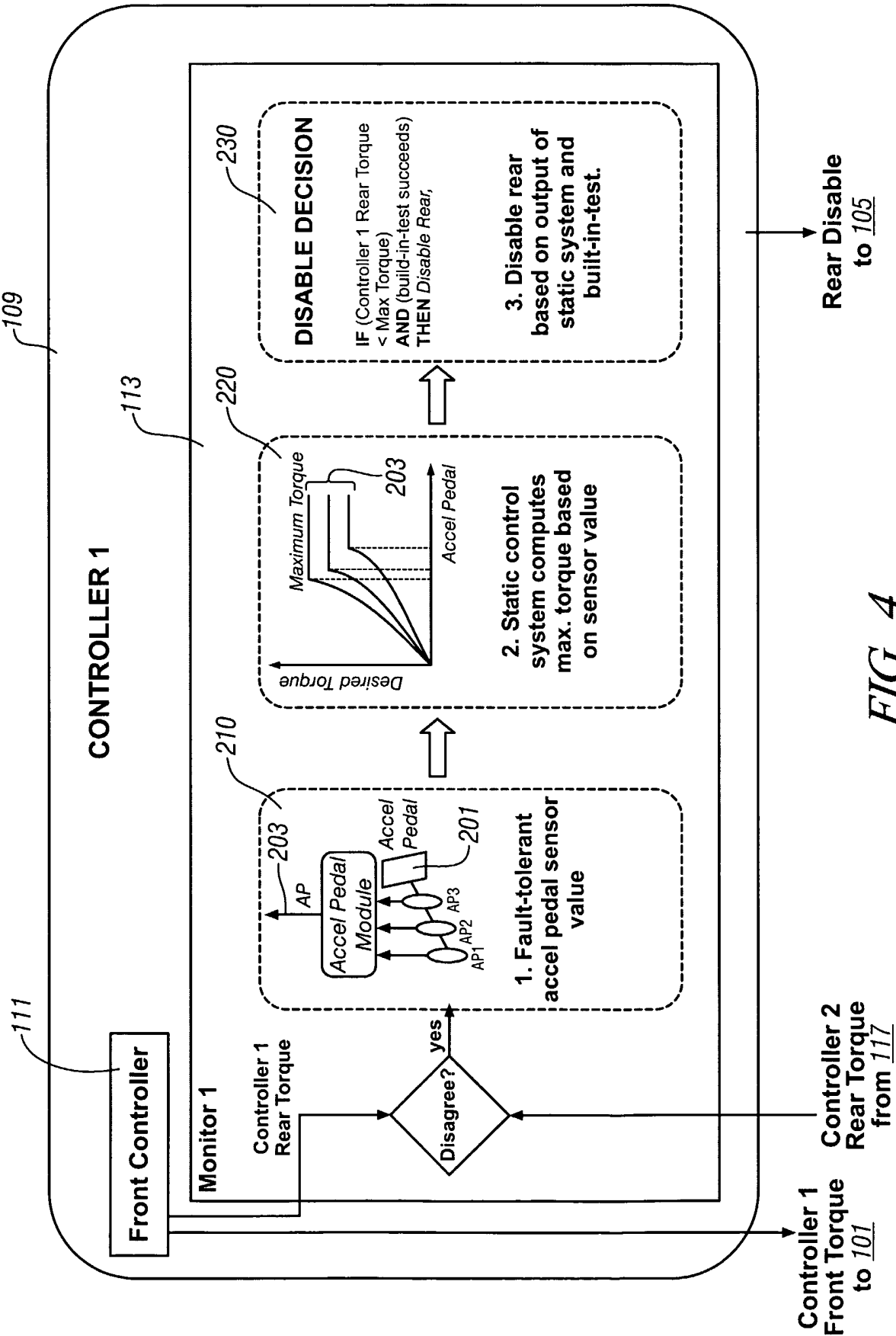


FIG. 4