



(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
29.12.2010 Bulletin 2010/52

(51) Int Cl.:
F02D 41/22 (2006.01) F02D 41/26 (2006.01)

(21) Application number: **09163596.1**

(22) Date of filing: **24.06.2009**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK TR
Designated Extension States:
AL BA RS

(72) Inventor: **Walker, Darren**
Lower Halling, Kent ME2 1ET (GB)

(74) Representative: **Gregory, John David Charles**
Delphi Diesel Systems
Patent Department
Courteney Road
Gillingham
Kent ME8 0RU (GB)

(71) Applicant: **Delphi Technologies Holding S.à.r.l.**
4940 Bascharage (LU)

(54) **Engine Control System**

(57) A vehicle engine control system is described. The system comprises a main microprocessor (10) for controlling the vehicle engine and a monitoring microprocessor (12) for monitoring the correct operation of the main microprocessor (10). The monitoring microprocessor (12) is configured to receive a first signal (20) indicative of a driver command, and a second signal (18) indicative of an actual engine output parameter. The mon-

itoring microprocessor (12) is further configured to determine from the first and second signals (20, 18) if the actual engine output parameter is within a predefined acceptable operating envelope. In the event that a fault is detected in the main microprocessor (10), the main microprocessor is allowed to continue to operate the vehicle engine provided that the actual engine output parameter is within the acceptable operating envelope as monitored by the monitoring microprocessor (12).

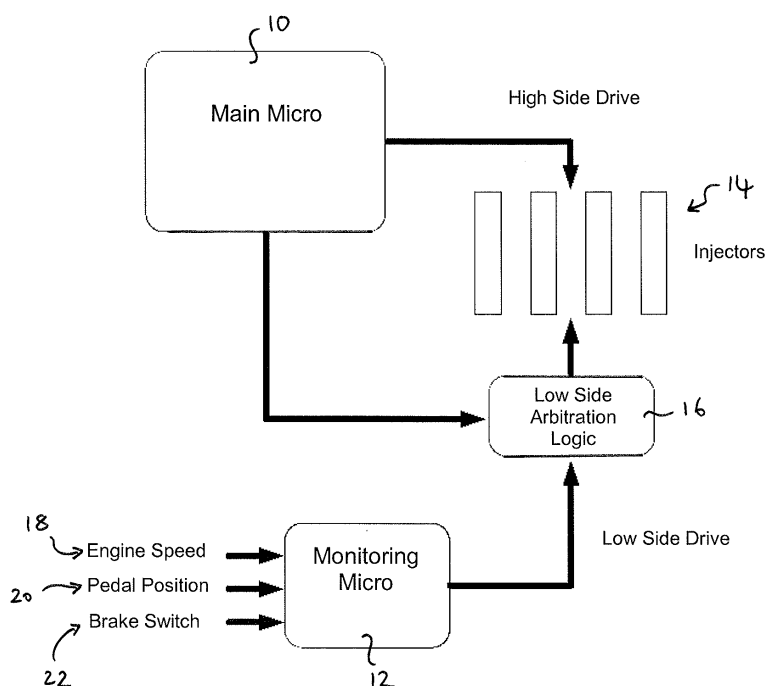


Fig. 2

Description

Technical Field

[0001] The present invention relates to a vehicle engine control and monitoring system, and in particular to an improved system that increases vehicle availability in the event of a fault condition.

Background

[0002] The engine control unit (ECU) of a vehicle engine includes a main microprocessor for controlling various engine functions, including vehicle drive. If the main microprocessor (hereinafter the "main micro") develops an error, for example an algorithmic error, then potentially dangerous consequences can arise. For example, the engine may be caused to deliver torque in excess of the driver demanded torque. For this reason, modern ECUs often include an electronic safety monitor (ESM). The ESM may comprise a dedicated microprocessor (hereinafter referred to as a "monitoring micro"), which is configured to monitor the correct operation of the main micro.

[0003] At present, if a fault develops in the main micro, the default action is to shut down the main micro or execute a so-called "safe state". In either case, injection events are disabled in the engine, which results in an immediate loss of power. This causes the engine to stall and consequently reduces vehicle availability in the event of a main micro fault. In some circumstances, shutting down the system in this way can be dangerous, for example if a fault develops when the vehicle is travelling at speed in the outside lane of a motorway.

[0004] In addition to the aforesaid problems, prior art systems may not be capable of detecting certain faults. In general, prior art monitoring systems are configured to monitor output signals from the ECU before those signals reach the engine. The problem with this is that these systems are not able to detect faults that occur downstream of where the feedback signal is taken. This is illustrated schematically in Figure 1.

[0005] Referring to Figure 1, there is shown an ECU (1) having a main micro (10), an output module (2), and an ESM (3). External to the ECU (1) is an engine subsystem (4), which comprises a plurality of fuel injectors (5). The output module (2) of the ECU (1) is connected to the injectors (5) via a drive line (6). The ECU (1) operates the injectors (5) according to a drive signal (7), which is calculated by the main micro (10). The drive signal (7), which comprises a series of injector drive pulses, is communicated to the injectors (5) via the output module (2) and the drive line (6). As shown in Figure 1, the ESM (3) receives a feedback signal (8) from the output module (2) corresponding to the drive signal (7) output by the output module (2).

[0006] The ESM (3) performs a 'torque transform' on the drive signal (7) in order to estimate the torque delivered by the engine when operating in accordance with

the drive signal (7). The ESM (3) then performs a check to verify if the estimated delivered torque corresponds to the driver-requested torque. The driver-requested torque can be determined from monitoring the pedal position (9) of the driver's accelerator pedal. If the estimated delivered torque corresponds to the driver-requested torque, then no fault is reported. Conversely, if the estimated delivered torque does not correspond to the driver-requested torque, a fault is reported and the system is shut down.

[0007] Referring still to Figure 1, if a fault developed within the ECU (1), but downstream of the output module (2), for example at position "X", this could affect the actual drive signal communicated to the fuel injectors (5), and would consequently affect the actual torque delivery. However, the ESM (3) would not detect this fault. This is because the ESM (3) receives its feedback from the output module (2), which is upstream of the fault at position "X", and hence the fault would not be reflected in the feedback signal (8) provided to the ESM (3). Similarly, this system would not detect mechanical faults occurring downstream of the ECU (3), for example faults occurring in the engine subsystem (4), which could also affect the actual torque delivered by the engine.

[0008] Against this background, the present invention aims to provide an improved control and monitoring system that increases vehicle availability in the event of a fault developing in the main micro, and which is capable of detecting a wider range of faults than the prior art system described above.

Summary of the invention

[0009] According to the present invention there is provided a vehicle engine control system comprising: a main microprocessor for controlling the vehicle engine; and a monitoring microprocessor for monitoring the correct operation of the main microprocessor; the monitoring microprocessor being configured to receive a first signal indicative of a driver command, and a second signal indicative of an actual engine output parameter, wherein, in the event that a fault is detected in the main microprocessor:

- (i) the monitoring microprocessor is configured to determine from the first and second signals if the actual engine output parameter is within a predefined acceptable operating envelope, and
- (ii) the main microprocessor is allowed to continue to operate the vehicle engine provided that the actual engine output parameter is within the acceptable operating envelope.

[0010] The monitoring microprocessor may be configured to intervene in order to bring the actual engine output parameter to within the acceptable operating envelope in the event that the acceptable operating envelope is exceeded. To this end, the monitoring micro may disable

one or more fuel injectors from an injector drive circuit of the vehicle engine. Alternatively or additionally, the monitoring microprocessor may be configured to intervene by reducing fuel pressure in a common rail supplying one or more fuel injectors of the vehicle engine.

[0011] Advantageously, the monitoring microprocessor may be configured to receive a brake switch signal indicative of the driver applying the vehicle brakes. The monitoring microprocessor may be configured to intervene to reduce the engine speed on receiving the brake switch signal. Preferably, the monitoring microprocessor is configured to reduce the engine speed to an engine idle speed immediately on receiving the brake switch signal.

[0012] The first signal may be indicative of the position of a driver accelerator pedal. The second signal may be indicative of the rotational speed of the vehicle engine, cylinder pressure or vehicle acceleration. The second signal may be sampled on an output side of the vehicle engine.

[0013] The system may be configured to enter a limp-home mode on detection of a fault associated with the main microprocessor. In the limp-home mode, the vehicle engine may be operated according to an engine speed control model. The set point for the engine speed control model may be replicated in both the main microprocessor and the monitoring microprocessor. The monitoring microprocessor may be operable to control the vehicle engine in accordance with the limp-home mode by utilising the first and second signals in the event of a failure of the main microprocessor.

Brief description of the drawings

[0014] Figure 1, which is a schematic representation indicating where feedback signals are taken in a typical prior art control and monitoring system, has already been described above by way of background to the present invention.

[0015] The invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 2 is a block diagram of a control and monitoring system according to an embodiment of the present invention;

Figure 3 is a flow chart showing the process flow of the system of Figure 2;

Figure 4 is a graph showing an engine-speed pedal map utilised in the system of Figures 2 and 3; and

Figure 5 is a schematic representation of the system of Figures 2 to 4, illustrating where feedback signals are taken.

Detailed description

[0016] A control and monitoring system is shown schematically in Figure 2. The system comprises a main micro 10 and a monitoring micro 12. The main micro 10 is configured to control an injector drive circuit, in which a plurality of fuel injectors 14 are connected. Whilst not shown in Figure 1, the injectors 14 are connected in respective parallel branches of the injector drive circuit, between high and low voltage rails. Each parallel branch includes a switch (not shown) for enabling and disabling the respective injector 14 in that branch from the injector drive circuit; these switches are provided on the low-voltage side of the injectors 14, and are referred to collectively herein as the "low side arbitration logic" 16.

[0017] The monitoring micro 12 is configured to monitor the correct operation of the main micro 10, and is connected on the low voltage side of the injectors 14. The monitoring micro 12 has the capability to control the injectors 14 via the low side arbitration logic 16 should this be required in the event of a fault developing in the main micro 10 or otherwise in the event of a main micro failure.

[0018] The monitoring micro 12 is configured to receive three feedback signals: (i) engine speed 18; (ii) pedal position 20; and (iii) brake switch 22. The engine speed 18 refers to the actual, real-time, rotational speed of the vehicle engine, and is obtained via a suitable engine speed sensor known in the art. The pedal position 20 refers to the position of the driver's accelerator pedal, and is indicative of the real-time driver-demanded torque; the pedal position may be monitored by any suitable pedal-position sensing means known in the art. The brake switch 22 relates to the vehicle brakes, and this signal informs the monitoring micro 12 when the driver is applying the brakes; any suitable monitoring means known in the art may be employed for this purpose, for example a suitable sensor configured to detect when the brake pedal is pressed.

[0019] Whilst not shown in Figure 2, the main micro 10 also receives the three signals 18, 20 and 22. However, providing these signals to the monitoring micro 12 independently from the main micro 10 gives the monitoring micro 12 the capability to control the engine in the event of a fault, as described in further detail later.

[0020] Operation of the system in the event of a fault occurring in the main micro 10 will now be described with reference to Figure 3. Referring to Figure 3, at Step A1 the monitoring micro 12 detects the presence of a fault or error in the main micro 10. In order to detect the fault/error, the monitoring micro 12 may perform algorithmic checks on the main micro 10 to confirm that the main micro 10 is programming correctly, and/or the monitoring micro 12 may perform time-based checks. Any number of standard techniques may be employed for detecting the presence of faults in the main micro 10, and these techniques would be readily apparent to person skilled in the art. In the interests of conciseness, examples of

suitable monitoring techniques are not discussed in detail herein because the present invention is concerned with the action that is taken once a fault has been detected, and not with the detection of faults per se. However, it should be noted that a main micro fault may be detected initially by the main micro's onboard diagnostics rather than by the monitoring micro 12, as indicated at Step B1 in Figure 3.

[0021] Still referring to Figure 3, following the detection of a fault in the main micro 10 at Step A1, the monitoring micro 12 reports to the main micro 10 that a fault has been detected (Step A2), and the process flow of Figure 3 continues to Step A3 as described below. If the main micro fault is detected by the main micro's onboard diagnostics (Step B1), then the monitoring micro 12 is not required to report the fault, and the process flow of Figure 3 continues directly to Step A3.

[0022] At Step A3, the main micro 10 enters a "limp home" mode in response to receiving the fault report from the monitoring micro 12 or in response to a fault being detected by the onboard diagnostics. The limp-home mode is known, and consists essentially of the main micro 10 controlling the engine according to a reduced-power regime. This allows the driver to continue to drive the vehicle in the event of a fault, so that the vehicle can be driven safely off the road, or to a service centre where the fault can be repaired. It is important to note that, whilst it may be known to enter a limp-home mode when a vehicle develops certain faults, it is not known in the prior art to enter a limp-home mode when faults are detected in the main micro 10. As mentioned in the introduction, the default action in the prior art on detection of faults in the main micro 10 is to shut down the system, which results in an immediate loss of power and hence an immediate loss of vehicle availability.

[0023] In the limp home mode (Step A3), the main micro 10 operates the engine according to an engine speed control model, the set point of which is defined by a pedal map duplicated in both the main micro 10 and the monitoring micro 12. An example of a pedal map is shown in Figure 4. Referring to Figure 4, the x-axis represents driver pedal position, whilst the y-axis represents engine speed. At 0 % pedal, i.e. when the driver is not pressing the accelerator pedal, the target engine speed is set at 700 rpm (the idle speed). At 100 % pedal, i.e. when the driver presses the accelerator pedal to its maximum extent, the target engine speed is limited to 2000 rpm. In this example, a linear increase in engine speed is defined between these two extreme pedal positions. However, it will be appreciated that a non-linear characteristic could be defined in other examples.

[0024] Returning to Figure 3, whilst the main micro 10 controls the engine in the limp-home mode (Step A3), the monitoring micro 12 monitors whether the engine is running within a so-called "SAFE" operating envelope (Step A4), which in this example is an envelope of allowable engine speeds. This envelope is represented by the hatched region below the line in Figure 4, and is denoted

as "SAFE". Conversely, the region above the line in Figure 4 is denoted as "UNSAFE" and corresponds to engine speeds outside of the allowable envelope. The monitoring micro utilises the pedal and engine speed feedback signals (Figure 2) to determine if the engine is operating within the allowable operating envelope or outside of the allowable envelope.

[0025] If the monitoring micro at Step A4 (Figure 3) determines that the engine is operating within the allowable operating envelope (SAFE - Figure 4), then the monitoring micro 12 allows the main micro 10 to continue to operate the engine in the limp home mode, i.e. the process flow in Figure 3 returns to Step A3 and the monitoring micro 12 continues to check that the allowed operating envelope (SAFE - Figure 4) is respected. Therefore, even though a fault has been detected in the main micro 10, vehicle availability is maintained because the monitoring micro 12 has confirmed that the actual torque experienced by the driver does not exceed the allowable driver-demanded torque as defined in the engine speed control model. Consequently, the driver is able to continue to drive the vehicle to safety in the event of a main micro fault.

[0026] However, if at Step A4 (Figure 3) the monitoring micro 12 detects that the engine is operating outside of the allowable operating envelope (UNSAFE - Figure 4), then the monitoring micro 12 intervenes (Step A6) to reduce the engine speed as described in further detail below. Intervention is required because the UNSAFE region of Figure 4 indicates that the actual torque is greater than the driver-demanded torque.

[0027] At Step A6, if the engine speed exceeds the allowable operating envelope, then the monitoring micro intervenes to reduce the engine speed to within the allowed operating envelope (SAFE region in Figure 4). To achieve this, the monitoring micro utilises the arbitration logic (Figure 2) on the low side of the injectors to disable one or more of the injectors. Whilst not shown in the drawings, the monitoring micro may also be configured to control fuel pressure, for example in a common rail supplying the injectors. In such a configuration, the monitoring micro could intervene by reducing the fuel pressure in the event that the allowable engine speed envelope is exceeded to bring the engine speed back into the SAFE region of Figure 4.

[0028] In addition to ensuring that the allowable operating envelope is respected whilst the main micro 10 operates the limp home mode, the monitoring micro 12 simultaneously monitors the brake switch (Step A5 in Figure 3). If the monitoring micro 12 detects that the driver is applying the brake, then it will intervene at Step A6 (either via the arbitration logic or by reducing rail pressure) to bring the engine speed immediately down to the idle speed of 700 rpm; this is irrespective of the current (accelerator) pedal position. This intervention provides an additional level of safety to the system, and ensures safe operation even in the event of an accelerator pedal failure, or if the monitoring micro 12 receives an errone-

ous pedal position signal for another reason.

[0029] For comparison purposes with the prior art system shown in Figure 1, the feedback signals that are provided to the monitoring micro 12 in the present system are illustrated schematically in Figure 5. Referring to Figure 5, there is shown an ECU 30 comprising the main micro 10 and the monitoring micro 12. External to the ECU 30 is the engine subsystem 32, which includes the fuel injectors 34. An output module 36 of the ECU 30 communicates with the fuel injectors 34 via a control line 38. The output module 36 sends injector drive pulses 40 to the injectors 34 to control the injection of fuel. The monitoring micro 12 receives three feedback signals, i.e. the engine speed signal 18, the pedal position signal 20, and the brake switch signal 22.

[0030] Notably, in the present system the monitoring micro 12 receives feedback from the output side of the engine subsystem 32. In this example, that feedback is the sampled engine speed 18, which is indicative of the actual behaviour of the engine experienced by the driver. This is in contrast to the prior art, which takes its feedback from the input side of the engine subsystem (see Figure 1), and hence is only indicative of target or predicted parameters and thus provides no indication of the actual conditions experienced by the driver. Whereas the prior art system of Figure 1 would not detect faults occurring downstream of the output module of the ECU, the system shown in Figure 5 is able to detect a wider range of faults, including faults occurring downstream of the output module (36) that may affect actual torque delivery.

[0031] It is clear from the above description that the present system increases vehicle availability in the event of a fault developing in the main micro 10. In summary, this is achieved by allowing the main micro 10 to continue to operate within a predefined operating envelope that has been deemed to be safe, with the monitoring micro 12 subsequently managing the failed state by intervening when required. Consequently, in the event of main micro failure, the driver is able to continue to drive the vehicle to safety or to a service centre where the fault can be repaired.

[0032] It will be appreciated that many modifications may be made to the examples described above without departing from the scope of the present invention as defined in the following claims. For example, in addition to or instead of monitoring engine speed, the monitoring micro 12 may monitor other parameters such as cylinder pressure or vehicle acceleration in order to determine the actual engine output.

Claims

1. A vehicle engine control system comprising:

- a main microprocessor (10) for controlling the vehicle engine; and
- a monitoring microprocessor (12) for monitoring

the correct operation of the main microprocessor (10);

the monitoring microprocessor (12) being configured to receive a first signal (20) indicative of a driver command, and a second signal (18) indicative of an actual engine output parameter,

wherein, in the event that a fault is detected in the main microprocessor (10):

(i) the monitoring microprocessor (12) is configured to determine from the first and second signals (20, 18) if the actual engine output parameter is within a predefined acceptable operating envelope, and

(ii) the main microprocessor (10) is allowed to continue to operate the vehicle engine provided that the actual engine output parameter is within the acceptable operating envelope.

2. The system of Claim 1, wherein in the event that the acceptable operating envelope is exceeded, the monitoring microprocessor (12) is configured to intervene in order to bring the actual engine output parameter to within the acceptable operating envelope.
3. The system of Claim 2, wherein the monitoring microprocessor (12) is configured to intervene by disabling one or more fuel injectors from an injector drive circuit of the vehicle engine.
4. The system of Claim 2 or Claim 3, wherein the monitoring microprocessor (12) is configured to intervene by reducing fuel pressure in a common rail supplying one or more fuel injectors of the vehicle engine.
5. The system of any preceding claim, wherein the monitoring microprocessor (12) is configured to receive a brake switch signal (22) indicative of the driver applying the vehicle brakes.
6. The system of Claim 6, wherein the monitoring microprocessor (12) is configured to intervene to reduce the engine speed on receiving the brake switch signal (22).
7. The system of Claim 6, wherein the monitoring microprocessor (12) is configured to reduce the engine speed to an engine idle speed immediately on receiving the brake switch signal (22).
8. The system of any preceding claim, wherein the first signal (20) is indicative of the position of a driver accelerator pedal.
9. The system of any preceding claim, wherein the second signal (18) is indicative of the rotational speed

of the vehicle engine, cylinder pressure or vehicle acceleration.

- 10.** The system of any preceding claim, wherein the second signal (18) is sampled on an output side of the vehicle engine. 5
- 11.** The system of any preceding claim, wherein the system is configured to enter a limp-home mode on detection of a fault associated with the main microprocessor (10). 10
- 12.** The system of Claim 11, wherein the vehicle engine is operated according to an engine speed control model in the limp-home mode. 15
- 13.** The system of Claim 12, wherein the set point for the engine speed control model is replicated in both the main microprocessor (10) and the monitoring microprocessor (12). 20
- 14.** The system of Claim 13, wherein the monitoring microprocessor (12) is operable to control the vehicle engine in accordance with the limp-home mode by utilising the first and second signals in the event of a failure of the main microprocessor (10). 25

30

35

40

45

50

55

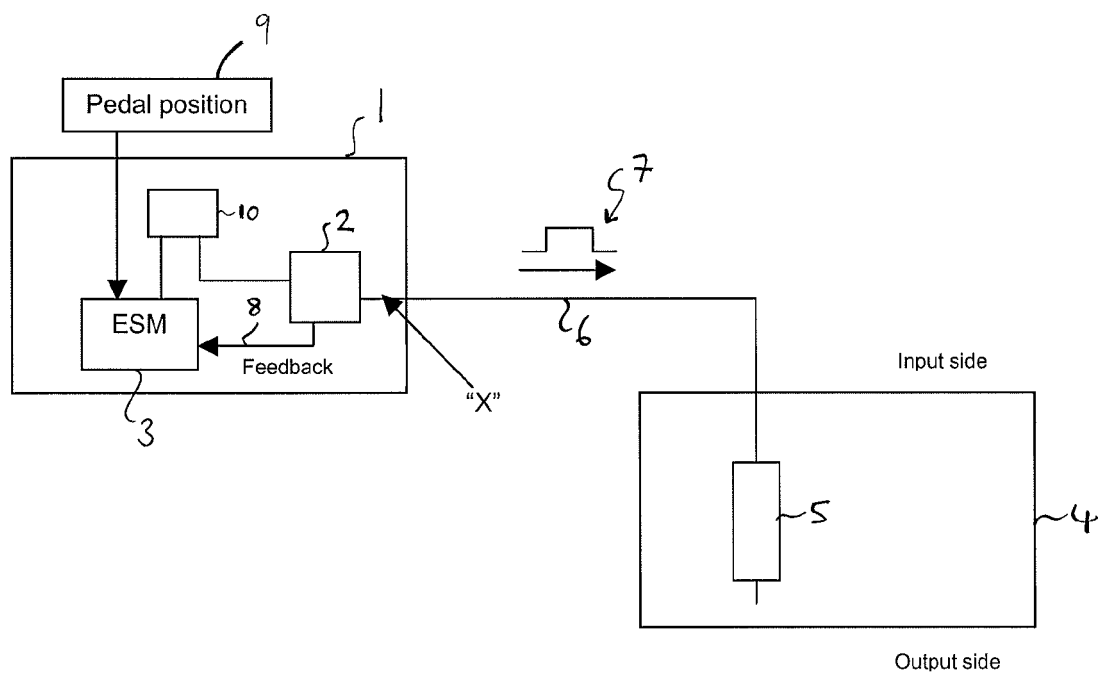


Fig. 1

[PRIOR ART]

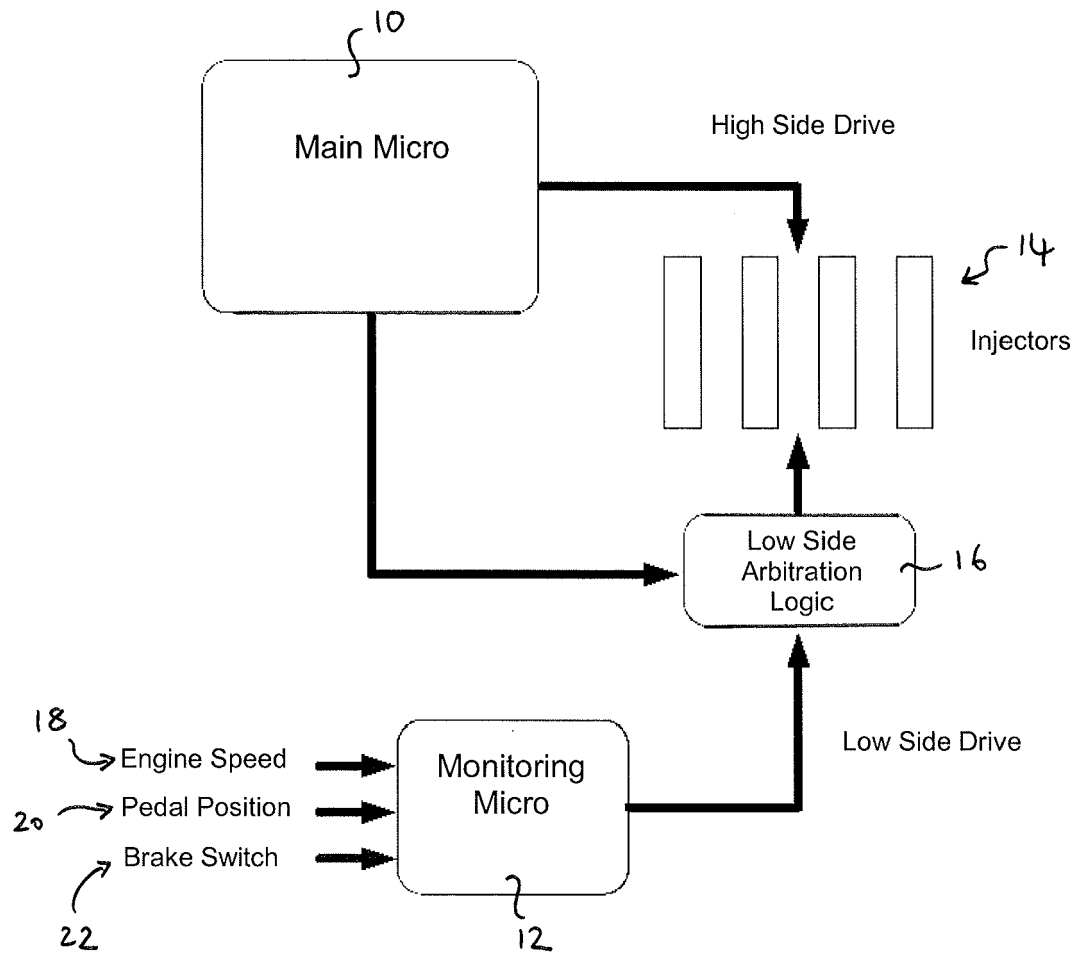


Fig. 2

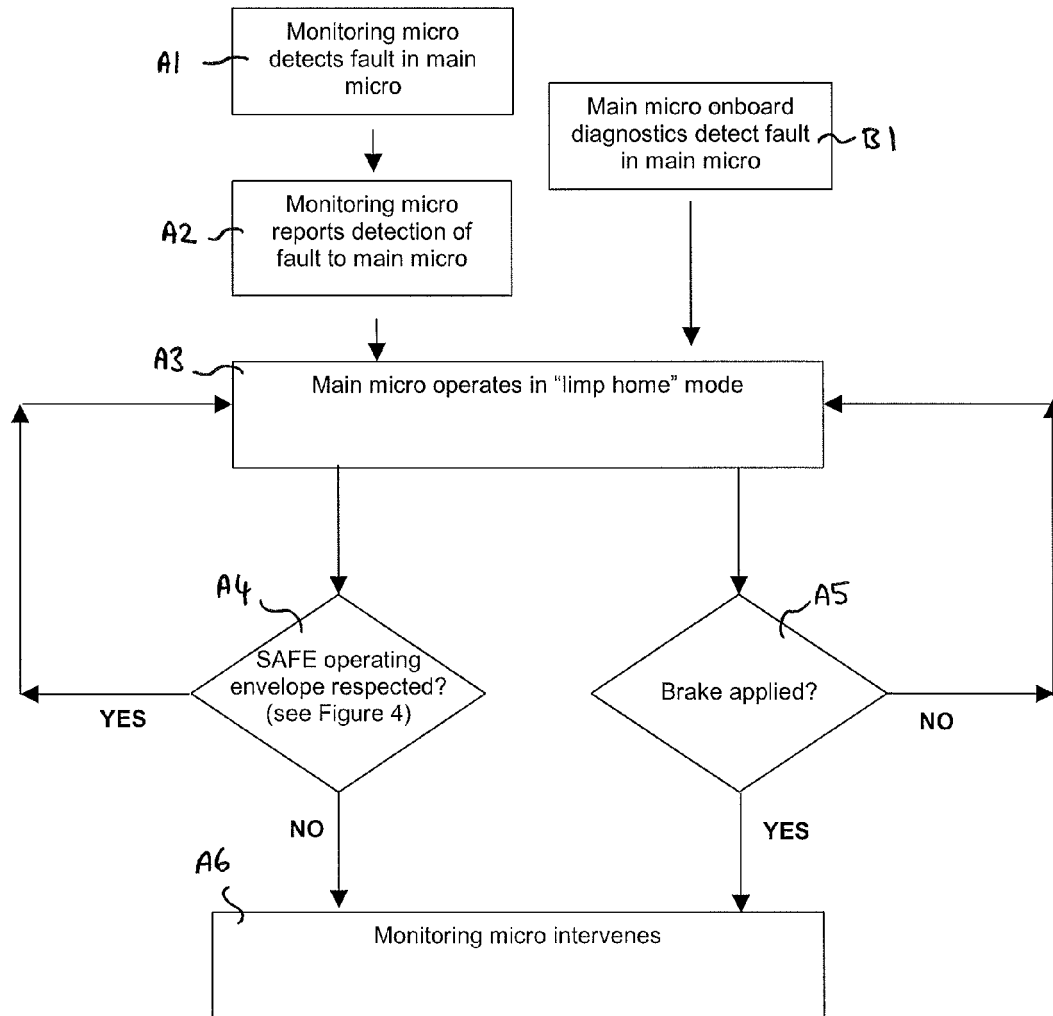


Fig. 3

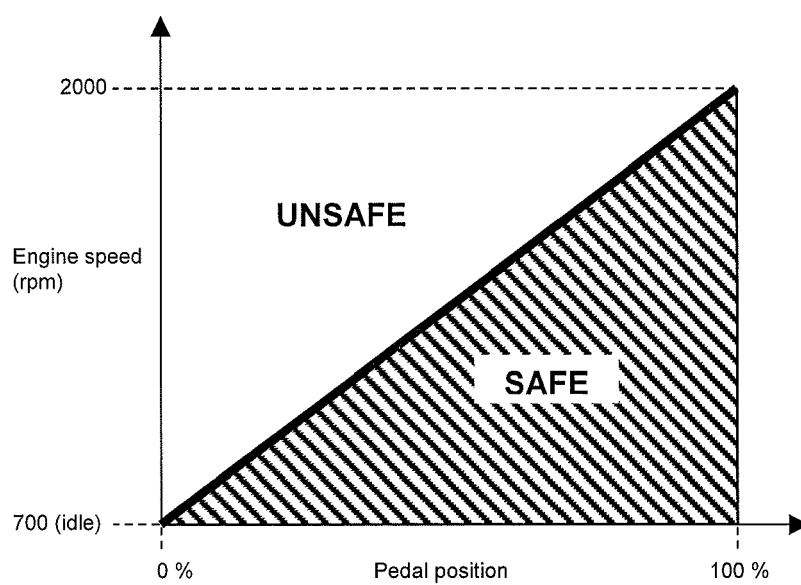


Fig. 4

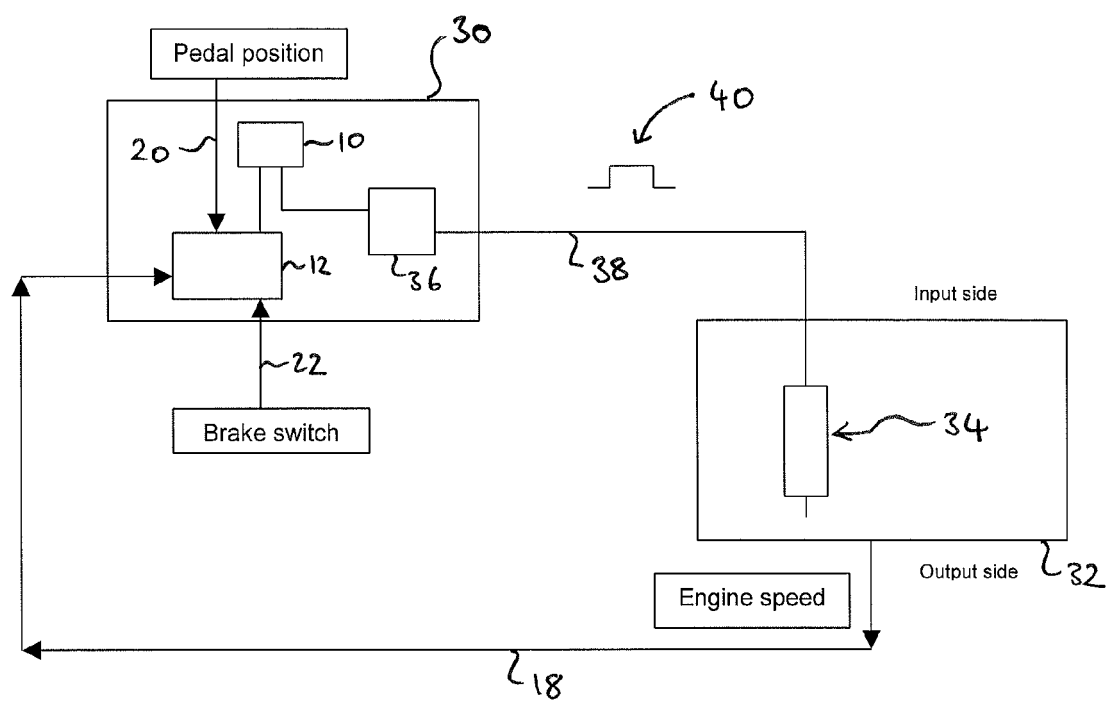


Fig. 5



EUROPEAN SEARCH REPORT

Application Number
EP 09 16 3596

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	JP 2003 155954 A (DENSO CORP) 30 May 2003 (2003-05-30)	1-4,8-14	INV. F02D41/22 F02D41/26
Y	* abstract; figure 3 * * paragraph [0016] * -----	5-7	
X	US 2003/144778 A1 (MIYANO HIDEMASA [JP] MIYANO HIDEMASA [JP] ET AL) 31 July 2003 (2003-07-31) * paragraphs [0019], [0020], [0021], [0024], [0025] * -----	1-3,9-12	
X	US 2003/088358 A1 (TAKEUCHI YOSHIHARU [JP] TAKEUCHI YOSHIHARU [JP] ET AL) 8 May 2003 (2003-05-08) * abstract; figure 4 * * paragraph [0031] * * paragraphs [0043] - [0045] * -----	1,8-11	
Y	DE 38 44 286 A1 (BOSCH GMBH ROBERT [DE]) 5 July 1990 (1990-07-05) * abstract * * column 5, paragraph 2 - column 6, paragraph 38 *	5-7	TECHNICAL FIELDS SEARCHED (IPC)
A	DE 38 04 012 A1 (DAIMLER BENZ AG [DE]) 24 August 1989 (1989-08-24) * abstract * * column 4, lines 2-47 * -----	5-7	F02D
The present search report has been drawn up for all claims			
Place of search The Hague		Date of completion of the search 2 December 2009	Examiner Röttger, Klaus
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	

1
EPO FORM 1503 03.82 (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 09 16 3596

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.

02-12-2009

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 2003155954 A	30-05-2003	JP 3883849 B2	21-02-2007
US 2003144778 A1	31-07-2003	DE 10255614 A1	07-08-2003
		JP 3967599 B2	29-08-2007
		JP 2003214233 A	30-07-2003
US 2003088358 A1	08-05-2003	JP 3883842 B2	21-02-2007
		JP 2003138981 A	14-05-2003
DE 3844286 A1	05-07-1990	FR 2641329 A1	06-07-1990
		GB 2226658 A	04-07-1990
		JP 2201055 A	09-08-1990
		JP 2999783 B2	17-01-2000
DE 3804012 A1	24-08-1989	NONE	