EUROPEAN PATENT SPECIFICATION

Date of publication and mention of the grant of the patent: 28.08.2002 Bulletin 2002/35

Application number: 95306432.6

Date of filing: 13.09.1995

Vehicular anti-theft system
Fahrzeug-Diebstahlsicherung
Dispositif antivol pour véhicule

Designated Contracting States: DE FR GB

19.06.1995 JP 15164295

Date of publication of application: 03.04.1996 Bulletin 1996/14

Divisional application: 99118681.8 / 0 967 130

Proprietor: DENSO CORPORATION
Kariya-City Aichi-Pref. 448 (JP)

Inventors:
- Hirata, Sanae
  Okazaki-City, Aichi-Pref. (JP)
- Hayakawa, Takahiro
  Okazaki-City, Aichi-Pref. (JP)

Representative: Dempster, Benjamin John Naftel et al
Withers & Rogers,
Goldings House,
2 Hays Lane
London SE1 2HW (GB)

References cited:
- EP-A- 0 607 455
- US-A- 4 246 639
- US-A- 4 583 176
- US-A- 4 646 008

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).
[0001] This application is based on and claims priorities of Japanese Patent Applications No. 6-229372 filed September 26, 1994 and No. 7-151642 filed June 19, 1995.

[0002] The present invention relates to an anti-theft system adopted for vehicles such as automobiles, motorcycles, boats and the like.

[0003] Hitherto, as a vehicular anti-theft system, there is one, as disclosed in Japanese Patent Laid-Open No. 64-56248 (US-A-4 965 460) for example, which keeps an engine which has once started running even if a supply of power voltage to an engine electronic control unit (hereinafter referred to as engine ECU) is unintentionally cut off, as long as a mechanical key is at a position of turning on an ignition switch, by maintaining the engine ECU on the ON state continuously by a security electronic control unit (hereinafter referred to as security ECU) by its holding circuit.

[0004] However, because the anti-theft system disclosed in Japanese Patent Laid-Open No. 64-56248 has the following problem as it is arranged so that after when the ignition switch is turned on, the security ECU sends an injection enabling signal for enabling to inject fuel to the engine to the engine ECU only once and the engine ECU shifts to a control of the injection of fuel after checking the transmission of the injection enabling signal from the security ECU by an initialization process along reset of its CPU.

[0005] That is, only a measure for preventing the stoppage of the engine during its operation is taken and no measure for a case when the CPU of the engine ECU is reset after the transmission of the injection enabling signal from the security ECU is taken in this system.

[0006] Accordingly, when the CPU of the engine ECU is reset when a power voltage of a car battery drops or is instantaneously cut off for example in activating a starter to start the engine, the injection enabling signal is not transmitted again as described above from the security ECU after when the power voltage has returned. Due to that, the injection of fuel is disabled. The same applies to a case when the CPU of the engine ECU is reset due to an abnormality thereof caused by an overrun of its function for example.

[0007] Further, as disclosed in Japanese Patent Laid-Open No. 3-32962, there is a vehicular anti-theft system which is arranged so that a function of an engine ignition system is stopped when a theft is detected and so that the function of ignition system is not stopped to hence keep running the engine once started when a circuit for detecting an operative state of the engine has detected the operative state of the engine.

[0008] The vehicular anti-theft system disclosed in Japanese Patent Laid-Open No. 3-32962 has a problem that the engine ignition system is also cut off in addition to the problem similar to the case described above.

[0009] EP-A-0354102 discloses, according to the preamble of claim 1, a vehicular anti-theft system in which a code signal is transmitted from a microprocessor to a unit to control engine injection. The unit includes a further microprocessor and a memory for data storage. The further microprocessor is arranged to be reset.

[0010] Accordingly, it is an object of the present invention to solve the aforementioned problems by providing a vehicular anti-theft system which is arranged so that operation of an engine is maintained as it is even if a CPU of an engine control unit is reset for some reason during the operation of the vehicular engine.

[0011] According to a first aspect of the invention, there is provided a vehicular anti-theft system according to the pending claim 1. Accordingly, even if the CPU is reset again due to a drop or instant cut-off of a voltage supplied from a power source, the CPU can maintain, without being influenced by that, the starting of the engine and operation thereafter by utilizing the information stored in the storage means.

[0012] Preferably the CPU performs arithmetic operations so as to maintain starting of the engine, operation thereafter or inhibition of starting based on information stored in storage means even if it is reset again after transmission of a start enabling data or start inhibiting data. Accordingly, even if the CPU is reset again due to a drop or instant cut-off of a voltage supplied from a power source, the CPU can maintain, without being influenced by that, the starting of the engine, the operation thereafter or the inhibition of the starting by utilizing the information stored in the storage means.

[0013] Preferably, when the start enabling information is stored in the storage means before detected number of revolutions of engine speed detecting means reaches a start completing number of revolutions of the engine, the CPU can maintain the starting of the engine based on the stored start enabling information even if it is reset again due to a drop of the voltage supplied from the power source.

[0014] Preferably, the CPU can maintain the operation of the engine based on the stored start enabling data even if it is reset again by a cut-off of a voltage supplied from the power source after when the detected number of revolutions reached the start enabling data of the engine.

[0015] Preferably, when the pre-starting start enabling data of the engine is stored in the storage means as start enabling information before the detected number of revolutions of the engine speed detecting means reaches the start completing number of revolutions, the CPU can maintain the operation of the engine even if it is reset again due to a drop of the voltage supplied from the power source, without being influenced by that, based on the start enabling information of the pre-starting start enabling data. Further, when the post-starting start enabling data of the engine is stored in the storage means as start enabling information instead of the pre-starting start enabling data after when the detected number of revolutions has reached to the start
completing number of revolutions of the engine, the CPU can maintain the operation of the engine even if it is reset again by a cut-off of the voltage supplied from the power source Ba based on the start enabling information of the post-starting start enabling data.

More preferably, the pre-starting start enabling data, post-starting start enabling data and start inhibiting data are composed respectively of a value of predetermined digits and a part of at least two digits of the start inhibiting data is different from that of the pre-starting start enabling data and the post-starting start enabling data. Thereby, even if noise or the like which is generated when the engine rotates at high-speed is produced, no change which otherwise takes place among the start inhibiting data and the pre-starting start enabling data or the post-starting start enabling data that they coincide from each other will not take place. As a result, the engine will not be erroneously started or its operation will not be erroneously inhibited.

Preferably, the storage means is a non-volatile memory, and the data stored in the storage means is continuously stored as it is even when the voltage supplied from the power source is cut off. Preferably, when the pre-starting start enabling data of the engine is stored in the storage means as start enabling information before the detected number of revolutions of the engine speed detecting means reaches the start completing number of revolutions, the CPU can maintain the operation of the engine even if it is reset again due to a drop of the voltage supplied from the power source, without being influenced by that, based on the start enabling information of the pre-starting start enabling data. Further, because the storage means stores the post-starting start enabling data of the engine as start enabling information instead of the pre-starting start enabling data when the detected number of revolutions has reached to the start completing number of revolutions of the engine, the CPU can maintain the operation of the engine even if it is reset again as the voltage supplied from the power source is cut off based on the start enabling information of the post-starting start enabling data. released, a third party who tries to start the engine illegitimately cannot start the engine thereafter. As a result, the engine can be inhibited from being illegitimately started.

A second aspect of the invention, is to provide a method of operating an engine according to the pending method claim 12.

In the accompanying drawings:

FIG. 1 is a schematic structural view of a whole circuit showing a embodiment of the present invention;
FIG. 2 is a flowchart of a security program executed by a CPU of a security ECU in FIG. 1;
FIG. 3 shows a part of a flowchart of an engine control program executed by a CPU of an engine ECU in FIG. 1;
FIG. 4 shows another part of the flowchart of the engine control program executed by the CPU of the engine ECU in FIG. 1;
FIG. 5 shows a further part of the flowchart of the engine control program executed by the CPU of the engine ECU in FIG. 1;
FIG. 6 shows a flowchart of an interrupt control program executed by the CPU of the engine ECU in FIG. 1;
FIG. 7 is a table showing contents of injection enabling data before starting, injection enabling data after starting and injection inhibit data;
FIGs. 8A to 8G are time charts showing operations of the first embodiment shown in FIG. 1.

The present invention will be described in detail with reference to the presently preferred embodiment shown in the accompanying drawings.

The preferred embodiment of the present invention will be explained below with reference to FIGs. 1 through 8G.

FIG. 1 schematically shows a structure of a whole circuit of a vehicular anti-theft system to which the present invention is applied.

In FIG. 1, an ignition key 1 is equipped with a memory 1a for storing a predetermined password code and an ignition key cylinder 2 is equipped with a reader (not shown) for reading this password code.

The anti-theft system includes a security ECU 20 which is connected to a door key switch 10a, an ignition switch 10b and the ignition key cylinder 2 of a vehicle. The door key switch 10a is turned on when a lock of the door of the vehicle is released by inserting a door key to a door key cylinder lock and by turning it.

When the ignition key 1 is inserted to the ignition key cylinder 2 and is turned, the ignition switch 10b turns on, supplying a power voltage (hereinafter referred to as +B voltage) from a car battery Ba to the security ECU 20, an engine ECU 30 and a starter 40 described later.

The security ECU 20 is equipped with a microcomputer 21 comprising a CPU 21a, a timer 21b, a ROM 21c, a RAM (not shown), and the like.

A password code is stored in the ROM 21c and the CPU 21a collates the password code within the key read by the ignition key cylinder 2 with the password code within the ROM 21c to determine whether the key inserted to the ignition key cylinder 2 is a legitimate or a valid key or not.

The CPU 21a is set by +B voltage supplied from the battery Ba via the ignition switch 10b and executes a security program in accordance with a flowchart shown in FIG. 2 described later. During the execution, an arithmetic processing for enabling or inhibiting injection of fuel to the engine and an arithmetic processing for enabling an activation of the starter 40 are performed on condition that the both the door key switch 10a and the ignition switch 10b are turned on. The timer 21b...
The engine ECU 30 has a serial input circuit 31 which receives signals transmitted from the CPU 21a of the security ECU 20 and outputs them to a microcomputer 32.

The microcomputer 32 comprises a CPU 32a, a timer 32b, a ROM (not shown), a RAM (not shown) and the like. The CPU 32a is reset when it receives a constant-voltage of 5 V from a voltage stabilizing circuit (VSC) 36 and executes an engine control program in accordance with flowcharts shown in FIGs. 3 through 5 described later as well as an interrupt control program in accordance with a flowchart shown in FIG. 6 described later.

During the execution of the engine control program, a number of revolutions or rotation speed Ne of the engine is calculated on the basis of pulse signals sequentially generated from a pulse sensor 33 per 30° of angle of revolution of the engine. Further, a process for writing/reading data to/from a backup RAM 34, a process for rewriting data and a process for enabling or inhibiting injection of fuel are carried out.

Meanwhile, during the execution of the interrupt control program, a process for starting injection of fuel is selectively carried out. The timer 32b starts to time at the same time when the CPU 32a is reset. It is to be noted that the voltage stabilizing circuit 36 generates the above-mentioned constant-voltage by receiving +B voltage from the battery Ba via the ignition switch 10b.

The B/U RAM 34 always receives +B voltage from the battery Ba to be put into a writable/readable state. Data from the CPU 32a is written into the B/U RAM 34 and is held as it is even when +B voltage from the battery Ba is cut off. A driving transistor 35 is turned on based on injection data from the CPU 32a and drives a fuel injector 50. By being driven by the transistor 35, the fuel injector 50 injects a predetermined amount of fuel to the engine.

The starter 40 has a magnet switch 41. The magnet switch 41 is driven by a coil 41a thereof by receiving a starter enabling signal from the CPU 21a of the security ECU 20 and turns on a normally opened switch 41b. A starter motor 42 turns by receiving +B voltage from the battery Ba via the switch 41b and a starter switch 10c and keeps the engine in a cranking state. The starter switch 10c turns on when the ignition key 1 is turned within the ignition key cylinder 2 when the ignition switch 10b is ON.

Operations of the embodiment constructed as described above will be explained below.

It is assumed that +B voltage is supplied from the battery Ba to the security ECU 20, the engine ECU 30 and the starter 40 (see time t0 to t1 in FIGs. 8A to 8G showing time charts representing operations of the main components shown in FIG. 1).

Then, the CPU 21a is reset by +B voltage in the security ECU 20 and starts to execute the security program in accordance with the flowchart shown in FIG. 2. At the same time, the CPU 32a is reset by +B voltage in the engine ECU 30 and executes the engine control program in accordance with each flowchart shown in FIGs. 3 through 5. An interrupt process of the interrupt control program made by the CPU 21a is carried out per generation of the pulse signal from the pulse sensor 33 in accordance with the flowchart shown in FIG. 6.

Hereinbelow, each processing mode of the security ECU 20 and the engine ECU 30 will be explained separately.

[0040] The security program is executed by the CPU 21a based on the flowchart in FIG. 2, as follows.

[0041] At first, the timer 21b is reset and started at Step 101. Thereby, the timer 21b starts to time. Until when a timer value of the timer 21b reaches two seconds after the reset of the CPU 21a, the following processing is carried out.

[0042] In Step 102, it is determined to be NO based on the timer value of the timer 21b. Because the door lock of the vehicle has been released by the door key of the owner of the vehicle, it is determined to be YES in Step 103 if the door key switch 10a has been turned on.

Then, the password code within the ignition key 1 is collated with the password code within the ROM 21c as described before and it is determined to be YES in Step 104 if the both password codes coincide. Thus, it is determined that the door key switch 10a and the ignition switch 10b are both normally turned on.

[0043] After that, an injection enabling signal signaling that the fuel injector 50 is permitted to inject fuel to the engine is transmitted within two seconds from the CPU 21a to the engine ECU 30 in Step 105 (see times t0 to t1 in FIG. 8B). Then, a starter activation enabling signal signaling that the starter 40 is permitted to be activated is transmitted from the CPU 21a to the starter 40 in Step 107. This starter activation enabling signal is continuously transmitted thereafter until when the ignition switch 10b is turned off. Thereby, the coil 41a of the magnet switch 41 is continuously driven, holding the switch 41b in the ON state. As a result, the anti-theft system is put into an injection enabling mode by the security ECU 20.

[0044] Meanwhile, when the door lock is forcibly released somehow, not by the valid door key of the owner of the vehicle, or when a state equal to that the ignition switch 10b is ON is being realized somehow, not by the valid door key of the owner of the vehicle, or when a state equal to that the ignition switch 10b is ON is being realized somehow, the valid door key of the owner of the vehicle is not validly inserted into the key cylinder, or when a state equal to that the ignition switch 10b is turned on is being forcibly short-circuiting each wire connected to both terminals of the ignition switch 10b for example, it is determined to be NO in Step 103 or 104 since the password code is not confirmed to coincide.

[0045] In such case, determining that the door lock of
Due to that, it is determined to be NO in Step 204 and the present stage, the number of revolutions Ne is zero.

After when the timer value of the timer 21b reaches two seconds, it is determined to be YES in Step 202 and the security program returns to Step 202. This means that the transmission of the injection enabling signal or the injection inhibiting signal from the security ECU 20 is limited within the time until when the timer value of the timer 21b reaches two seconds.

1) Processing mode until when timer value of timer 32b reaches two seconds

When the CPU 32a is reset as described above, the timer 32b is reset and starts to time in Step 200 of the flowchart in FIG. 3.

It is to be noted that the flowchart in FIG. 3 is repeatedly executed after the reset of the CPU 32a (after the reset (power-on reset) as the ignition switch 10b is turned on in starting the engine or after the reset made by a watch dog timer when an overrun of the CPU 32a is detected). However, both Steps 200 and 201 represent an initialization process executed only after the above-mentioned reset.

Because the injection enabling signal is transmitted from the security ECU 20 within two seconds after the reset of the CPU 21a as described above, a process for determining the injection enabling signal transmitted from the security ECU 20 is performed and other processes are carried out in conjunction with that as follows until when the timer value of the timer 32b reaches two seconds after the reset of the CPU 32a.

At first, an injection enabling flag described later is reset as XLSECRI = 0 in Step 201. Next, it is determined to be YES in Step 202 because the timer value of the timer 32b is within two seconds. Then, a number of revolutions Ne of the engine is calculated based on the pulse signals from the pulse sensor 33 in Step 203.

Next, it is determined whether the number of revolutions or rotational speed Ne is more than 500 rpm or not in Step 204. 500 rpm is a number of revolutions which is lower than an idle number of revolutions of the engine and by which starting is completed without stopping the engine when the number of revolutions Ne increases up to 500 rpm through the activation of the starter 40.

If the starter switch 10c is not turned on yet at the present stage, the number of revolutions Ne is zero. Due to that, it is determined to be NO in Step 204 and it is determined in Step 205 whether data D5C (hereinafter referred to as pre-starting injection enabling data D5C) indicating that fuel may be injected to the engine prior to its start is written in the B/U RAM 34 or not. The pre-starting injection enabling data D5C shows one byte of predetermined value (01011100) as shown in FIG. 7.

It is to be noted that FIG. 7 shows contents of data D76 (hereinafter referred to as post-starting injection enabling data D76) enabling to inject fuel to the engine after its start and data DA3 (hereinafter referred to as injection inhibiting data DA3) indicating that the injection of fuel to the data is inhibited.

Then, if the pre-starting injection enabling data D5C has not been written in the B/U RAM 34, it is determined to be NO in Step 205. If the injection enabling signal has been transmitted from the CPU 21a as described before at this time, the injection enabling signal is input to the CPU 32a via the serial input circuit 31.

Accordingly, it is determined to be YES in Step 206 determining that the injection enabling signal exists, and the pre-starting injection enabling data D5C is written into the B/U RAM 34 at the trailing edge of the injection enabling signal in Step 210 (see time t1 in FIG. 8E) and the injection enabling flag is set as XLSECRI = 1 in Step 210. Thereby, the engine ECU 30 can hold the injection enabling mode given initially by the security ECU 20 even if the injection enabling signal is not transmitted from the CPU 21a any more.

When the processes going through each Step of 203 through 206 and Step 210 of the flowchart in FIG. 3 are completed as described above, it is determined in Step 212 of the flowchart in FIG. 4 whether more than two seconds has passed since the reset of the CPU 32a.

Because the timer value of the timer 32b has not reached two seconds at this stage, it is determined to be NO in Step 212. It is determined to be NO also in Step 216 of the flowchart in FIG. 4 for the same reason.

When the starter switch 10c is turned on at such stage, the starter motor 42 is activated by receiving +B voltage from the battery Ba via the ignition switch 10b, the switch 41b and the starter switch 10c, because the switch 41b of the magnet switch 41 is kept in the ON state, and keeps the engine in the cranking state (see time between t1 and t3 in FIG. 8C).

Meanwhile, as the engine is put into the cranking state, the pulse sensor 33 generates pulse signals sequentially. Then, the CPU 32a repeatedly executes the interrupt control program per generation of the pulse signal in accordance with the flowchart in FIG. 6.

During each of this execution, it is determined whether the injection enabling flag XLSECRI = 1 or not in Step 301. Because it has been set as XLSECRI = 1 (see Step 210), it is determined to be YES in Step 301 and a process for starting to inject fuel to the engine is performed in Step 302, outputting an injection starting output signal to the driving transistor 35.

Due to that, the driving transistor 35 turns on, thus driving the fuel injector 50. Thereby, the fuel injector...
50 starts to inject a predetermined amount of fuel to the engine.

[0060] When the engine control program reaches again to Step 204 of the flowchart in FIG. 3 in such state, it is determined whether the number of revolutions $N_e$ is more than 500 rpm or not. If the number of revolutions $N_e$ has not reached 500 rpm in the engine cranking state described above, it is determined to be NO in Step 204. Then, because the pre-starting injection enabling data D5C has been already written into the B/U RAM 34 (see Step 210), it is determined to be YES in Step 205. Because the pulse signals have been already generated from the pulse sensor 33 at this stage, it is determined to be YES in Step 209 and the process in Step 210 is performed in the same manner described above.

[0061] Accordingly, although the process is executed from Step 200 again when $+B$ voltage drops as the starter 40 is activated as described above and the CPU 32a is reset again without resetting the CPU 21a (see time t2 in FIGs. 8F anf 8G), the engine ECU 30 can hold the injection enabling mode given initially by the security ECU 20 by the processes through each Step 204, 205, 209 and 210 even the injection enabling signal is not transmitted from the CPU 21a any more. Accordingly, the injection of fuel to the engine may be maintained by executing the interrupt control program in accordance with the flowchart in FIG. 6 in the engine cranking state.

[0062] It is to be noted that when there is no pulse signal from the pulse sensor 33 after the determination of YES in Step 205, a situation that the injection enabling mode is effected based on the post-starting injection enabling data D76 within the B/U RAM 34, even though the starter 40 is inhibited from activating, is prevented by inhibiting the shift from Step 209 to Step 210.

[0063] After that, when the number of revolutions $N_e$ increases more than 500 rpm (see time $t_3$ in FIG. 8D), it is determined to be YES in Step 204 in FIG. 3 and the same process as described before is carried out in Step 210.

[0064] In other words, that the number of revolutions $N_e$ exceeds 500 rpm means that the start of the engine has been completed before the timer value of the timer 32b reaches two seconds.

[0065] Because the starter 40 has stopped already at this stage, $+B$ voltage will not drop due to the activation of the starter 40 before the starting of the engine as described before.

[0066] Instead of that, an instant cut-off of $+B$ voltage may be caused due to an improper connection between the CPU 32a and the battery 3a after starting the engine. Then, even when only the CPU 32a is reset again without resetting the CPU 21a due to such instant cut-off of the $+B$ voltage, the engine ECU 30 can hold the injection enabling mode given initially by the security ECU 20 even if no injection enabling signal is transmitted again from the CPU 21a by the above-mentioned process in Step 210 carried out upon the determination of YES in Step 204.

[0067] As a result, the engine operative state after completing the starting may be held by maintaining the injection of fuel to the engine by executing the interrupt control program in accordance with the flowchart in FIG. 6.

2) Processing mode after when timer value of timer 32b has reached two seconds:

[0068] After when the timer value of the timer 32b has reached two seconds, i.e. when two seconds has passed since when the CPU 32a was initially reset, it is determined to be NO in Step 202 of the flowchart in FIG. 3. Succeedingly, it is determined to be YES in Step 211 if there is an injection enabling signal to be transmitted from the CPU 21a to the engine ECU 30 during the two seconds after the initial reset of the CPU 32a.

[0069] After that, when it is determined to be YES in Step 212 in FIG. 4 based on the timer value of the timer 32b, it is determined whether the number of revolutions $N_e$ is more than 500 rpm or not.

[0070] When the number of revolutions $N_e$ is more than 500 rpm, it is determined to be YES in Step 213 and it is determined in Step 214 whether the pre-starting injection enabling data D5C has been already written in the B/U RAM 34 or not. Because the pre-starting injection enabling data D5C has been already written in the B/U RAM 34 at this stage as described before (see Step 210), it is determined to be YES in Step 214.

[0071] Then in Step 215, the data to be written into the B/U RAM 34 is rewritten into the post-starting injection enabling data D76. It prevents an occurrence of a situation that the injection enabling mode is maintained by the process of each Step 205, 209 and 210 even when no injection enabling signal is transmitted again from the security ECU 20 when the ignition switch 10b is turned on again after it has been turned off when the data written into the B/U RAM 34 remains to be the pre-starting injection enabling data D5C.

[0072] The post-starting injection enabling data D76 represents one byte of predetermined value (01110110) as shown in FIG. 7 and is different as compared with the pre-starting injection enabling data D5C at each bit of the second, fourth and sixth digits. That is, a difference of three bits is provided between the pre-starting injection enabling data D5C and the post-starting injection enabling data D76.

[0073] It is to be noted that the engine control program is executed shifting from Step 215 to the flowchart in FIG. 5. The same applies to the case when it is determined to be NO in any one of each Step 212, 213 and 214.

[0074] When the timer value of the timer 32b has reached two seconds and it is determined to be YES in Step 216 in FIG. 5, it determined in Step 217 whether the number of revolutions $N_e$ is more than 500 rpm or not. When the number of revolutions $N_e$ is more than
500 rpm, it is determined to be YES in Step 217 and it is determined in Step 218 whether the data written into the B/U RAM 34 is the post-starting injection enabling data D76 or not.

[0075] Because the data written into the B/U RAM 34 is the post-starting injection enabling data D76 at this stage (see Step 215), it is determined to be YES in Step 218 and the injection enabling flag is set again as XLSECRI = 1 in Step 219.

[0076] Thereby, the engine ECU 30 can maintain the fuel injection enabling mode given by the security ECU 20 even if +B voltage is instantly cut off after when the timer value has reached second after starting the engine.

[0077] When the number of revolutions Ne is not more than 500 rpm on the other hand, it is determined to be NO in Step 217 and it is determined in Step 220 whether the data written into the B/U RAM 34 is the injection inhibiting data DA3 or not. Because the injection inhibiting data DA3 is not written into the B/U RAM 34 at this stage, it is determined to be NO in Step 220.

[0078] The injection inhibiting data DA3 represents one byte of predetermined value (10100011) as shown in FIG. 7. The injection inhibiting data DA3 is different from the post-starting injection enabling data D76 respectively at the first, third, fifth, seventh and eighth digits. Due to that, the injection inhibiting data DA3 has a difference of 5 bits from the post-starting injection enabling data D76.

[0079] Further, because the post-starting injection enabling data D76 has a difference of 3 bits from the pre-starting injection enabling data D5C as described before, a difference of 8 bits is given between the injection inhibiting data DA3 and the pre-starting injection enabling data D5C.

[0080] Accordingly, because of the bit difference between the post-starting injection enabling data D76 and the injection inhibiting data DA3, the post-starting injection enabling data D76 is not transformed to the injection inhibiting data DA3 due to bit transformation caused by noise produced when the engine rotates at high-speed, for example, thereby inhibiting the injection of fuel to the engine.

[0081] Further, even if the post-starting injection enabling data D76 is transformed into the injection inhibiting data DA3 due to the bit transformation, the data written into the B/U RAM 34 is corrected as the post-starting injection enabling data D76 by setting again as XLSECRI = 1 in Step 219 as described above.

[0082] Thereby, it allows to prevent the situation that the injection of the fuel to the engine is inhibited as described above from occurring more reliably. As a result, the injection of fuel to the engine is insured in the interrupt process in FIG. 6 thereafter.

3) Although the engine ECU 30 is allowed to maintain the injection enabling mode when +B voltage drops due to the activation of the starter 40 or when it drops due to the instant cut-off of +B voltage after the start of the engine in the processing mode of the engine ECU 30 in the injection enabling mode described above, the injection enabling mode may be insured based on the pre-starting injection enabling data D5C or post-starting injection enabling data D76 within the B/U RAM 34 even when the CPU 32a is returned to the normal condition after when it has been reset due to an abnormal operation such as an overrun thereof.

[0083] When the engine control program reaches Step 206 of the flowchart in FIG. 3, it is determined whether the injection enabling signal from the security ECU 20 exists or not similarly to the case described above. If the injection inhibiting signal is transmitted from the security ECU 20 at this time, it is determined to be NO in Step 206 and then determined to be YES in Step 207.

[0084] Then, the injection inhibiting data DA3 is written into the B/U RAM 34 and the injection enabling flag is reset as XLSECRI = 0 in Step 208. Thereby, the engine ECU 30 can maintain the injection inhibiting mode given from the security ECU 20 even no injection inhibiting signal is transmitted again from the CPU 21a when only the CPU 32a is reset again without resetting the CPU 21a as +B voltage drops due to its instant cut-off. Accordingly, even if the starter switch 10c is illegitimately turned on, the engine will not start.

[0085] When it is determined to be NO in Step 202 of the flowchart in FIG. 3 similarly to the case described above, it is determined to be YES in Step 211 if there is the injection inhibiting signal transmitted from the CPU 21a to the engine ECU 30 during two seconds since the initial reset of the CPU 32a.

[0086] Next, when it is determined to be YES in Step 212 in FIG. 4 similarly to the case of Step 202, it is determined to be NO in Step 213 because no pulse signal is generated from the pulse sensor 33.

[0087] After that, it is determined to NO also in Step 217 in FIG. 5 for the same reason. Then, it is determined in Step 220 whether data written into the B/U RAM 34 is the injection inhibiting data DA3 or not.

[0088] Because the injection inhibiting data DA3 has been written into the B/U RAM 34 at this stage (see Step 208), it is determined to be YES in Step 220 and the injection enabling flag is reset again as XLSECRI = 0 in Step 221.

[0089] Thereby, the engine ECU 30 can maintain the
fuel injection inhibiting mode given by the security ECU 20 even if +B voltage is instantly cut off after when the timer value of the timer 32b has reached two seconds after starting the engine.

[0090] In such case, because the bit difference as described before is given between the injection inhibiting data DA3 and the pre-starting injection enabling data D5C or the post-starting injection enabling data D76, the injection inhibiting data DA3 is not transformed to the pre-starting injection enabling data D5C or the post-starting injection enabling data D76 due to the bit transformation caused by noise or the like.

[0091] Further, even if the injection inhibiting data DA3 is transformed to the pre-starting injection enabling data D5C or the post-starting injection enabling data D76 due to the bit transformation, the data written into the B/U RAM 34 is corrected as the injection inhibiting data DA3 by resetting again as X$LSECR$ = 0 in Step 221 as described above. Due to that, a situation that the injection of fuel to the engine is erroneously permitted is more reliably prevented from occurring.

[0092] It is to be noted that when there is no signal from the CPU 21a during two seconds after when the CPU 32a has been initially reset, it is determined to be NO in Step 211 and the process in Step 208 is carried out in the same manner as described above.

[0093] In the embodiment, the post-starting injection enabling data D76, not the pre-starting injection enabling data D5C or the post-starting injection enabling data D76 due to the bit transformation, the data written into the B/U RAM 34 is rewritten from the pre-starting injection enabling data D5C to the post-starting injection enabling data D76. Accordingly, it allows to normally start the engine and to prevent the engine from being started by illegitimate manipulation even when +B voltage of the battery Ba drops as the starter is activated and the CPU 32a is reset. In other words, the following problem may be reliably prevented from occurring by rewriting the data written into the B/U RAM 34 from the pre-starting injection enabling data D5C to the post-starting injection enabling data D76.

[0094] In other words, the following problem may be prevented from occurring. That is, when the injection enabling signal is transmitted from the security ECU 20 to the engine ECU 30 after when the vehicle has been stopped by normally stopping the engine. Due to that, it is determined to be NO in Step 205 (see FIG. 3) based on the post-starting injection enabling data D76 even if +B voltage of the battery Ba is illegitimately supplied to the engine ECU 30 and the starter 40 during when the vehicle is stopped. Accordingly, the injection of fuel is not enabled, preventing the vehicle from being stolen.

[0095] Due to that, when +B voltage of the battery Ba is supplied illegitimately (e.g. by short-circuiting the battery Ba and a terminal of the ignition switch 10b on the side of security ECU 20) to the engine ECU 30 and the starter 40 in such state, the engine ECU 30 starts the engine regardless of the result of the collation of the password codes because the data written into the B/U RAM 34 is still the pre-starting injection enabling data D5C. However, according to the embodiment, such problem may be reliably prevented from occurring by rewriting the data written into the B/U RAM 34 from the pre-starting injection enabling data D5C to the post-starting injection enabling data D76 as described above.

[0096] Further, according to the first embodiment, a criterion of the number of revolutions Ne in Step 204 is set to be more than 500 rpm as described above. Due to that, when the number of revolutions Ne exceeds the number of revolutions for completing the engine start, the data written into the B/U RAM 34 is rewritten from the pre-starting injection enabling data D5C to the post-starting injection enabling data D76. Accordingly, it allows to normally start the engine and to prevent the engine from being started by illegitimate manipulation even when +B voltage of the battery Ba drops as the starter is activated and the CPU 32a is reset.

[0097] In other words, it allows to prevent the following problem from occurring. That is, if the criterion of the number of revolutions Ne in Step 204 is more than 2000 rpm and when the legitimate owner of the vehicle has started the engine and stops it before the number of revolutions Ne exceeds 2000 rpm, the data written into the B/U RAM 34 remains to be the pre-starting injection enabling data D5C.

[0098] Due to that, when +B voltage of the battery Ba is illegitimately supplied to the engine ECU 30 and the starter 40 in such state, the engine is illegitimately started after determining to be YES in Step 205. However, according to the first embodiment, such problem may be reliably prevented by setting the criterion of the number of revolutions Ne in Step 204 as more than 500 rpm as described above.

[0099] Meanwhile, if the criterion of the number of revolutions Ne in Step 204 is set to be more than 300 rpm (a number of revolutions lower than the number of revolutions for completing the engine start), although the engine will not be illegitimately started, the data written into the B/U RAM 34 is rewritten from the pre-starting injection enabling data D5C to the post-starting injection enabling data D76 before completing to start the engine.

[0100] Due to that, when the CPU 32a is reset when the starter is activated when the drop of +B voltage of the battery Ba is feared, the engine is disabled to start. However, according to the embodiment, such problem may be reliably prevented by setting the criterion of the number of revolutions Ne in Step 204 to be more than 500 rpm.

[0101] The present invention is not confined only to the embodiment described above. Rather, it may be realized by various variations as follows.

[0102] Although the case when the engine of the vehicle is a motor has been explained in the embodiment described above, the present invention may be applied and practiced even for an electric motor of an electric car, an engine of a motor-cycle and a boat whose driving source is a motor.
Although the case in which the present invention is applied to the fuel injection system and starter of the engine has been explained in the embodiment described above, the present invention may be applied and practiced not only to an engine ignition system, but also to the fuel injection system and the starter as well as the ignition system.

Although the case when the security ECU 20 has the CPU 21a has been explained in the embodiment described above, the present invention is not confined only to that and is applicable also to a case when the security ECU 20 does not have the CPU 21a.

Although the case wherein the engine is started by manipulating the ignition switch 10b and the starter switch 10c has been explained in the embodiment described above, the present invention is not confined only to that and is arranged so that the engine is started by a key-less entry system.

In the embodiment described above, the B/U RAM 34 may be a memory capable of backing up such as a DRAM or be a non-volatile memory.

Although the case when the engine start completing number of revolutions is 500 rpm has been explained in the embodiment described above, the present invention is not confined to that and it may be practiced by changing the start completing number of revolutions as necessary.

The present invention may be practiced by changing each value of the pre-starting injection enabling data D5C, the post-starting injection enabling data D76 and the injection inhibiting data DA3 described above in the embodiment adequately in a range in which either one value is not transformed to another value from each other by bit transformation.

Each step in each flowchart of the embodiment described above may be realized by a hard logic structure, respectively, as function executing means.

Although the case when the completion of engine start is determined by the number of revolutions Ne has been explained in the embodiment described above, the present invention may be practiced to determine the completion of engine start by a total number of times of ignition of the engine when the starter is off for example.

Further, the content stored in the storage means of the engine control ECU for preventing engine starting by an unauthorized person. That is, it is changed when the engine speed has reached 500 rpm after the turn on of the key switch. The storage content changing timing may be modified to such timing as when the starter once driven is stopped, the engine speed reaches the idling speed, when a pre-determined time lapses after the turning on of the ignition switch, when the engine speed falls to zero after stopping the vehicle, or when the main relay turns off after the turning off of the key switch. Thus, the timing to change the stored content in the memory stored at the time of engine starting operation may be made until the time the voltage supply from the power source to the engine control unit is stopped.

1. A vehicular anti-theft system comprising:

   a security unit (20) for transmitting first engine start enabling data when a vehicular engine is operated to be started;
   an engine control unit (30;30A) equipped with a CPU (32a) arranged to be reset by a voltage supplied from a power source (Ba) at the time of the starting operation and arranged to perform arithmetic operations for starting said engine based on said first start enabling data; and storage means (34) for storing second start enabling data (D5C) as start enabling information if said first start enabling data is transmitted to said engine control unit;

   wherein said CPU (32a) is arranged to perform arithmetic operations so as to maintain the starting of said engine and the operation thereafter based on said information stored in said storage means (34) even if it is reset again after the transmission of said start enabling data, characterised in that the second start enabling data (D5C) is changed to an engine start inhibiting signal (D76) before the vehicle has been stopped by normally stopping the engine.

2. The vehicular anti-theft system of claim 1, wherein:

   the security unit (20) is arranged to transmit engine start inhibiting data when said engine is illegitimately started;
   said CPU (32a) is arranged to be reset by said illegitimate starting operation and to perform arithmetic operations for inhibiting starting of said engine based on said start inhibiting data (DA3);
   the storage means (34) is arranged to store start inhibiting data as start inhibiting information, and;
   said CPU (32a) is arranged to perform arithmetic operations so as to maintain the starting of said engine, the operation thereafter and the inhibition of starting based on the information stored in said storage means (34) even if said CPU (32a) is reset again after the transmission of said start inhibiting data and start inhibiting data.

3. The vehicular anti-theft system of claim 1 or 2 further comprising:

   engine speed detecting means (33) for detect-
ing the number of revolutions of said engine per unit time,

wherein said CPU (32a) is arranged to perform arithmetic operations so as to maintain the starting of said engine based on said stored start enabling information even if it is reset again when said storage means (34) stores said start enabling information before said detected number of revolutions per unit time reaches a number sufficient to complete starting the engine.

4. The vehicular anti-theft system of claim 3,

wherein said CPU (32a) is arranged to perform arithmetic operations so as to maintain the operation of said engine even if it is reset again after said detected number of revolutions per unit time reaches the number sufficient to complete starting of the engine.

5. The vehicular anti-theft system of claim 1 or 2 further comprising:

   engine speed detecting means (33) for detecting the number of revolutions of said engine per unit time,

   wherein said CPU (32a) is arranged to maintain the starting of said engine based on said start enabling information of pre-starting start enabling data even if it is reset again when said storage means (34) stores said pre-starting start enabling data as said start enabling information before said detected number of revolutions per unit time reaches the number of revolutions of said engine, sufficient to complete starting,

   wherein said storage means (34) is arranged to store post-starting start enabling data of said engine as said start enabling information instead of said pre-starting start enabling data after said detected number of revolutions per unit time has reached the number of revolutions of said engine per unit time sufficient for starting, and

   wherein said CPU (32a) is arranged to perform arithmetic operations so as to maintain the operation of said engine even if it is reset again based on said start enabling information of said stored post-starting start enabling data.

6. The vehicular anti-theft system of claim 5,

   wherein said pre-starting start enabling data, post-starting start enabling data and start inhibiting data are composed respectively of a value of pre-determined digits and at least a part of two digits of said start inhibiting data is different from that of said pre-starting start enabling data and said post-starting start enabling data.

7. The vehicular anti-theft system of claim 6,

   wherein each value of pre-determined digits of said pre-starting start enabling data, post-starting start enabling data and start inhibiting data are composed respectively of a value of eight bits and said start inhibiting data has a difference of three bits from said post-starting start enabling data and has a difference of eight bits from said pre-starting start enabling data.

8. The vehicular anti-theft system of any preceding claim,

   wherein said storage means (34) is a non-volatile memory.

9. The vehicular anti-theft system of claim 1 or claim 2 further comprising:

   engine speed detecting means (33) for detecting the number of revolutions of said engine per unit time,

   wherein said CPU (32a) is arranged to maintain the starting of said engine based on the start enabling information of pre-starting start enabling data even if it is reset again when said storage means (34) stores said pre-starting start enabling data as said start enabling information before said detected number of revolutions reaches a number of revolutions of said engine per unit time sufficient to complete starting,

   wherein said storage means (34) stores post-starting start enabling data of said engine as said start enabling information instead of said pre-starting start enabling data after said detected number of revolutions per unit time has reached said number of revolutions of said engine per unit time sufficient for starting, and

   wherein said CPU (32a) performs arithmetic operations so as to maintain the operation of said engine even if it is reset again based on said start enabling information of said stored post-starting start enabling data.

10. The vehicular anti-theft system of any preceding claim,

   wherein said information stored in said storage means (34) at the time of starting said engine is arranged to be changed to another information to be stored in said storage means (34) during the time before the supply of voltage from said power source (Ba) to said engine control unit (30;30A) to stop the operation of said engine.

11. The vehicular anti-theft system of any one of claims 1 to 10, further comprising:

   data carrying means (1a) storing therein first
data and usable for starting said vehicular engine; and
reader means (2) for reading said first data when said data carrying means (1a) is used for starting said vehicular engine,

wherein said security unit (20) stores therein second data and is connected to receive said first data from said reader means (2) and collate said received first data with said second data so that said engine start enabling data is transmitted to said engine control unit (30) at a time of supply of said voltage from said power source (Ba) when said first data and second said data agree.

12. A method of operating an engine including an anti-theft system which includes a security unit, an engine control unit (30; 30A) including a CPU (32a); a power source (Ba); and, storage means (34), wherein the method comprises the steps of,
supplying a voltage from the power source to the CPU (32a) to reset the CPU (32a);
transmitting first engine start enabling data from the security unit to the CPU (32a); if the first start enabling data is transmitted to said engine control unit, transmitting second start enabling data to the storage means; the storage means (34) storing the second start enabling data as start enabling information; the CPU (32a) being arranged to perform arithmetic operations for starting the engine based on the first, start enabling data and so as to maintain the starting of said engine and the operation thereafter based on said information stored in said storage means (34) even if it is reset again after the transmission of said first start enabling data;

characterised in that the method further includes the step of: changing the second start enabling data (D5C) to an engine start inhibiting signal (D76) before the vehicle has been stopped by normally stopping the engine.

Patentansprüche

1. Fahrzeug-Einbruchsicherungssystem, mit:
ineiner Sicherheitseinheit (20) zum Aussenden von ersten, einen Maschinenstart ermöglichen- den Daten, wenn eine Fahrzeugmaschine betätigt wird, um sie zu starten;
einer Maschinensteuereinheit (30; 30A), die mit einer CPU (32a) ausgestattet ist und dafür ausgebildet ist, durch eine Spannung zurückgestellt zu werden, die von einer Stromversorgungsquelle (Ba) zum Zeitpunkt des Startbetriebes zugeführt wird, und die dafür ausgebildet ist, um arithmetische Operationen zum Starten der Maschine basierend auf den ersten, den Start ermöglichen Daten durchzuführen; und

einer Speichereinrichtung (34) zum Speichern von zweiten, den Start ermöglichen Daten (D5C) als Startfreigabeinformationen, wenn die ersten, den Start ermöglichen Daten zu der Maschinensteuereinheit gesendet werden;

wobei die CPU (32a) dafür ausgebildet ist, arithmetische Operationen in solcher Weise auszuführen, um den Startvorgang der Maschine aufrecht zu erhalten und den Betrieb derselben danach aufrechtzuerhalten und zwar basierend auf den genannten Informationen, die in der Speichereinrichtung (34) abgespeichert sind und selbst dann, wenn sie nach der Übertragung der ersten, den Start ermöglichen Daten erneut rückgestellt wird,
dadurch gekennzeichnet, daß

die zweiten, den Start ermöglichen Daten (D5C) in ein den Maschinenstart verhindern des Signal (D76) geändert werden bevor das Fahrzeug durch normales Stoppen der Maschine angehalten wird.

2. Fahrzeug-Einbruchsicherungssystem nach Anspruch 1, bei dem die Sicherheitseinheit (20) dafür ausgebildet ist, um die den Start der Maschine verhindern Daten dann auszusenden, wenn die Maschine in unlegitimierter Weise gestartet wird; die CPU (32a) dafür ausgebildet ist, durch den unlegitimierten Startvorgang zurückgestellt zu werden und um arithmetische Operationen durchzuführen, so daß der Startvorgang der Maschine basierend auf den Startverhinderungsdaten (D3A) verhindert wird;
die Speichereinrichtung (34) dafür ausgebildet ist, um die Startverhinderungsdaten als Starverhinde- runginformationen zu speichern; und
die CPU (32a) dafür ausgebildet ist, um arithmetische Operationen in solcher Weise durchzuführen, daß der Startvorgang der Maschine aufrecht erhalten wird, ebenso der Betrieb danach und die Verhinderung des Startvorgangs basierend auf den in der Speichereinrichtung (34) gespeicherten Informationen aufrecht erhalten wird, selbst wenn die CPU (32a) erneut nach dem Aussenden der den Start ermöglichen Daten und der den Start verhindern Daten zurückgestellt wird.

3. Fahrzeug-Einbruchsicherungssystem nach An-
prücht 1 oder 2, ferner mit:

einer der Maschinendrehzahl detektierenden Einrichtung (33) zum Detektieren der Zahl der Umdrehungen der Maschine pro Zeiteinheit, wobei die CPU (32a) dafür ausgebildet ist, um arithmetische Operationen durchzuführen, um den Startvorgang der Maschine basierend auf den gespeicherten Startfreigabeinformationen aufrecht zu erhalten, selbst wenn sie erneut zurückgestellt wird, wenn die Speichereinrichtung (34) die Startfreigabeinformationen speichert bevor die detektierte Zahl der Umdrehungen pro Zeiteinheit eine Zahl erreicht, die ausreichend ist, um den Startvorgang der Maschine zu vervollständigen.

4. Fahrzeug-Einbruchsicherungssystem nach Anspruch 3, bei dem die CPU (32a) dafür ausgebildet ist, um arithmetische Operationen durchzuführen, um den Betrieb der Maschine aufrecht zu erhalten und zwar selbst dann, wenn sie erneut zurückgestellt wird, nachdem die detektierte Zahl der Umdrehungen pro Zeiteinheit die Zahl erreicht hat, die ausreichend ist, um den Startvorgang der Maschine zu vervollständigen.

5. Fahrzeug-Einbruchsicherungssystem nach Anspruch 1 oder 2, ferner mit:

einer der Maschinendrehzahl detektierenden Einrichtung (33) zum Detektieren der Zahl der Umdrehungen der Maschine pro Zeiteinheit, wobei die CPU (32a) dafür ausgebildet ist, um den Startvorgang der Maschine basierend auf den Startfreigabeinformationen der Vorstart-Startfreigabedaten aufrecht zu erhalten und zwar selbst dann, wenn diese erneut zurückgestellt wird, wenn die Speichereinrichtung (34) die Vorstart-Startfreigabedaten als Startfreigabeinformationen speichert bevor die detektierte Zahl der Umdrehungen pro Zeiteinheit die Zahl der Umdrehungen der Maschine erreicht, die ausreichend ist, um den Startvorgang zu komplettieren, wobei die Speichereinrichtung (34) dafür ausgebildet ist, Nach-Sort-Startfreigabedaten der Maschine als Startfreigabeinformationen anstelle der Vorstart-Startfreigabedaten zu speichern, nachdem die detektierte Zahl der Umdrehungen pro Zeiteinheit die Zahl der Umdrehungen der Maschine pro Zeiteinheit erreicht hat, die ausreichend ist, um den Startvorgang zu komplettieren, und die CPU (32a) dafür ausgebildet ist, um arithmetische Operationen in solcher Weise durchzuführen, daß der Betrieb der Maschine aufrecht erhalten wird und zwar selbst dann, wenn sie erneut zurückgestellt wird, basierend auf den Startfreigabeinformationen der gespeicherten Nach-Start-Startfreigabedaten.


7. Fahrzeug-Einbruchsicherungssystem nach einem der vorhergehenden Ansprüche, bei dem die Speichereinrichtung (34) aus einem nicht flüchtigen Speicher besteht.

8. Fahrzeug-Einbruchsicherungssystem nach einem der vorhergehenden Ansprüche, bei dem die Speichereinrichtung (34) aus einem nicht flüchtigen Speicher besteht.

9. Fahrzeug-Einbruchsicherungssystem nach Anspruch 1 oder Anspruch 2, ferner mit:

einer der Maschinendrehzahl detektierenden Einrichtung (33) zum Detektieren der Zahl der Umdrehungen der Maschine pro Zeiteinheit, wobei die Speichereinrichtung (34) die Nachstart-Startfreigabedaten der Maschine als Startfreigabeinformationen anstelle der Vorstart-Startfreigabedaten speichert bevor die detektierte Zahl der Umdrehungen pro Zeiteinheit die Zahl der Umdrehungen der Maschine erreicht hat, die für den Startvorgang ausreichend ist, und wobei die CPU (32a) arithmetische Operationen in solcher Weise durchführt, um den Betrieb der Maschine selbst dann aufrecht zu erhalten, wenn sie erneut zurückgestellt wird, und zwar basierend auf
den Startfreigabeadaten der gespeicherten Nachstart-Startfreigabeadaten.

10. Fahrzeug-Einbruchsicherungssystem nach einem der vorhergehenden Ansprüche, bei dem die in der Speichereinrichtung (34) zum Zeitpunkt des Startens der Maschine gespeicherten Informationen in andere Informationen änderbar sind, die in der Speichereinrichtung (34) während der Zeit vor der Zufuhr der Spannung von der Stromversorgungsquelle (Ba) zu der Maschinensteuereinheit (30; 30A) zum Stoppen des Betriebes der Maschine abgespeichert werden.

11. Fahrzeug-Einbruchsicherungssystem nach einem der Ansprüche 1 bis 10, ferner mit:

einer Datenaufbewahrungseinrichtung (1a) (data carrying means), die erste Daten speichert und zum Starten der Fahrzeugmaschine verwendbar ist; und
einer Leseeinrichtung (2) zum Lesen der ersten Daten, wenn die Datenaufbewahrungseinrichtung (1a) zum Starten der Fahrzeugmaschine verwendet wird,

wobei die Sicherheitseinheit (20) zweite Daten speichert und so angeschlossen ist, um die ersten Daten von der Leseeinrichtung (2) zu empfangen, und um die empfangenen ersten Daten mit den zweiten Daten zusammen zu führen bzw. so zu ordnen, daß die den Maschinenstart ermöglichen Daten zu der Maschinensteuereinheit (39) zu einem Zeitpunkt der Zufuhr der Spannung von der Stromversorgungsquelle (Ba) aus übertragen werden, wenn die ersten Daten und die zweiten Daten übereinstimmen.

12. Verfahren zum Betreiben einer Maschine mit einem Einbruchsicherungssystem, welches enthält:

eine Sicherheitseinheit,
eine Maschinensteuereinheit (30; 30A) mit einer CPU (32a);
eine Stromversorgungsquelle (Ba); und
eine Speichereinrichtung (34),

wobei das Verfahren beim Starten der Maschine die folgenden Schritte umfaßt:

Zuführen einer Spannung von der Stromversorgungsquelle zu der CPU (32a), um die CPU (32a) zurückzustellen; Übertragen von ersten, den Start der Maschine ermöglichen Daten von der Sicherheitseinheit zu der CPU (32a);
dann, wenn die ersten, den Start ermöglichen Daten zu der Maschinensteuereinheit übertragen werden, die zweiten Startfreigabe- daten zu der Speichereinrichtung übertragen werden;
die Speichereinrichtung (34) die zweiten den Start ermöglichen Daten als Startfreigabe- informations speichert;
die CPU (32a) dafür ausgebildet ist, um arithmetische Operationen zum Starten der Maschine basierend auf den ersten, den Start ermöglichen Daten durchzuführen, und um den Startvorgang der Maschine und den danach erfolgenden Betrieb derselben basierend auf den Informationen aufrecht zu erhalten, die in der Speichereinrichtung (34) gespeichert sind und zwar selbst dann, wenn die CPU erneut nach der Übertragung der ersten, den Start ermöglichen Daten zurückgestellt wird;
dadurch gekennzeichnet, daß das Verfahren ferner die folgenden Schritte umfaßt: Ändern der zweiten den Start ermöglichen Daten (DSC) in ein den Start verhindendes Signal (D76) bevor das Fahrzeug durch ein normales Anhalten der Maschine angehalten wird.

Revalidications

1. Système antivol pour véhicule comprenant :

une unité de sécurité (20) destinée à transmettre des premières données permettant le démarrage du moteur lorsqu’un moteur pour véhicule est actionné pour démarrer ;
eine unité de commande de moteur (30 ; 30A) munie d’une CPU (32a) prévue pour être remise à zéro par une tension délivrée à partir d’une source d’alimentation (Ba) au moment de le fonctionnement de démarrage et prévue pour réaliser des opérations arithmétiques destinées à démarrer ledit moteur sur la base des dites premières données permettant le démarrage ; et
un moyen de mémorisation (34) destiné à mémoriser des deuxième données permettant le démarrage (D5C) en tant qu’informations permettant le démarrage si lesdites premières données permettant le démarrage sont transmises à ladite unité de commande du moteur ;
dans lequel ladite CPU (32a) est prévue pour réaliser des opérations arithmétiques de façon à maintenir le démarrage dudit moteur et le fonctionnement après ceci basé sur lesdites informations mémorisées dans ledit moyen de mémorisation (34) même si elle est remise à zéro à nouveau après la transmission desdites premières données permettant le démarrage, caractérisé en ce que lesdites deuxième données permettant le démarrage (D5C) sont changées en un signal interdisant le démarrage du moteur (D76) avant que le véhicule ait été arrêté en arrêtant normalement le moteur.

2. Système antivol pour véhicule selon la revendication 1, dans lequel :

l’unité de sécurité (20) est prévue pour transmettre des données interdisant le démarrage du moteur lorsque ledit moteur est démarré sans moyen être autorisé ;

ladite CPU (32a) est prévue pour être remise à zéro par ladite opération de démarrage non autorisée et pour réaliser les opérations arithmétiques destinées à interdire le démarrage dudit moteur sur la base desdites données d’interdiction de démarrage (DA3) ;

le moyen de mémorisation (34) est prévu pour mémoriser les données d’interdiction de démarrage en tant qu’informations d’interdiction de démarrage, et ;

ladite CPU (32a) est prévue pour réaliser des opérations arithmétiques de façon à maintenir le démarrage dudit moteur, le fonctionnement après cela et l’interdiction du démarrage basée sur les informations mémorisées dans ledit moyen de mémorisation (34) même si ladite CPU (32a) est à nouveau remise à zéro après la transmission desdites données d’autorisation de démarrage et desdites données d’interdiction de démarrage.

3. Système antivol pour véhicule selon la revendication 1 ou 2, comprenant de plus :

un moyen de détection de vitesse du moteur (33) destiné à détecter le nombre de tours dudit moteur par unité de temps,

dans lequel ladite CPU (32a) est prévue pour réaliser des opérations arithmétiques de façon à maintenir le démarrage dudit moteur sur la base desdites informations autorisant le démarrage dudit moteur même si elle est à nouveau remise à zéro lorsque ledit moyen de mémorisation (34) même si ladite CPU (32a) est à nouveau remise à zéro après la transmission desdites données d’autorisation de démarrage et desdites données d’interdiction de démarrage.

4. Système antivol pour véhicule selon la revendication 3,

dans lequel ladite CPU (32a) est prévue pour réaliser des opérations arithmétiques de façon à maintenir le fonctionnement dudit moteur même si elle est à nouveau remise à zéro après que ledit nombre de tours par unité de temps détecté ait atteint le nombre suffisant pour achever le démarrage du moteur.

5. Système antivol pour véhicule selon la revendication 1 ou 2, comprenant de plus :

un moyen de détection de vitesse du moteur (33) destiné à détecter le nombre de tours dudit moteur par unité de temps,

dans lequel ladite CPU (32a) est prévue pour maintenir le démarrage dudit moteur sur la base desdites informations autorisant le démarrage des données autorisant le démarrage du prédémarrage même si elle est à nouveau remise à zéro lorsque ledit moyen de mémorisation (34) même si ladite CPU (32a) est à nouveau remise à zéro après la transmission desdites données d’autorisation de démarrage et desdites données d’interdiction de démarrage.

6. Système antivol pour véhicule selon la revendication 5,

dans lequel lesdites données permettant le démarrage de prédémarrage, les données autorisant le démarrage après le démarrage et les données d’interdiction de démarrage sont composées respectivement d’une valeur composée de chiffres préétablis et au moins une partie de deux chiffres desdites données d’interdiction de démarrage et différente de celles desdites données autorisant le démarrage de prédémarrage et desdites données d’autorisation de démarrage après démarrage.
7. Système antivol pour véhicule selon la revendication 6,
dans lequel chaque valeur des chiffres prédéterminés desdites données permettant le démarrage du prédémarrage, des données d’autorisation de démarrage après démarrage et des données d’interdiction de démarrage sont composées respectivement d’une valeur de huit bits et lesdites données d’interdiction de démarrage comportent une différence de trois bits par rapport aux données d’autorisation de démarrage après démarrage et comportent une différence de huit bits par rapport aux données d’autorisation de démarrage avant démarrage.

8. Système antivol pour véhicule selon l’une quelconque des revendications précédentes,
dans lequel le moyen de mémorisation (34) est une mémoire non volatile.

9. Système antivol pour véhicule selon la revendication 1 ou la revendication 2, comprenant de plus :

   un moyen de détection de vitesse du moteur (33) destiné à détecter le nombre de tours du dit moteur par unité de temps,

   dans lequel le ledit moyen de mémorisation (34) mémorise lesdites données d’autorisation de démarrage avant démarrage en tant que dites informations d’autorisation de démarrage avant démarrage et le ledit nombre de tours détecté atteigne un nombre de tours dudit moteur par unité de temps suffisant pour achever le démarrage,

   dans lequel le ledit moyen de mémorisation (34) mémorise les données d’autorisation de démarrage après démarrage dudit moteur en tant que dites informations d’autorisation de démarrage après démarrage et le ledit nombre de tours détecté atteigne le nombre de tours dudit moteur par unité de temps suffisant pour le démarrage, et

   dans lequel le ledit CPU (32a) réalise les opérations arithmétiques de façon à maintenir le fonctionnement dudit moteur même si elle est à nouveau remise à zéro sur la base desdites informations d’autorisation de démarrage desdites données d’autorisation de démarrage après démarrage mémorisées.

10. Système antivol pour véhicule selon l’une quelconque des revendications précédentes,
dans lequel lesdites informations mémorisées dans le ledit moyen de mémorisation (34) au moment du démarrage dudit moteur sont prévues pour changer en autre informations devant être mémorisées dans le ledit moyen de mémorisation (34) pendant l’instant avant l’alimentation en tension provenant de ladite source d’alimentation (Ba) vers ladite unité de commande du moteur (30 ; 30A) pour arrêter le fonctionnement du moteur.

11. Système antivol pour véhicule selon l’une quelconque des revendications 1 à 10, comprenant de plus :

   un moyen de support de données (1a) mémorisant dans celui-ci les premières données et pouvant être utilisé pour démarrer ledit moteur de véhicule ; et

   un moyen de lecture (2) destiné à lire les premières données lorsque le ledit moyen de support de données (1a) est utilisé pour démarrer ledit moteur de véhicule,

   dans lequel ladite unité de sécurité (20) mémorise dans celle-ci les deuxièmes données et est connectée pour recevoir lesdites premières données provenant dudit moyen de lecture (2) et interclasser lesdites premières données reçues avec lesdites deuxième données de sorte que lesdites données d’autorisation de démarrage du moteur soient transmises à ladite unité de commande du moteur (30) à un moment d’alimentation de ladite tension provenant de ladite source d’alimentation (Ba) lorsque lesdites premières données et lesdites deuxièmes données s’accordent.

12. Procédé d’actionnement d’un moteur comprenant un système antivol qui comprend une unité de sécurité,

   une unité de commande de commande de moteur (30 ; 30A) comprenant une CPU (32a)

   une source d’alimentation (Ba) ; et

   un moyen de mémorisation (34),

   dans lequel le procédé comprend les étapes consistant à, lorsque le moteur est actionné pour démarrer :

   délivrer une tension provenant de la source d’alimentation à la CPU (32a) pour remettre à zéro la CPU (32a) ;

   transmettre des premières données d’autorisation de démarrage du moteur provenant de l’unité de sécurité à la CPU (32a) si les premières données d’autorisation de démarrage sont transmises à ladite unité de commande de moteur, transmettre les deuxièmes données d’autorisation de démarrage au moyen de mémorisation ; le moyen de mémo-
risation (34) mémorisant les deuxième données d’autorisation de démarrage en tant qu’informations d’autorisation de démarrage ;
la CPU (32a) étant prévue pour réaliser des opérations arithmétiques destinées à démarrer le moteur sur la base desdites premières données d’autorisation de démarrage et de façon à maintenir le démarrage dudit moteur et le fonctionnement après cela basé sur lesdites informations mémorisées dans ledit moyen de mémorisation (34) même si elle est à nouveau remise à zéro après la transmission desdites premières données d’autorisation de démarrage ;

**caractérisé en ce que** ledit procédé comprend de plus l’étape consistant à : changer les deuxième données d’autorisation de démarrage (D5C) en un signal d’interdiction de démarrage du moteur (D76) avant que le véhicule ait été arrêté en arrêtant normalement le moteur.
FIG. 2

START

RESET AND START TIMER 21b

101

2 SEC. AFTER RESET OF CPU 21a

102

YES

RELEASE OF DOOR LOCK

103

NO

NO

COINCIDENCE OF PASS WORD

104

YES

INJ. ENABLING SIGNAL TO ECU30

105

NO

INJ. INHIBITING SIGNAL TO ECU30

106

STA. ENABLING SIGNAL TO STARTER 40

107

1
START

RESET AND START TIMER32b

XLSECRI = 0

WITHIN 2 SEC. AFTER RESET OF CPU32a?

CALCULATE Ne

Ne ≥ 500 rpm?

B/U RAM34 = D5C

INJ. ENABLING SIGNAL?

INJ. INHIBITING SIGNAL?

SIGNAL FROM CPU32a?

B/U RAM34 ← D5C

XLSECRI = 1

B/U RAM34 ← DA3

XLSECRI = 0

FIG. 3
FIG. 4

2 SEC. AFTER RESET OF CPU32a

NO

YES

Ne ≥ 500 rpm ?

NO

YES

B/U RAM = D5C?

NO

YES

B/U RAM ← D76

3
FIG. 5

2 SEC. AFTER
RESET OF CPU32a
?

YES

Ne ≥ 500 rpm?

NO

B/U RAM=D76?

NO

YES

B/U RAM=DA3?

NO

YES

XLSECRI=1

XLSECRI=0

4
FIG. 6

INTERRUPT

301

XLSECRI = 1?

NO

YES

302

INJ. START PROCESS

END

FIG. 7

D5C  0 1 0 1 1 1 0 0

D76  0 1 1 1 0 1 1 0

DA3  1 0 1 0 0 0 1 1

3 BITS DIFFERENCE

5 BITS DIFFERENCE

8 BITS DIFFERENCE
FIG. 8A

FIG. 8B

FIG. 8C

FIG. 8D

FIG. 8E

FIG. 8F

FIG. 8G

ONE TRIP
IG. SW. ON
INJ. ENABLING SIGNAL
2 SEC.
STA. ON
Ne
500 rpm
14V
0V
CPU32a
+ B
D76 D5C D76 D5C
t0 t1 t2 t3
TIME