(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 June 2016 (16.06.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/091439 A1

(51) International Patent Classification:
B60R 25/00 (2013.01)

(21) International Application Number:
PCT/EP2015/074273

(22) International Filing Date:
20 October 2015 (20.10.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1422063.6 11 December 2014 (11.12.2014) GB

(71) Applicant: **DIGITPOL LIMITED** [CN/CN]; Dept of Fraud - 502, Bank of America Tower, 12 Harcourt Road, Central, Hong Kong (CN).

(72) Inventors; and

(71) Applicants *(for US only)*: **SMIT, Robin, Robert** [NL/NL]; Kopspoor 55, Capelle ad IJssel (NL). **COYNE, Martin, John** [IE/NL]; Schiedamsedijk 177, Rotterdam (NL).

(74) Agent: **O'CONNOR, Michael**; O'Connor Intellectual Property, Suite 207 Q House, Furze Road, Sandyford, Dublin, 18 (IE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: A SECURITY DEVICE FOR A VEHICLE'S ELECTRONIC SYSTEM

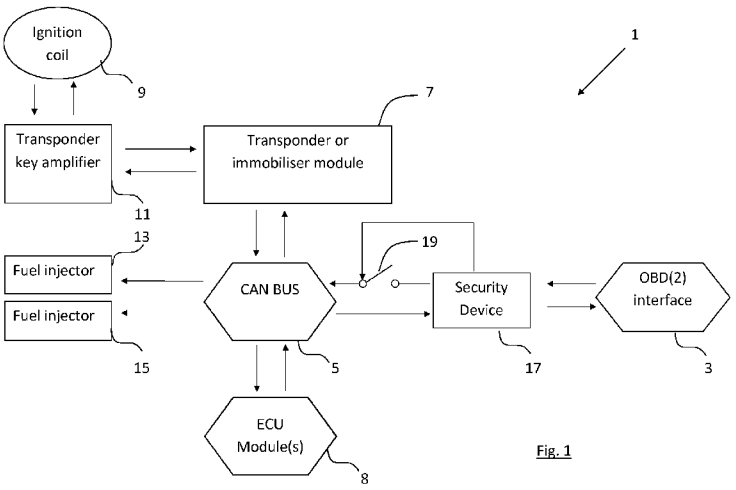

Fig. 1

(57) **Abstract**: This invention relates to a security device (17) for a vehicle's electronic system. The vehicles electronic system comprises a Control Area Network (CAN) Bus (5) connected to a plurality of engine control units (ECUs) (7, 8) and an On-Board Diagnostics (OBD) plug (3). The ECUs (7, 8) are accessible from the OBD plug (3) through the CAN Bus. The security device comprises an input port (21) for connection to the OBD plug, and an output port (23) for connection to the CAN Bus. Communications to and from the CAN Bus and the OBD plug are routed through the security device (17). The security device comprises means to detect whether a valid ignition key has been presented in the vehicle and means to permit write communications to pass from the OBD plug to the ECUs via the CAN Bus on detection of a valid ignition key and prevent write communications from passing from the OBD plug to the ECUs via the CAN Bus in the absence of a valid ignition key.

WO 2016/091439 A1

Title of Invention:

"A security device for a vehicle's electronic system"

Technical Field:

This invention relates to a security device for a vehicle's electronic system. More specifically, the present invention relates to a security device that is operable to prevent theft of the vehicle perpetrated through exploitation of the vulnerabilities of the On-Board Diagnostics (OBD) plug.

Background Art:

A recent study has shown that although the number of car thefts in the EU has fallen by 12% over the last five years, the total value of cars stolen has increased by 51% over the same period. The increase in value is due predominantly to the fact that the cars are now being stolen at a much younger age than was heretofore the case. Of the cars stolen in the EU, 72% are now estimated to be only between 1 and 5 years old. This represents a massive problem for insurers. These figures are taken from official European police figures provided by the Dutch national institute against vehicle crime.

It has also been estimated that 82% of all cars stolen in the EU are stolen by unscrupulous individuals exploiting the vulnerabilities of the On-Board Diagnostics (OBD) plug. Once access to the OBD plug has been gained, the connection to the OBD plug can be used to communicate with one or more engine control units (ECUs) or modules via the Control Area Network (CAN) Bus. This connection can be used to turn off the immobiliser module, thereby allowing the car to be started with practically any key, or can be used to allow access to the key programming module thereby allowing programming of a new key for the vehicle.

Worryingly, the tools necessary for carrying out such nefarious activities are readily available to buy over the internet and as they are typically described as "locksmith" tools, they are often perfectly legal for members of the public to own in most jurisdictions. Furthermore, these tools are typically very compact, small enough to fit into an

individual's pocket. This represents a significant problem for the authorities as these crimes are becoming increasingly easier to perpetrate and increasingly harder to prevent.

A number of solutions have been proposed to address the problem of attacks via the OBD plug. One solution is that proposed in GB2510099 in the name of Shaw. This patent application proposes to provide a cover for the OBD plug with tamper resistant fasteners to prevent quick and easy access to the OBD. Although such a device may slow down a thief, this solution can be readily circumvented once the thief has the appropriate equipment. Other solutions to the problem of attacks via the OBD plug are proposed in DE202014104646 in the name of Matzke and WO2014181094 in the name of Chambers et al. Both of these disclosures propose providing a theft protection device that connects to the OBD plug and presents an alternative external interface. The theft protection devices have one or more switches for interrupting throughpassage of signals to the OBD plug. Although such devices may also help to slow down a thief, the devices are readily detectable and therefore may be circumvented by the determined thief.

It is an object of the present invention to provide a security device for a vehicle's electronic system that overcomes at least some of the above-identified problems. It is a further object of the present invention to provide a security device that protects vehicles from theft through an OBD plug attack.

Summary of Invention:

According to the invention there is provided a security device for a vehicle's electronic system, the vehicles electronic system comprising a Control Area Network (CAN) Bus connected to a plurality of engine control units (ECUs) and an On-Board Diagnostics (OBD) plug, the ECUs being accessible from the OBD plug through the CAN Bus, characterised in that the security device comprises an input port for connection to the OBD plug and an output port for connection to the CAN Bus so that communications to and from the CAN Bus and the OBD plug are routed through the security device, the security device comprising means to detect whether a valid ignition key has been presented in the vehicle and means to permit write communications to pass from the OBD plug to one or more of the ECUs via the CAN Bus on detection of a valid ignition

key and prevent write communications from passing from the OBD plug to the ECUs via the CAN Bus in the absence of a valid ignition key.

By having such a security device, the security device will prevent any write commands from being passed from the OBD port to the ECUs over the CAN Bus if a valid ignition key is not present. In this way, if an unscrupulous individual should gain access to the interior of the car and the OBD port, they will not be able to send write commands to the ECUs as there will not be a valid ignition key present. Therefore, these individuals will not be able to turn off the immobiliser or program a new key using this method. This will obviate a significant portion of all car thefts each year. However, it will still be possible for car dealers and others with access to a valid ignition key to send write commands to one or more of the ECUs if they need to. Furthermore, the present invention is seen as a particularly simple device to manufacture and install. The solution only requires one piece of equipment, located intermediate the OBD port and the CAN Bus, and it will be possible to retrofit the device into an existing vehicle with relatively little difficulty.

In one embodiment of the invention there is provided a security device in which the means to detect whether a valid ignition key has been presented in the vehicle comprises means to detect a communication on the CAN Bus from an immobilizer ECU indicative that a valid ignition key has been presented in the vehicle. This is seen as a simple way to determine whether or not a valid ignition key has been presented and will require the immobilizer to be activated in order to operate. This embraces the inherent security of the immobilizer in the vehicle resulting in a robust, secure device.

In one embodiment of the invention there is provided a security device in which the means to detect a communication on the CAN Bus from an immobilizer ECU indicative that a valid ignition key has been presented in the vehicle comprises means to detect a communication on the CAN Bus from the immobilizer ECU to operate a fuel pump. As this requirement is highly specific and requires that the immobilizer security protocols have been fully satisfied before it will send a communication to the fuel pump, the device is seen as particularly secure as it benefits from the full security mechanisms of the immobilizer module.

In one embodiment of the invention there is provided a security device in which the means to detect a communication on the CAN Bus from an immobilizer ECU indicative that a valid ignition key has been presented in the vehicle comprises means to detect a communication on the CAN Bus from the immobilizer ECU to operate a start engine. This requirement is also highly specific and requires that the immobilizer security protocols have been fully satisfied before it will send a communication to the start engine. Accordingly, the device is seen as particularly secure as it benefits from the full security mechanisms of the immobilizer module. It is envisaged that the immobilizer ECU may be connected to both the fuel pump and the start engine and the means to detect a communication on the CAN Bus from an immobilizer ECU indicative that a valid ignition key has been presented in the vehicle comprises means to detect one or more communications on the CAN Bus from the immobilizer ECU to operate the start engine and the fuel pump.

In one embodiment of the invention there is provided a security device in which the security device is connected intermediate the CAN Bus and the OBD plug adjacent a CAN Gateway of the CAN Bus. This is seen as particularly effective as it will be difficult to circumvent the security device in this location.

In one embodiment of the invention there is provided a security device in which the security device comprises an accessible memory and in which there is provided a data table stored in accessible memory with a list of acceptable commands, and the security device is operable to block any commands not listed in the data table. This is seen as a particularly useful embodiment of the present invention as this will allow for certain commands to be blocked or redirected while other commands may be allowed to pass through. This will help prevent detection of the security device by an unscrupulous third party with access to the OBD port.

In one embodiment of the invention there is provided a security device in which the security device comprises a catch-can filter and the security device comprises means to direct unverified data or commands received through the OBD plug to the catch-can filter. This is seen as a particularly useful embodiment of the present invention as such a device will counteract counter-surveillance measures attempting to detect the presence of a security device. Any commands or data will be transmitted onwards onto the catch-

can filter. This may be via the CAN Bus or indeed may be separate from the CAN Bus. However, it will not be possible from the OBD plug to detect whether or not the command or data has been transmitted onwards to the ECU. There will be no indication that the command or data has been blocked or re-routed.

In one embodiment of the invention there is provided a security device in which the catch-can filter is connected to the CAN bus. In this way, the command will be passed onto the CAN bus but will be readdressed to the catch-can filter rather than the original intended target ECU for the command.

In one embodiment of the invention there is provided a security device in which the security device is provided with means to permit read communications to pass to and from the OBD plug and one or more of the ECUs via the CAN Bus on detection of a valid ignition key and prevent read communications to pass to and from the OBD plug and the ECUs via the CAN Bus in the absence of a valid ignition key. This is seen as a useful alternative embodiment of the present invention. By preventing read communications, it will be possible to detect that there is a security device present however this method will also prevent any potential weaknesses that could be exposed by allowing read communications to be transmitted and received by the CAN Bus.

In one embodiment of the invention there is provided a security device in which the security device is provided with a wireless communications module for communications with a remote entity. This is seen as useful as it will be possible for the security device to be updated remotely. For example, the security device may be provided with a SIM card and may be capable of communications over the GSM network.

In one embodiment of the invention there is provided a security device in which the security device is powered by the vehicle's electronic system.

In one embodiment of the invention there is provided a vehicle's electronic system comprising a security device connected in-line intermediate a CAN Bus and an OBD plug of the vehicle's electronic system.

Brief Description of the Drawings:

The invention will now be more clearly understood from the following description of some embodiments thereof given by way of example only with reference to the accompanying drawings, in which:-

Figure 1 is a diagrammatic representation of a security system incorporating the security device according to the invention; and

Figure 2 is a diagrammatic representation of a security device according to the invention; and

Figure 3 is a diagrammatic representation of an alternative embodiment of a security system incorporating the security device according to the invention.

Detailed Description of the Drawings:

Referring to Figure 1, there is shown a vehicle's electronic system, indicated generally by the reference numeral 1, comprising an On-Board Diagnostics (OBD) port 3, a Control Area Network (CAN) Bus 5 and a plurality of Engine Control Units (ECU) modules 7, 8, only two of which are shown. ECU module 7 is in fact an immobiliser module. There is further shown an ignition coil 9, a transponder key amplifier 11 and a pair of fuel injector components 13, 15. The vehicle's electronic system comprises a security device 17 located intermediate the OBD port 3 and the CAN Bus 5. All communications between the CAN Bus 5 and the OBD port 3 pass through the security device 17.

In use, the security device 17 is operable to selectively block write commands from the OBD port 3 directed towards the CAN Bus 5. As will be understood, the CAN Bus 5 is the system of communication between the vehicles central processing unit (not shown) and the peripheral computer components such as central locking, air bag control and a plurality of ECUs. Heretofore, the CAN Bus 5 would allow any data to be sent via the OBD port 3 however in this implementation, the security device 17 will prevent write

commands from being passed onwards from the OBD port 3 to the CAN Bus 5 unless there is a valid key (not shown) inserted in the vehicles ignition.

If a valid key is present in the vehicles ignition, a signal will be sent from the transponder key amplifier 11 to the immobiliser module 7 that a valid key has been inserted into the ignition. The immobiliser module 7 will in turn send an instruction over the CAN Bus 5 to the fuel injector components 13, 15. The security device 17 is however monitoring the communications over the CAN Bus and detects the instruction from the immobiliser module 7 to the fuel injector components 13, 15. This instruction is indicative that there is a valid key in the ignition and under those circumstances, the security device 17 will allow write commands to be transmitted from the OBD port 3 to the ECU module(s) 8 via the CAN Bus 5. This is graphically represented by a switch 19 on the transmission line from the security device to the CAN Bus. If the switch 19 is open, the communications from the OBD port 3 will be prevented from reaching the CAN Bus 5 but if the switch 19 is closed, the communications from the OBD port 3 will be allowed to pass onwards to the CAN Bus 5.

In an alternative embodiment, there is provided a catch-can filter (not shown) connected to one of the CAN Bus 5 or the security device. In that embodiment, the security device 17 is operable to redirect communications from the OBD to the catch-can filter in the event that there is no valid key present in the ignition. In other words, the commands are not allowed reach their intended target ECU but instead are redirected to a catch-can filter where the commands will have no further consequence on the operation of the vehicles electronic system. This will prevent detection of the security device 17 as there will be no evidence of the security device's existence other than the command did not work.

Referring to Figure 2, there is shown a diagrammatic representation of the security device 17. The security device 17 comprises an input port 21 and an output port 23. The input port 21 is arranged to be coupled to the OBD port 3 and the output port 23 is arranged to be coupled to the CAN Bus 5. The security device further comprises a processor 25, an accessible memory 27 including a data table 29, a wireless communications module 31, a detection circuit 33 and a write blocker 35.

In use, the input port 21 is connected to the OBD port and the output port 23 is connected to the CAN Bus. The detection circuit 33 monitors communications on the CAN Bus 5 to detect whether a valid key has been presented. If a valid key has been presented, for example inserted into the vehicle's ignition, the detection circuit will detect the presence of the valid key and will send a notification to the write blocker 35 to allow write communications from the OBD port (i.e. the input 21) to pass through to the CAN Bus (i.e. from the output 23). If a valid key is not detected, the detection circuit will not send the appropriate signal to the write blocker 35 and the write blocker 35 will prevent commands from being passed to the ECUs 8.

In one embodiment of the invention, there is provided a data table 29 in the accessible memory 27 and the data table 29 has a list of all permissible write commands. If a data table is provided, when a write command is received at the input 21, the write command is checked against the list of write commands and if the write command matches one of the valid write commands in the data table, the write command is allowed to proceed from the output 23 to an ECU 8. If however the write command does not match a valid write command in the data table, the write command will be terminated and not allowed to proceed to an ECU 8.

The wireless communication module 31 is provided to allow for remote access to the security device from a remote location. The wireless communications module 31 may comprise a SIM card to permit communications over a GSM network as would be understood in the art. Such a system would allow for the security device to be updated with software updates from a remote location.

Referring to Figure 3, there is shown an alternative embodiment of a security system, indicated generally by the reference numeral 41, incorporating the security device 17 according to the invention, The security device 17 further comprises a catch-can filter 43. In use, if invalid communications are sent via the OBD interface 3 along the CAN bus 5, the communications are intercepted by the security device 17. The invalid communications are redirected to the catch-can filter 43 where they may be stored for subsequent analysis. In the embodiment show, the switch 19 has been omitted however it may be provided in addition to the catch-can filter 43. There is further shown a start engine 45.

Various modifications can be made to the present invention without departing from the scope of the appended claims. For example, in the embodiment shown, an OBD(2) interface is provided and the invention has been described in terms of an OBD(2) interface. Furthermore, the invention has been described in terms of a CAN Bus. However, it is envisaged that the present invention is also relevant to other interfaces and other communication buses than those outlined above and is not so limited unless specified in the claims.

It is envisaged that the security device of the present invention may also be provided with various components and features to allow the information transmitted during an attempted attack to be captured and used as evidence subsequently. For example, it is envisaged that the imaging process of the security device will be changed to suit the justice aspect of collection and analysis of data to satisfy a global standard. The data collection process is built to the same standard used in Computer Forensics, which satisfies a global standard for Law Enforcement and commercial investigation of data. The main focus is on the steps taken to image (copy) and store data that is used as evidence.

For example, it is envisaged that hashing tools will be utilised. In the event of imaging (copying) a file or a number of files, it is necessary to compare the original hard disks to a copy or an image of the original. A hashing process analyses the copy and assigns it a unique number. If the hash numbers on the original and the copy match, the copy is a perfect replica of the original. The security device will store its log in a hashed and verified format. The security device also needs to implement a hashing process on the final read-out, meaning the saved file to the target disk or target location is proven to be identical to the original read-out. In a court of Law, a hashing process is the focus of any presented digital evidence.

It is envisaged that mechanisms will be put in place to facilitate a complete memory dump. Once an attack has taken place, the security device will collect the evidence file and the complete HEX image of the CAN BUS at the time of attack. This will preferably be saved in an encrypted format with a timestamp. The security device is also configured to include an audit trail that will be accessible by a super administrator user only. This

audit trail must be an encrypted file on the security device. The Audit trail will include the following: (i) the time the "key" switched on, registered in computer time; (ii) the number of CAN IDs sent (if any un-verified data was sent); (iii) the Vehicle Identification Number (VIN) number the end-user tried to program; and (iv) the Kilometre or Mileage (KM) the end-user tried to program. The audit trail will upload to the investigation team either using the mobile communications module upon a prompt to do so or through a direct connection once the vehicle enters a dealership, or, if the vehicle owner takes the vehicle for examination to explore when and how errors occurred.

It is envisaged that although the wireless communications module 31 illustrated in Figure 2 is useful to allow remote authorised communications with the security device by authorised personnel, it is not essential to the operation of the device and it is possible to provide a security device without the wireless communications module.

It will be understood that various parts of the present invention are performed in hardware and other parts of the invention may be performed either in hardware and/or software. It will be understood that the method steps and various components of the present invention will be performed largely in software and therefore the present invention extends also to computer programs, on or in a carrier, comprising program instructions for causing a computer or a processor to carry out steps of the method or provide functional components for carrying out those steps. The computer program may be in source code format, object code format or a format intermediate source code and object code. The computer program may be stored on or in a carrier, in other words a computer program product, including any computer readable medium, including but not limited to a floppy disc, a CD, a DVD, a memory stick, a tape, a RAM, a ROM, a PROM, an EPROM or a hardware circuit. In certain circumstances, a transmissible carrier such as a carrier signal when transmitted either wirelessly and/or through wire and/or cable could carry the computer program in which cases the wire and/or cable constitute the carrier.

It will be further understood that the present invention may be performed on two, three or more devices with certain parts of the invention being performed by one device and other parts of the invention being performed by another device. The devices may be connected together over a communications network. The present invention and claims

are intended to also cover those instances where the system is operated across two or more devices or pieces of apparatus located in one or more locations in the vehicle.

In this specification the terms “include, includes, included and including” and the terms “comprise, comprises, comprised and comprising” are all deemed totally interchangeable and should be afforded the widest possible interpretation.

The invention is in no way limited to the embodiment hereinbefore described but may be varied in both construction and detail within the scope of the appended claims.

Claims:

(1) A security device (17) for a vehicle's electronic system (1, 41), the vehicles electronic system comprising a Control Area Network (CAN) Bus (5) connected to a plurality of engine control units (ECUs) (7, 8) and an On-Board Diagnostics (OBD) plug (3), the ECUs being accessible from the OBD plug through the CAN Bus, characterised in that the security device (17) comprises an input port (21) for connection to the OBD plug (3) and an output port (23) for connection to the CAN Bus (5) so that communications to and from the CAN Bus and the OBD plug are routed through the security device (17), the security device comprising means to detect whether a valid ignition key has been presented in the vehicle and means to permit write communications to pass from the OBD plug (3) to one or more of the ECUs (7, 8) via the CAN Bus (5) on detection of a valid ignition key and prevent write communications from passing from the OBD plug to the ECUs via the CAN Bus in the absence of a valid ignition key.

(2) A security device (17) as claimed in claim 1 in which the means to detect whether a valid ignition key has been presented in the vehicle comprises means to detect a communication on the CAN Bus from an immobilizer ECU (7) indicative that a valid ignition key has been presented in the vehicle.

(3) A security device (17) as claimed in claim 2 in which the means to detect a communication on the CAN Bus from an immobilizer ECU (7) indicative that a valid ignition key has been presented in the vehicle comprises means to detect a communication on the CAN Bus from the immobilizer ECU to operate a fuel pump (13, 15).

(4) A security device (17) as claimed in claim 2 or 3 in which the means to detect a communication on the CAN Bus from an immobilizer ECU (7) indicative that a valid ignition key has been presented in the vehicle comprises means to detect a communication on the CAN Bus from the immobilizer ECU to operate a start engine (45).

(5) A security device (17) as claimed in any preceding claim in which the security device is connected intermediate the CAN Bus and the OBD plug adjacent a CAN Gateway of the CAN Bus.

(6) A security device (17) as claimed in any preceding claim in which the security device comprises an accessible memory (27) and in which there is provided a data table (29) stored in accessible memory with a list of acceptable commands, and the security device is operable to block any commands not listed in the data table.

(7) A security device (17) as claimed in any preceding claim in which the security device comprises a catch-can filter (43) and the security device comprises means to direct unverified data or commands received through the OBD plug to the catch-can filter.

(8) A security device (17) as claimed in claim 7 in which the catch-can (43) filter is connected to the CAN bus.

(9) A security device (17) as claimed in any preceding claim in which the security device is provided with means to permit read communications to pass to and from the OBD plug and one or more of the ECUs via the CAN Bus on detection of a valid ignition key and prevent read communications to pass to and from the OBD plug and the ECUs via the CAN Bus in the absence of a valid ignition key.

(10) A security device (17) as claimed in any preceding claim in which the security device is provided with a wireless communications module (31) for communications with a remote entity.

(11) A security device (17) as claimed in any preceding claim in which the security device is powered by the vehicle's electronic system.

(12) A vehicle's electronic system (1, 41) comprising a security device (17) as claimed in any preceding claim connected in-line intermediate a CAN Bus (5) and an OBD plug (3) of the vehicle's electronic system.

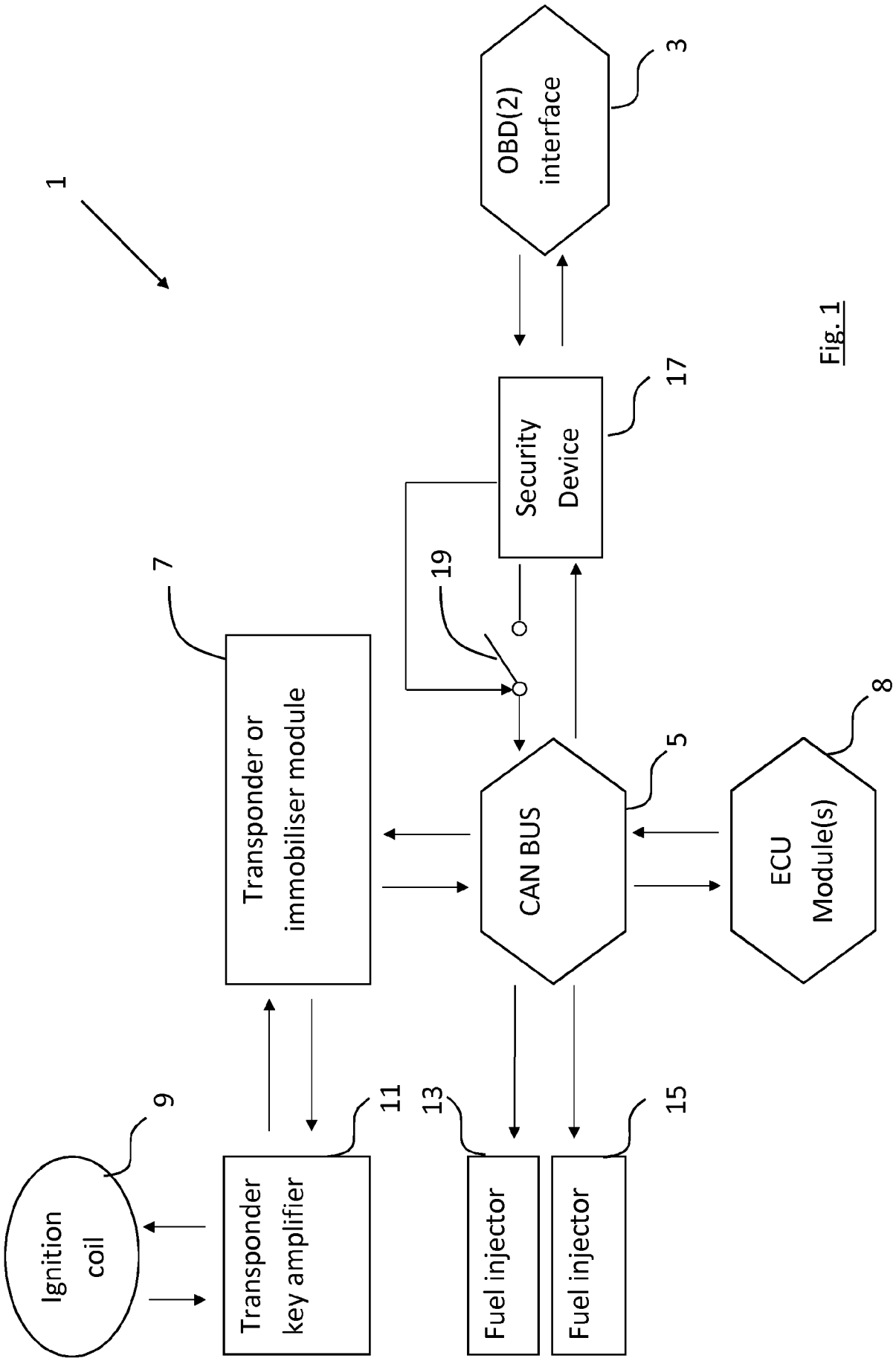
1
OBD(2) interface
3
Security Device
17
19
7
Transponder or immobiliser module
CAN BUS
5
ECU Module(s)
8
Ignition coil
9
Transponder key amplifier
11
Fuel injector
13
Fuel injector
15

Fig. 1

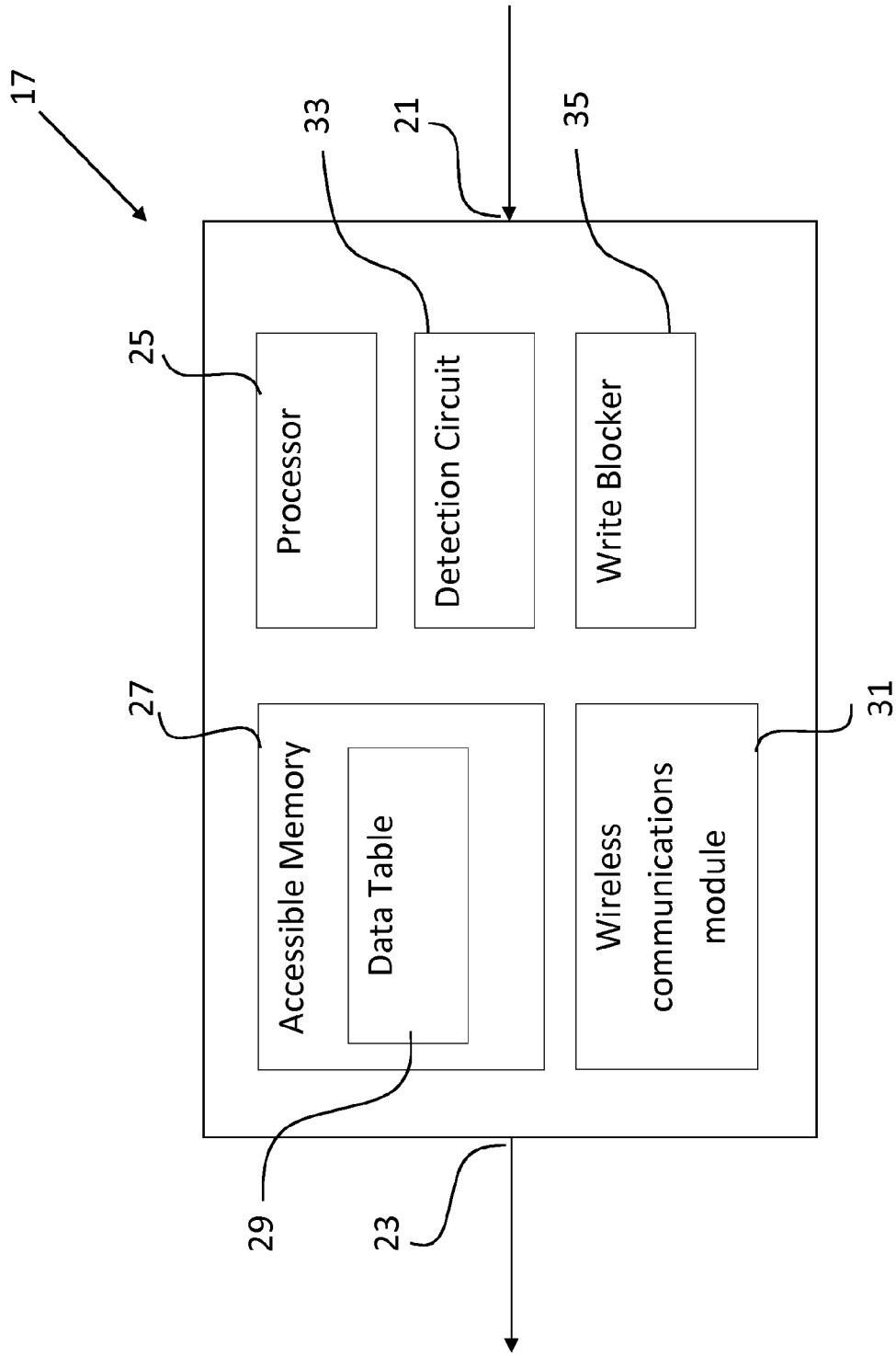
17
33
21
35
25
Processor
Detection Circuit
Write Blocker
27
Accessible Memory
Data Table
Wireless communications module
31
29
23

Fig. 2

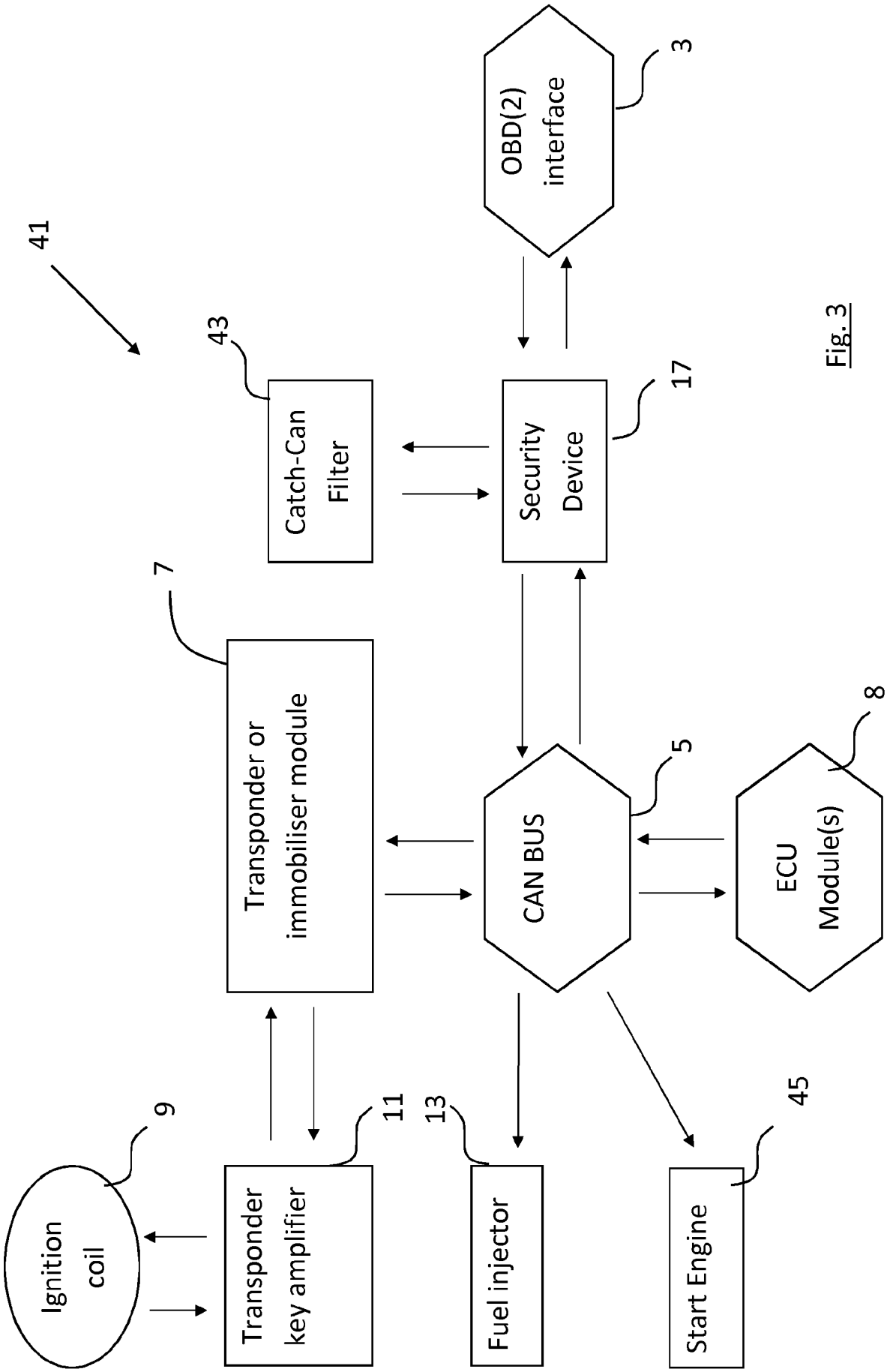
41
OBD(2) interface
3
43
Catch-Can Filter
Security Device
17
7
Transponder or immobiliser module
CAN BUS
5
ECU Module(s)
8
9
Ignition coil
Transponder key amplifier
11
13
Fuel injector
Start Engine
45

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/074273

A. CLASSIFICATION OF SUBJECT MATTER
INV. B60R25/00
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
B60R

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 20 2014 104646 U1 (MATZKE SÖREN [DE]) 24 October 2014 (2014-10-24) cited in the application paragraph [0030] - paragraph [0033] -----	1-5,9-12
X	WO 01/26338 A2 (SENSORIA CORP [US]; GELVIN DAVID C [US]; GIROD LEWIS D [US]; KAISER WI) 12 April 2001 (2001-04-12) page 23, line 26 - page 26, line 21 -----	1,12
X	EP 1 975 897 A2 (DENSO CORP [JP]) 1 October 2008 (2008-10-01) paragraph [0013] - paragraph [0018] paragraph [0043] - paragraph [0045] -----	1,12

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 February 2016	09/02/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Standring, Michael

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/074273

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2014/181094 A1 (CHAMBERS GREGORY [GB]; MAISEY PAUL JONATHAN [GB]; EATON KARL [GB]) 13 November 2014 (2014-11-13) cited in the application page 14, line 6 - page 15, line 19 -----	1-12

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2015/074273

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 202014104646 U1	24-10-2014	NONE	
WO 0126338 A2	12-04-2001	AU 7861500 A	10-05-2001
		AU 7861600 A	10-05-2001
		AU 7861700 A	10-05-2001
		AU 7871800 A	10-05-2001
		AU 7873000 A	10-05-2001
		WO 0126327 A2	12-04-2001
		WO 0126328 A2	12-04-2001
		WO 0126329 A2	12-04-2001
		WO 0126330 A2	12-04-2001
		WO 0126331 A2	12-04-2001
		WO 0126332 A2	12-04-2001
		WO 0126333 A2	12-04-2001
		WO 0126334 A2	12-04-2001
		WO 0126337 A2	12-04-2001
		WO 0126338 A2	12-04-2001
EP 1975897 A2	01-10-2008	CN 101281396 A	08-10-2008
		EP 1975897 A2	01-10-2008
		JP 2008239021 A	09-10-2008
		US 2008244757 A1	02-10-2008
WO 2014181094 A1	13-11-2014	NONE	