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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 December 2017 (14.12.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/211730 A1

(51) International Patent Classification:
F02D 41/22 (2006.01) *H04L 29/06* (2006.01)
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/EP2017/063505

(22) International Filing Date:
02 June 2017 (02.06.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1609862.6 06 June 2016 (06.06.2016) GB

(71) Applicant: **DELPHI INTERNATIONAL OPERATIONS LUXEMBOURG S.À R.L.** [LU/LU]; Avenue de Luxembourg, 4940 Bascharage (LU).

(72) Inventor: **WILLIAMS, Edward, T**; FLAT B, 1 HIGHGATE WEST HILL, London N6 6JS (GB).

(74) Agent: **DELPHI FRANCE SAS**; Bâtiment le Raspail - ZAC Paris Nord 2, 22, avenue des Nations CS65059 Villepinte, 95972 Roissy CDG Cedex (FR).

(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, DJ, 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, KH, KN, KP, KR, KW, 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).

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

(54) Title: METHOD TO CONTROL UNAUTHORISED HACKING OF FUEL INJECTOR OPERATION CONTROL

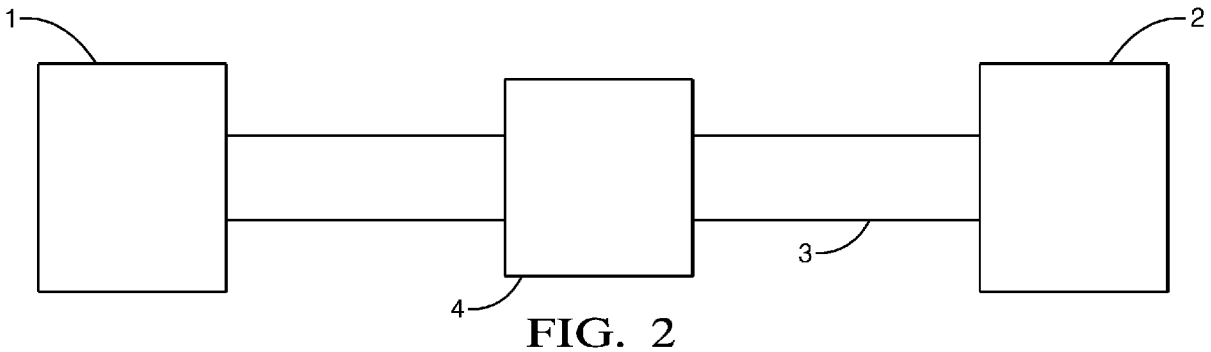

FIG. 2

(57) Abstract: A method to detect unauthorised hacking or manipulation of a control signal sent to a fuel injector from an Engine Control Unit (ECU), said control information comprising pulse profile data to be applied to the actuator of a said fuel injector, said fuel injector including processor mean associated therewith, said processor means adapted to communicate with said ECU, comprising: a) said processor means generating data indicative of at least one parameter of a pulse profile, comprising one or more actual pulses, provided to or implemented by, the actuator in a fuelling cycle; b) said processor means transmitting a message including said data indicative of said at least one parameter to said ECU, c) said ECU comparing the at least one parameter in said data with said corresponding parameters of the control signal sent to said fuel injector to determine if unauthorised alteration has occurred.

WO 2017/211730 A1

METHOD TO CONTROL UNAUTHORISED HACKING OF FUEL INJECTOR OPERATION CONTROL

FIELD OF THE INVENTION

This disclosure relates to methods and apparatus to prevent tampering and unauthorised amendment to fuel injector operation. It has specific, but not exclusive application, to injectors which include microprocessor (chips) associated with them.

BACKGROUND OF THE INVENTION

Modern engines use fuel injection, and typically have one or more fuel injectors to dispense fuel into a combustion space. Typically fuel injectors are controlled by an Electronic Control Unit (ECU). The ECU provides a control signal e.g. by way of an electrical pulse to be sent/applied to an actuator of the fuel injector to operate the injector to dispense i.e. inject fuel. The longer the electrical pulse, the more fuel is injected, and thus the power developed by the engine is increased. Thus in some examples injector operation is dictated by Pulse Width Modulation (PWM).

It is known to tamper with signals from the ECU to increase power in an unauthorised manner. It is possible to buy a device (such as a "pulse extender") that is connectable between the ECU and the injector; such devices typically for example can measure the electrical pulse from the ECU and then applies a longer pulse (i.e. amend the pulse length in an unauthrosed fashion) to the injector to make it inject more fuel than the ECU was planning to inject. This increases the power to the engine but will also increase emissions and shorten the life of the engine so engine manufacturers would like to stop this from happening. Other tampering methods include altering the data regarding the magnitude of one or more pulses in an activation profile or adding extra pulse(s)..

It is an object of the invention to overcome such problems and reduce the possibility of unauthrosed tampering with fuel injection control and signals.

STATEMENT OF THE INVENTION

In one aspect is provided a method to detect unauthorised hacking or manipulation of a control signal sent to a fuel injector from an Engine Control Unit (ECU), said control signal including control information comprising pulse profile data to be applied to the actuator of a said fuel injector, said fuel injector including processor mean associated therewith, said processor means adapted to communicate with said ECU, comprising:

a) said processor means generating data indicative of at least one parameter of a pulse profile, comprising one or more actual pulses, provided to or implemented by, the actuator in a fuelling cycle;

b) said processor means transmitting a message including said data indicative of said at least one parameter to said ECU,

c) said ECU comparing the at least one parameter in said data with said corresponding parameters of the control signal sent to said fuel injector to determine if unauthorised alteration has occurred..

Said data indicative of said at least one parameter sent to the ECU may be provided in an encrypted form or message.

Said processor means may encrypt the data and or message.

The method may include the initial step of sending a message request by the ECU to said injector to said processor means to transmit said data indicative of said at least one parameter.

Said message request may includes a message count or number, and said message transmitted to the ECU includes the message count or number.

Said encryption may uses an encryption key sent to the processor means by the ECU.

Said pulse profile parameter(s) may includes parameter(s) indicative of the number, magnitude or period of said one or more pulses applied, or implemented by said actuator in a fueling cycle.

BRIEF DESCRIPTION OF DRAWINGS

The invention will now be described by way of example and with reference to the following figures of which:

Figure 1 shows the connection between an ECU and an injector with an associated processor (chip).

Figure 2 shows the connection between an ECU and an injector with an associated processor (chip) with unauthorised hacking apparatus therebetween..

DETAILED DESCRIPTION OF THE INVENTION

Nowadays, fuel injectors often have a microprocessor or “chip” associated with them. Typically such a chip is located integral with the fuel injector. Such a chip is used to store identification parameters, trim data and operational parameters. The processors typically have processing functionality/ability which assists the diagnostics or control of the fuel injectors. The processor may for example receive signals from sensors e.g. on the

injector and process these to provide operational parameters or used to amend amended control. Such injectors are often referred to as "intelligent" or "smart" injectors. Such processors are often connected to the drive circuitry of the injector actuator. The term "chip" or "processor" hereinafter includes any semiconductor circuitry having a capable processing ability and includes application-specific integrated circuits (ASIC) or field-programmable gate arrays (FPGA) or similar.

In aspects, the methodology uses such intelligent injectors to flag up and/prevent unauthorized tampering or hacking of injector control signals

In a basic example, when using an (intelligent) injector with a processor that communicates to the ECU via the injector drive wires, it is possible to check tampering (e.g. by use of an unauthorised pulse extender) by the following methodology.
In a simple method, the processor (chip) on the injector is provided with, or determines, data on the duration or magnitude of one or more fuel pulses that actually occurs in a fueling cycle. This data may be obtained by any suitable means and would be understood by the person skilled in the art. The data may be provided for example by sensors measuring the activation pulse e.g. across the injectors terminals or by any other appropriate detection means.

The chip on the injector then sends an encrypted message to the ECU containing this data via appropriate communication means. The ECU then analyses the data and compares this data with corresponding demand injection pulse data that had been previously sent. The term "corresponding" would be understood to mean the measured and transmitted pulse data by the processor on the injector occurs for that pulse control data which was transmitted by the ECU, or at the same time, within the same short time span, time –stamped etc.

If the comparison shows that any (fuelling cycle) activation profile has one or more pulse durations or magnitudes which are different e.g. . longer than the corresponding (demand) pulse(s) sent by the ECU in an activation profile, the ECU determines that there has been tampering (unauthorised hacking). In addition the comparison may comprise comparing the number of pulses in the (activation) pulse profile sent by the ECU and those determined by the processor on the injector that have been implemeted i.e. applied.. The ECU may take appropriate measures.

In a preferred embodiment the encrypted message sent from the chip on the injector is sent as a result from a request (message) sent from the ECU. This message/enquiry may also be encrypted. So in such a method the following steps take place.

Step 1: The ECU sends an encrypted request to the smart injector to check the duration of one or more (e.g. particular) pulses. The message may include a unique message counter.

Step 2: The injector processor measures the duration of an injection pulse (i.e. corresponding to the particular pulse) that has been implemented in controlling the injector.

Step 3: The injector processor transmits the measured duration (and optionally the message counter) to the ECU in an encrypted message.

Step 4: The ECU can then compare the actual duration of the pulse received from the injector processor. If there is a significant deviation; then tampering is assumed. Any appropriate action may occur such as registering the tampering, over-riding it or limiting the operation of the engine.

If the injection extender device has been fitted, it can choose to allow the message to go to the ECU, in which case the ECU will know the duration of the pulse applied to the injector and can compare this to the duration it had output. Alternatively the injection extender can suppress the message, in which case the ECU will know that something has suppressed the message.

The injection extender device will not be able to modify the message from the injector processor because the message is encrypted.

The length or duration of the pulse as measured or computed by the injector processor can be performed in several ways and would be clear to the skilled person. In the most effective method, the length of pulse signal sent to the wires of the injectors, or associated drive circuitry may be determined.

In a preferred embodiment the request message includes a message counter. The injection extender device (tamper device) won't be able to replay a previous message from the injector processor because each request and reply has a different message counter value.

Detailed Examples

Referring to Figure 1 , this shows a first embodiment of the present invention, in which a fuel injector 2 including chip or microprocessor (including e.g. signal processing means) is coupled to an ECU 1 by means of e.g. a bi-directional data cable 3 connected between a first input/output of the injector and a first input/output of the ECU. The fuel injector includes e.g. sensor or other means to determine the length or magnitude of the fuel pulse used in the actual activation in a fuelling cycle of the fuel

injector. A cryptographic process may be employed whereby e.g. a digital data encryption may be used by the injector chip and encrypt the determined data using an encryption key (hereinafter referred to as the "Key") in order to generate an encrypted signal or message which is provided to the ECU.

Figure 2 shows the same figure as figure 1 but shows a tampering device 4 between the ECU and injectors used to e.g. extend the demand fuel injection pulses in an unauthorised fashion.

The ECU may have an input/output area including a digital signal processor arranged to receive an encrypted signal from the injector (chip). The injector chip may also be arranged to receive the Key from an Encryption Key Generator module within the ECU. The injector chip may be configured to communicate the Key to a decryption module within the ECU. A decryption module is either the ECU or the chip can be arranged to decrypt encrypted signals (using e.g. the Key and output a decrypted signal or message. the ECU may be arranged to receive the decrypted signal/message from the (e.g. decryption module of the injector chip and determine the sensed fuel injection pulse length from the decrypted signal.

When fuel injectors with such chips are initially associated with the ECU, for example during vehicle or engine assembly, a learning mode is activated. Whilst in the learning mode, an Encryption Key Generator module of the ECU may generates a Key, which is stored on a memory device (not shown) of the ECU. The Key may be sent or broadcast to the injector chip and stored in a memory device (not shown). The stored Key may be used d by the encryption in the chip on the injector.

Example 1

The following shows one detailed example of the invention: At engine start, an exchange occurs between the ECU and the injector chip in order to verify that the correct learnt components are present. The exchange involves the ECU sending a randomly generated data message to the injector chip, and the injector chip generating a response data message using the previously learnt Key. The injector chip transmits the response data message to the ECU and the ECU processes the response data message using the previously stored Key. If the response data message matches the randomly generated data message, then the ECU verifies that the Key corresponds to the Key exchanged during the learning process, i.e. that the correct injector chip is present. When the ECU has verified that the correct injector chip is present, the system commences exchanging encrypted pulse length data. In the event that the ECU determines that the response is incorrect, a

recovery strategy may be entered. The recovery strategy may prevent engine starting or activate an alternative operating mode, such as an engine speed control mode in which the engine speed is a function of the driver pedal position or fixed at a predetermined value.

The encryption process may use either a single encryption Key process to ensure that the data transfer is secure or may use a dual key process such as that described below. The pulse length data is encrypted using the Key (i.e. the learnt Key) and a second encryption key, which is hereinafter referred to as a "Period Specific Key". The Period Specific Key is also generated by the Encryption Key generator 38 of the ECU and provided to the injector chip. The function of the Period Specific Key is to alter the encryption algorithm during engine running thus enabling the system to detect unauthorised inference with the system components during engine running. The Period Specific Key is periodically updated, i.e. a new Period Specific Key is generated and exchanged with the injector chip at a frequency determined by a system calibration device (not shown). For example, the Period Specific Key may be fixed for a complete engine-running period, or updated one or more times during that period.

The data message provided to the ECU from the injector chip comprises the encrypted pulse length data. During normal running, the decryption unit of the ECU decrypts the encrypted data message and provides the decrypted data message to the injector chip. The value of the decrypted data message is used as the measured pulse length. In the event of the system determining that the received pulse length message is incorrect, the system will enter a recovery mode. By way of example, a recovery mode may involve the ECU activating an engine speed control mode, as described earlier.

CLAIMS:

1. A method to detect unauthorised hacking or manipulation of a control signal sent to a fuel injector (2) from an Engine Control Unit (ECU) (1), said control signal including control information comprising pulse profile data to be applied to the actuator of a said fuel injector (2), said fuel injector including processor means associated therewith, said processor means adapted to communicate with said ECU (1), comprising:

a) said processor means generating data indicative of at least one parameter of a pulse profile, comprising one or more actual pulses, provided to or implemented by, the actuator in a fuelling cycle;

b) said processor means transmitting a message including said data indicative of said at least one parameter to said ECU (1),

c) said ECU (1) comparing the at least one parameter in said data with said corresponding parameters of the control signal sent to said fuel injector (2) to determine if unauthorised alteration has occurred.

2. A method as claimed in claim 1 wherein said data indicative of said at least one parameter sent to the ECU (1) is provided in an encrypted form or message.

3. A method as claimed in claim 2 wherein said processor means encrypts the data and/or message.

4. A method as claimed in claims 1 to 3 including the initial step of sending a message request by the ECU (1) to said injector (2) for processor means to transmit said data indicative of said at least one parameter.

5. A method as claimed in claim 4 wherein said message request includes a message count or number, and said message transmitted to the ECU includes the message count or number.

6. A method as claimed in claim 2 to 5 wherein said encryption uses an encryption key sent to the processor means by the ECU.

7. A method as claimed in claims 1 to 6 wherein said pulse profile parameter(s) includes parameter(s) indicative of the number, magnitude or period of said one or more pulses applied, or implemented by said actuator in a fueling cycle.;

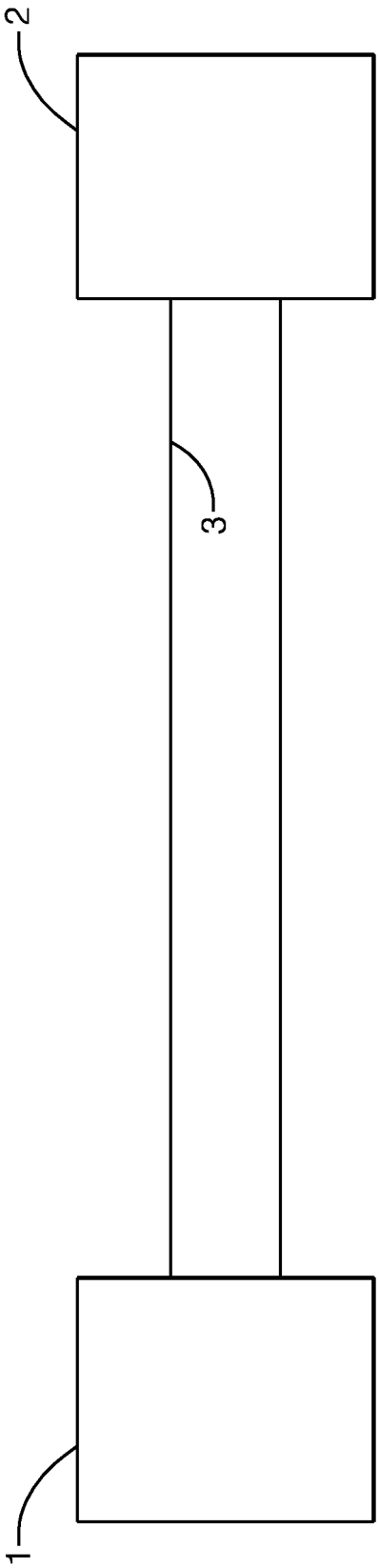

FIG. 1

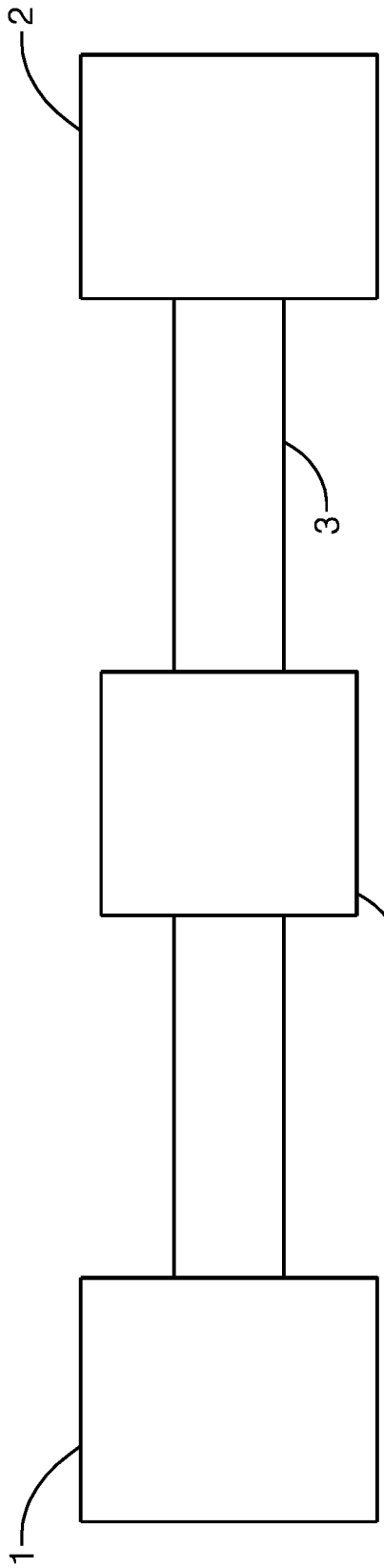

FIG. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/063505

A. CLASSIFICATION OF SUBJECT MATTER
INV. F02D41/22 H04L9/32 H04L29/06
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)
F02D H04L

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 Y	DE 197 28 841 A1 (BOSCH GMBH ROBERT [DE]) 4 February 1999 (1999-02-04) figure 1 column 1, line 30 - column 3, line 67 -----	1-3,6,7 4,5
A	FR 2 890 116 A1 (BOSCH GMBH ROBERT [DE]) 2 March 2007 (2007-03-02) figure 1 page 1, line 2 - page 1, line 6 page 2, line 1 - page 2, line 17 page 4, line 22 - page 5, line 5 -----	1-7
A	EP 2 194 257 A1 (DELPHI TECH HOLDING SARL [LU]) 9 June 2010 (2010-06-09) paragraphs [0004], [0010], [0012], [0014], [0022], [0032] -----	1-7

-/--

[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
31 July 2017	09/08/2017

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	Le Bihan, Thomas

1

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/063505

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2010/268949 A1 (SCHUETZE TORSTEN [DE]) 21 October 2010 (2010-10-21) paragraphs [0004], [0010], [0011], [0013], [0038] -----	4,5
A	EP 1 245 453 A2 (AUDI AG [DE]) 2 October 2002 (2002-10-02) paragraph [0023]; figure 1 -----	1-7
A	US 2013/104231 A1 (NINER ROD [US] ET AL) 25 April 2013 (2013-04-25) paragraphs [0005], [0014], [0015], [0017]; claims 1-5 -----	1-7
A	US 2006/093144 A1 (REINELT WOLFGANG [DE]) 4 May 2006 (2006-05-04) paragraphs [0009], [0044] - [0049]; figure 1 -----	1-7

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2017/063505

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19728841 A1	04-02-1999	NONE	
FR 2890116 A1	02-03-2007	CN 1920281 A	28-02-2007
		DE 102005039760 A1	01-03-2007
		FR 2890116 A1	02-03-2007
EP 2194257 A1	09-06-2010	EP 2194257 A1	09-06-2010
		JP 5643765 B2	17-12-2014
		JP 2012511116 A	17-05-2012
		US 2011246047 A1	06-10-2011
		WO 2010063642 A1	10-06-2010
US 2010268949 A1	21-10-2010	DE 102009002396 A1	21-10-2010
		US 2010268949 A1	21-10-2010
EP 1245453 A2	02-10-2002	DE 10111286 A1	19-09-2002
		EP 1245453 A2	02-10-2002
US 2013104231 A1	25-04-2013	CN 103078836 A	01-05-2013
		US 2013104231 A1	25-04-2013
US 2006093144 A1	04-05-2006	DE 102004036810 A1	23-03-2006
		EP 1622320 A2	01-02-2006
		US 2006093144 A1	04-05-2006