(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 150 460 A1**

# (12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
**05.04.2017 Bulletin 2017/14**

(51) Int Cl.:
***B61L 15/00*** *(2006.01)* ***B61L 27/00*** *(2006.01)*

(21) Application number: **15306545.3**

(22) Date of filing: **30.09.2015**

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

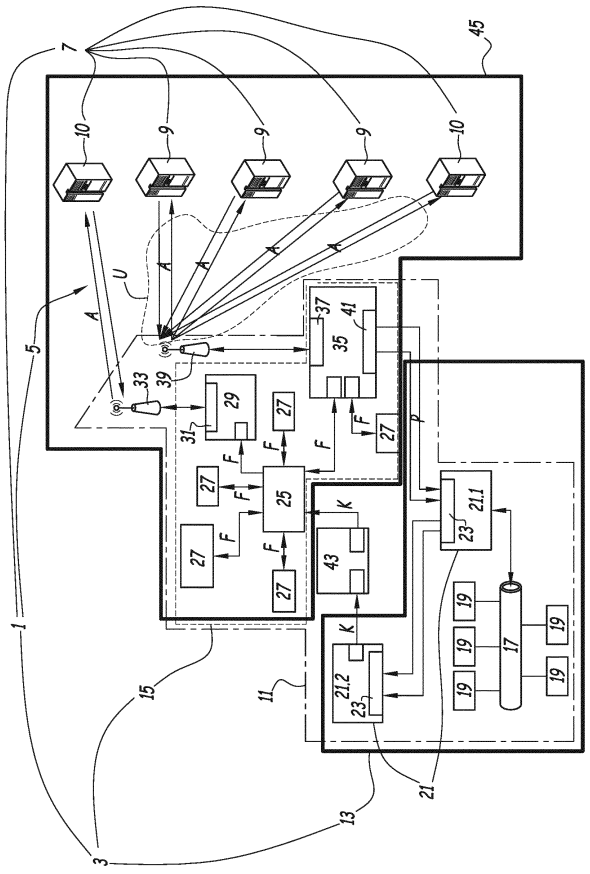
(71) Applicant: **ALSTOM Transport Technologies**
**93400 Saint-Ouen (FR)**

(72) Inventors:
- **FELLER, Reiner**
  **38116 Braunschweig (DE)**
- **VETTER, Jörg**
  **38300 Wolfenbüttel (DE)**
- **TIMME, Michael**
  **38108 Braunschweig (DE)**

(74) Representative: **Lavoix**
**Bayerstrasse 83**
**80335 München (DE)**

## (54) RAILWAY VEHICLE WITH UNIDIRECTIONAL SECURITY GATEWAY FOR SECURE DIAGNOSIS DATA TRANSMISSION

(57) A railway vehicle (11) comprising a safety relevant component (19) providing status data about its operation, a diagnosing device (21) controlling said safety relevant component (19), processing said status data and generating diagnosis data about the railway vehicle condition, a safety relevant data network (13) interconnecting the safety relevant component (19) and the diagnosing device (21), an information data network (15), a transmitting device (29) sending data from the railway vehicle (11) to a remote back office (10), which is part of the information data network (15), and a unidirectional security gateway (43) interconnecting the safety relevant data network (13) and the information data network (15), which only allows data communication from the former to the latter and relays said diagnosis data from said diagnosing device (21) to the information data network (15). Said transmitting device (29) sends the diagnosis data to the back office (10).




EP 3 150 460 A1

## Description

**[0001]** The present invention concerns railway vehicles that are equipped with one or more data buses for exchanging data between numerous components of the railway vehicle.

**[0002]** The article "Informations- und Steuerungstechnik auf Schienenfahrzeugen - Bussysteme im Zug" by Barbara Schmitz, published in the journal "elektronik industrie", 8/9 2008, InnoTrans Special: Bahnelektronik, describes various known bus system architectures for railway vehicles.

**[0003]** These known bus systems are inter alia used to transmit status and diagnosis data from the railway vehicle's subcomponents, such as traction or braking units, to a central diagnosis system, which is located for example in the driver's cab. The driver of the railway vehicle can then visualise the diagnosis data in his cab via a corresponding display unit. For further details, reference is made to the book "Schienenfahrzeugtechnik" by J. Janicki et al., 2nd edition, Bahn Fachverlag, p. 375.

**[0004]** Lately, train operators have requested train manufacturers to develop a communication system for transmitting said diagnosis data from the railway vehicle to a remote back office. By transmitting the diagnosis data out of the railway vehicle to a back office, the train operator is aware of the railway vehicle's current condition in real time. Hence, the train operator can anticipate necessary repairs and already prepare in advance the maintenance workflow for the railway vehicle's next maintenance stop, thus saving time and increasing efficiency.

**[0005]** However, by providing a communication system for transmitting diagnosis data from the railway vehicle to a remote back office, one creates a point of access for an outsider to the railway vehicle's safety relevant components, such as the traction motors or brakes. As a consequence, the railway vehicle becomes vulnerable to a potential attack from a hacker trying to take over the control of the railway vehicle. This is a serious security risk.

**[0006]** It is therefore an object of the present invention to provide a railway vehicle with tamper proof capabilities for the remote transmission of diagnosis data.

**[0007]** According to the present invention, this object is achieved with a railway vehicle comprising:

- a safety relevant component for safely operating the railway vehicle, such as a traction or a braking unit, said safety relevant component being adapted to provide status data about its operation;
- a processing and diagnosing device for controlling said safety relevant component, for receiving and processing said status data and for generating diagnosis data about the condition of the railway vehicle;
- a safety relevant data network interconnecting the safety relevant component and the processing and diagnosing device;
- an information data network, different from the safety relevant data network, for distributing information data, such as traffic or seat reservation data, inside the railway vehicle;
- a transmitting device for sending data from the railway vehicle to a remote back office, said transmitting device being part of the information data network; and
- a gateway interconnecting the safety relevant data network and the information data network,

wherein said gateway is a unidirectional security gateway, which allows data communication from the safety relevant data network to the information data network and prevents any data communication from the information data network to the safety relevant data network,
wherein said unidirectional security gateway is adapted to relay said diagnosis data from said processing and diagnosing device to the information data network, and
wherein said transmitting device is adapted to send the relayed diagnosis data from the railway vehicle to the remote back office.

**[0008]** By having a unidirectional security gateway between the safety relevant data network and the information data network, it is impossible for a hacker to remotely send control signals to the railway vehicle's safety relevant components and thus to take over control of the railway vehicle. Thanks to the unidirectional security gateway, malicious control signals cannot cross from the information data network to the safety relevant data network.

**[0009]** According to preferred embodiments, the inventive railway vehicle may comprise one, several or all of the following features, in all technically feasible combinations:

- said unidirectional security gateway includes a Field-Programmable Gate Array or FPGA that is programmed to allow only unidirectional data communication from the safety relevant data network to the information data network;
- the unidirectional security gateway further includes a dedicated physical FPGA access port, which is the only way to reprogram the FPGA;
- a receiving device; and
- a diagnosis data requests relaying device interconnecting the receiving device and the safety relevant data network;
  said diagnosis data requests relaying device being adapted to relay a request for diagnosis data received by the receiving device from the back office to the processing and diagnosing device via the safety relevant data network;
- the diagnosis data requests relaying device is only able to send predefined and fixed messages, of which there only is a limited number of different ones, to the processing and diagnosing device via the safety relevant data network;

- the diagnosis data requests relaying device includes a dedicated physical programming access port, which is the only way to reprogram the diagnosis data requests relaying device;
- the safety relevant data network includes a Multifunction Vehicle Bus or MVB and/or the information data network is an Ethernet network;
- the transmitting device and/or the receiving device are adapted to communicate wirelessly with the back office, in particular via radio waves using e.g. the GSM standard;
- the railway vehicle is an electric multiple unit, preferably for passenger transport.

**[0010]** A preferred embodiment of the present invention will not be described in detail with reference to the only drawing, which is a block diagram of a communication network according to the invention, including a railway vehicle's wired communication network, a wireless network and a plurality of remote back offices.

**[0011]** The figure represents a communication network 1 comprising a wired communication network 3, a wireless network 5 and an array 7 of remote back offices 9, 10.

**[0012]** The wireless network 5 may for example be a radio network using e.g. the GSM standard.

**[0013]** The remote back offices are preferably implemented in the form of remote servers 9, 10. Each remote server 9, 10 communicates bi-directionally with the wired communication network 3 via the wireless network 5, as indicated by the arrows A. Each remote server 9, 10 has a different function. One remote server 9 may for example manage the seat reservation in the railway vehicle and exchange reservation data with the wired communication network 3. The remote servers 10 (top and bottom of the figure) are diagnosis servers that receive or request diagnosis data from the wired communication network 3.

**[0014]** The reference sign U designates a common wireless interface with a single antenna and modem that is shared by four of the five remote servers 9, 10.

**[0015]** The wired communication network 3 is located in a railway vehicle. The boundaries of the railway vehicle are represented by the dashed line 11. The railway vehicle may for example be an electric multiple unit, preferably for passenger transport.

**[0016]** The wired communication network 3 includes a safety relevant data network 13 (identified by the solid line) and an information data network 15 (identified by the chain-dotted line).

**[0017]** The safety relevant data network 13 has a safety relevant data bus 17. Preferably, the safety relevant data bus 17 is a Multifunction Vehicle Bus or MVB.

**[0018]** Several safety relevant components 19 for safely operating the railway vehicle, such as a traction or braking unit, are connected to the MVB 17. At least some of the safety relevant components 19 are adapted to provide status data about their operation. This status data is sent over the MVB 17.

**[0019]** A processing and diagnosing device 21 for controlling said safety relevant components 19, for receiving and processing said status data and for generating diagnosis data about the condition of the railway vehicle is also connected to the MVB 17. The processing and diagnosing device 21 includes a main processing unit or MPU 21.1 and a driver display unit or DDU 21.2. Both the MPU 21.1 and the DDU 21.2 are connected to the MVB 17 via an MVB card 23.

**[0020]** The information data network 15 is used to distribute information data, such as traffic or seat reservation data, inside the railway vehicle. It preferably has a star topology with a central switch 25. It is preferred to implement the information data network 15 in the form of an Ethernet network. The switch 25 is a central hub managing the communication between the various elements of the information data network 15. These elements are all connected to the switch 25, as indicated by the arrows F. Some of these elements are terminal information equipment 27, such as a dynamic passenger information unit or a video camera.

**[0021]** The information data network 15 also includes a transmitting device 29 that is connected to the switch 25. Preferably, the transmitting device 29 is a transceiver with a modem 31. The transceiver 29 is connected to a radio antenna 33 so that it can communicate wirelessly with one of the remote diagnosis servers 10.

**[0022]** The information data network 15 also includes a receiving device 35 that is connected to the switch 25. Preferably, the receiving device 35 is a Passenger Information System controller or PIS controller. The PIS controller 35 is configured for bidirectional radio communication with one of the remote diagnosis servers 10 and the remote servers 9. For this purpose, the PIS controller 35 has a modem 37 and is connected to a radio antenna 39.

**[0023]** A diagnosis data requests relaying device 41, such as a specially modified MVB card, interconnects the PIS controller 35 and the safety relevant data network 13. The MVB card 41 is adapted to relay a request for diagnosis data received by the PIS controller 35 from the remote diagnosis server 10 to the MPU 21.1 via the safety relevant data network 13, as indicated by the arrows P.

**[0024]** The MVB card 41 has a special design such that it is only able to send predefined and fixed messages, of which there only is a limited number of different ones, to the MPU 21.1 via the safety relevant data network 13.

**[0025]** In order to prevent any remote hacking of the MVB card 41, the same includes a dedicated physical programming access port, which is the only way to reprogram the MVB card 41.

**[0026]** A unidirectional security gateway 43 interconnects the DDU 21.2 and the Ethernet network 15. As indicated by the arrows K, the unidirectional security gateway 43 allows data communication from the DDU 21.2 to the information Ethernet network 15 but prevents any data communication from the information Ethernet network 15 to the DDU 21.2.

**[0027]** The function of the unidirectional security gate-

way 43 is to relay railway vehicle diagnosis data from said DDU 21.2 to the information Ethernet network 15.

**[0028]** Preferably, said unidirectional security gateway 43 includes a Field-Programmable Gate Array or FPGA that is programmed to allow only unidirectional data communication from the DDU 21.2 to the information Ethernet network 15.

**[0029]** In order to prevent any remote hacking of the unidirectional security gateway 43, the same has a dedicated physical FPGA access port, which is the only way to reprogram the FPGA.

**[0030]** Thanks to the unidirectional security gateway 43, the communication network 1 is clearly split up into a first secure sub-network corresponding to the MVB network 13, and a second unsecure sub-network (indicated by the polygon 45 in solid lines) corresponding to the Ethernet network 15 and the wireless network 5.

## Claims

**1.** A railway vehicle (11) comprising:

- a safety relevant component (19) for safely operating the railway vehicle, such as a traction or a braking unit, said safety relevant component (19) being adapted to provide status data about its operation;
- a processing and diagnosing device (21) for controlling said safety relevant component (19), for receiving and processing said status data and for generating diagnosis data about the condition of the railway vehicle (11);
- a safety relevant data network (13) interconnecting the safety relevant component (19) and the processing and diagnosing device (21);
- an information data network (15), different from the safety relevant data network (13), for distributing information data, such as traffic or seat reservation data, inside the railway vehicle (11);
- a transmitting device (29) for sending data from the railway vehicle (11) to a remote back office (10), said transmitting device (29) being part of the information data network (15); and
- a gateway (43) interconnecting the safety relevant data network (13) and the information data network (15),

wherein said gateway (43) is a unidirectional security gateway, which allows data communication from the safety relevant data network (13) to the information data network (15) and prevents any data communication from the information data network (15) to the safety relevant data network (13),

wherein said unidirectional security gateway (43) is adapted to relay said diagnosis data from said processing and diagnosing device (21) to the information data network (15), and

wherein said transmitting device (29) is adapted to send the relayed diagnosis data from the railway vehicle (11) to the remote back office (10).

**2.** The railway vehicle (11) of claim 1, wherein said unidirectional security gateway (43) includes a Field-Programmable Gate Array or FPGA that is programmed to allow only unidirectional data communication from the safety relevant data network (13) to the information data network (15).

**3.** The railway vehicle (11) of claim 2, wherein the unidirectional security gateway (43) further includes a dedicated physical FPGA access port, which is the only way to reprogram the FPGA.

**4.** The railway vehicle (11) of any one of the previous claims, further comprising:

- a receiving device (35); and
- a diagnosis data requests relaying device (41) interconnecting the receiving device (35) and the safety relevant data network (13),

said diagnosis data requests relaying device (41) being adapted to relay a request for diagnosis data received by the receiving device (35) from the back office (10) to the processing and diagnosing device (21) via the safety relevant data network (13).

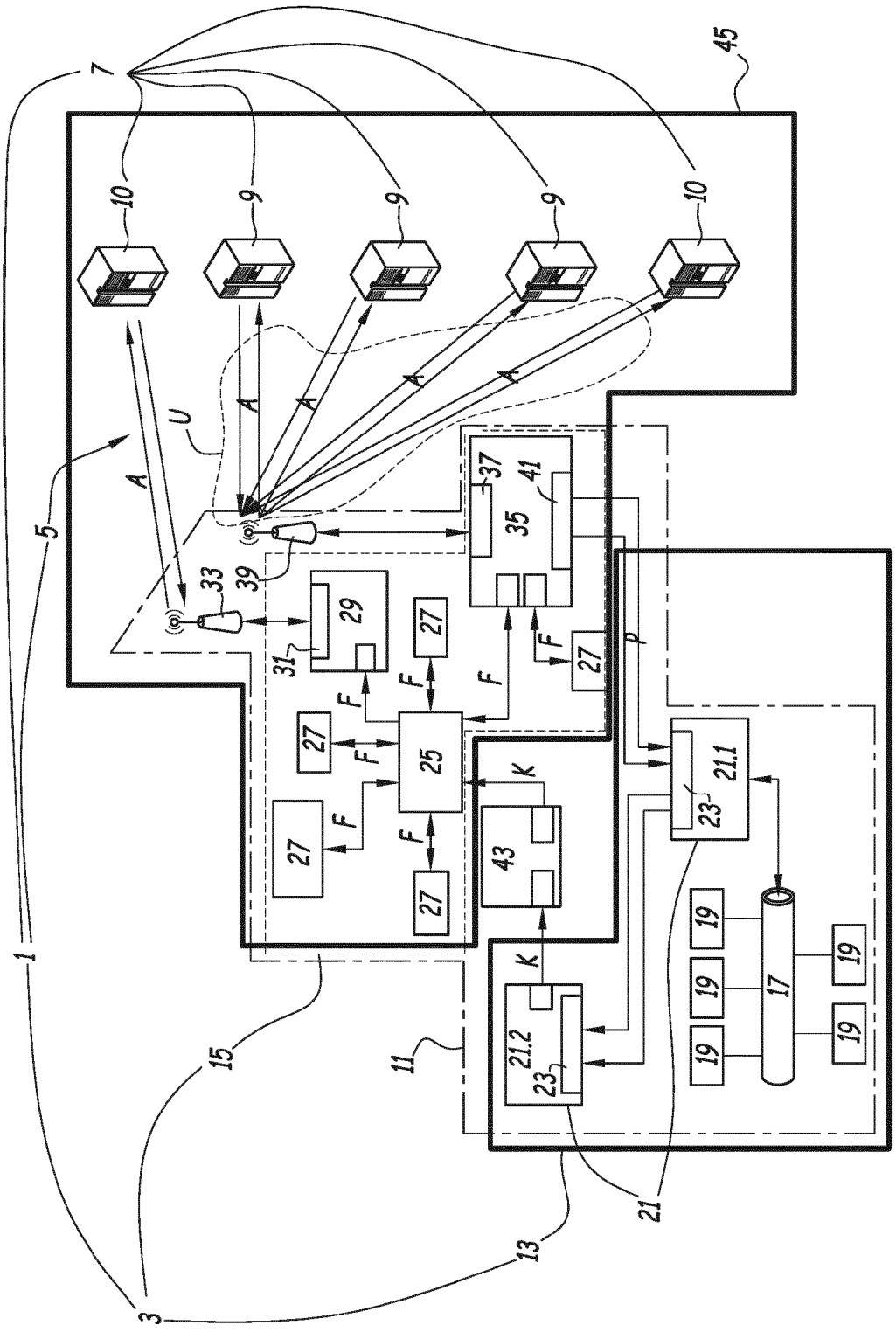
**5.** The railway vehicle (11) of claim 4, wherein the diagnosis data requests relaying device (41) is only able to send predefined and fixed messages, of which there only is a limited number of different ones, to the processing and diagnosing device (21) via the safety relevant data network.

**6.** The railway vehicle (11) of claim 4 or 5, wherein the diagnosis data requests relaying device (41) includes a dedicated physical programming access port, which is the only way to reprogram the diagnosis data requests relaying device.

**7.** The railway vehicle (11) of any one of the previous claims, wherein the safety relevant data network (13) includes a Multifunction Vehicle Bus or MVB and/or the information data network (15) is an Ethernet network.

**8.** The railway vehicle (11) of any one of the previous claims, wherein the transmitting device (29) and/or the receiving device (35) are adapted to communicate wirelessly with the back office (10), in particular via radio waves using e.g. the GSM standard.

**9.** The railway vehicle (11) of any one of the previous claims, wherein the railway vehicle is an electric multiple unit, preferably for passenger transport.


7
45
10
9
9
9
10
A
A
A
A
A
U
5
37
41
35
33
39
29
31
27
F
F
F
27
F
27
25
K
27
F
F
43
27
21.1
23
19
19
19
17
19
19
K
21.2
23
11
15
13
21
3
1

Europäisches Patentamt
European Patent Office
Office européen des brevets

# EUROPEAN SEARCH REPORT

Application Number
EP 15 30 6545

## DOCUMENTS CONSIDERED TO BE RELEVANT

| Category | Citation of document with indication, where appropriate, of relevant passages | Relevant to claim | CLASSIFICATION OF THE APPLICATION (IPC) |
|---|---|---|---|
| X<br>Y | WO 2014/129107 A1 (TOYOTA MOTOR CO LTD [JP]; MORIYA TOMOKAZU [JP]; GOTO HIDEKI [JP]; YURA) 28 August 2014 (2014-08-28)<br>* paragraph [0008] - paragraph [0131]; figures 1-11 * | 1,4,5,7, 8<br>2,3,6,9 | INV.<br>B61L15/00<br>B61L27/00 |
| X | US 2014/107875 A1 (BEYER RALF [DE] ET AL) 17 April 2014 (2014-04-17)<br>* paragraph [0014] - paragraph [0093]; figures 1-3 * | 1,7,8 | |
| Y | US 2006/203844 A1 (KNITTLE CURTIS D [US] ET AL) 14 September 2006 (2006-09-14)<br>* paragraphs [0017], [0021] * | 2,3 | |
| Y | US 2014/172422 A1 (HEFETZ YARON [IL]) 19 June 2014 (2014-06-19)<br>* paragraph [0036] * | 3,6 | |
| A | ZUR BONSEN G A ED - DECOTIGNIE J-D: "The Multifunction Vehicle Bus (MVB)", FACTORY COMMUNICATION SYSTEMS, 1995. WFCS '95, PROCEEDINGS., 1995 IEEE INTERNATIONAL WORKSHOP ON LEYSIN, SWITZERLAND 4-6 OCT. 1995, NEW YORK, NY, USA,IEEE, US, 4 October 1995 (1995-10-04), pages 27-34, XP010154281, ISBN: 978-0-7803-3059-7<br>* page 1 * | 7 | TECHNICAL FIELDS SEARCHED (IPC)<br>B61L |
| Y | WO 00/52851 A1 (SPRINGBOARD WIRELESS NETWORKS [CA]; OPREA ALEX [CA]; ELLIOTT CHARLES [] 8 September 2000 (2000-09-08)<br>* page 24, paragraph 3 * | 9 | |

The present search report has been drawn up for all claims

| Place of search | Date of completion of the search | Examiner |
|---|---|---|
| Munich | 4 March 2016 | Mäki-Mantila, M |

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

## ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 15 30 6545

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

04-03-2016

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| WO 2014129107 A1 | 28-08-2014 | CN 105009546 A | 28-10-2015 |
| | | EP 2959654 A1 | 30-12-2015 |
| | | JP 5838983 B2 | 06-01-2016 |
| | | JP 2014165641 A | 08-09-2014 |
| | | US 2015372975 A1 | 24-12-2015 |
| | | WO 2014129107 A1 | 28-08-2014 |
| US 2014107875 A1 | 17-04-2014 | CA 2837139 A1 | 29-11-2012 |
| | | CN 103547975 A | 29-01-2014 |
| | | DE 102011076350 A1 | 29-11-2012 |
| | | EP 2684154 A2 | 15-01-2014 |
| | | RU 2013156572 A | 27-06-2015 |
| | | US 2014107875 A1 | 17-04-2014 |
| | | WO 2012159940 A2 | 29-11-2012 |
| US 2006203844 A1 | 14-09-2006 | US 2006203844 A1 | 14-09-2006 |
| | | WO 2006099236 A1 | 21-09-2006 |
| US 2014172422 A1 | 19-06-2014 | NONE | |
| WO 0052851 A1 | 08-09-2000 | AU 2788800 A | 21-09-2000 |
| | | CA 2263031 A1 | 26-08-2000 |
| | | EP 1166465 A1 | 02-01-2002 |
| | | NZ 513887 A | 28-09-2001 |
| | | WO 0052851 A1 | 08-09-2000 |

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

## REFERENCES CITED IN THE DESCRIPTION

*This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.*

### Non-patent literature cited in the description


- **BARBARA SCHMITZ.** Informations- und Steuerungstechnik auf Schienenfahrzeugen - Bussysteme im Zug. *journal "elektronik industrie",* August 2008 **[0002]**
- **J. JANICKI et al.** Schienenfahrzeugtechnik. Bahn Fachverlag, 375 **[0003]**