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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 April 2013 (11.04.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/050409 A1

(51) International Patent Classification:
G07C 9/00 (2006.01) *E05B 49/00* (2006.01)
B60R 25/00 (2013.01)

(21) International Application Number:
PCT/EP2012/069520

(22) International Filing Date:
3 October 2012 (03.10.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1641/11 7 October 2011 (07.10.2011) CH

(71) Applicant *(for all designated States except US)*: **ASSA ABLOY CZECH & SLOVAKIA S.R.O.** [CZ/CZ]; Odštepný závod FAB Vehicle Security, V. Opatrného 1050, 517 21 Týnište nad Orlicí (CZ).

(72) Inventors; and
(71) Applicants *(for US only)*: **MUTTI, Carlo Secondo** [CH/CH]; Via Gianed 9, CH-6945 Origlio (CH). **SPEDALIERE, Davide** [IT/IT]; Via Cesare Battisti 26/H, I-28823 Ghiffa (IT).

(74) Agent: **FRISCHKNECHT, Harry**; Isler & Pedrazzini AG, Postfach 1772, CH-8027 Zürich (CH).

(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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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, 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, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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

(54) Title: SOLUTIONS FOR RELAY ATTACKS ON PASSIVE KEYLESS ENTRY AND GO

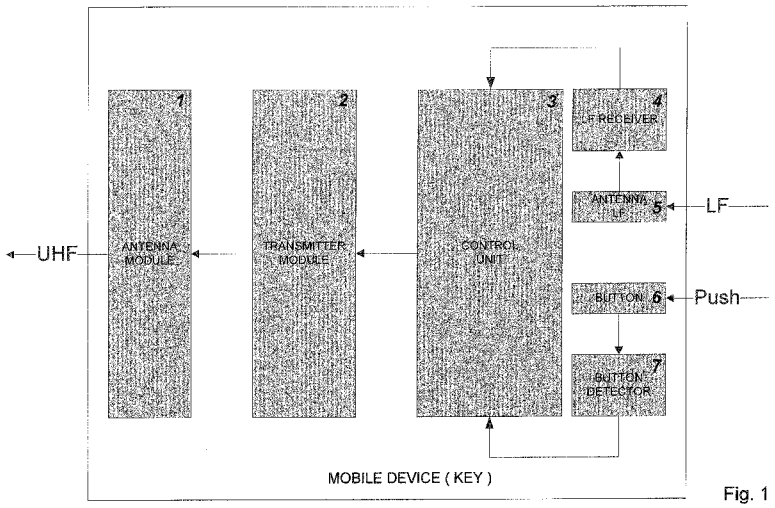


Fig. 1

(57) Abstract: A passive entry system, in particular for a motor vehicle, comprising: a mobile device to be carried by a user, said mobile device comprising a low-frequency transceiver for short range communication, an ultra-high-frequency transceiver for long range communication and information concerning access, such as an access code, which is transmittable by said transceivers; and a locking device which is to be unlocked by the mobile device, said locking device comprising a low-frequency transceiver for short-range communication and an ultra-high frequency transceiver for long range communication to receive said information concerning access, such the access code. The transceivers of the mobile device communicates with the transceiver of the locking device and exchange information concerning access, such as said access code,to the locking system via the respective transceivers, wherein the communication range of the ultra-high-frequency transceiver of the mobile device is limited to a short range in a normal operating mode of the mobile device.

WO 2013/050409 A1

Title

SOLUTIONS FOR RELAY ATTACKS ON PASSIVE KEYLESS ENTRY and GO

TECHNICAL FIELD OF THE INVENTION

The present invention relates to a system for preventing relay attacks against radio frequency based locking systems according to preamble of claim 1.

PRIOR ART

Nowadays the major issue regarding the Passive Keyless Entry and/or Passive Keyless Go (PKE/GO) system in modern vehicles is the "Relay Attack". Using the system characteristics, with very inexpensive tools, it is possible to open and to start all the new vehicles with PKE/GO system.

Only by amplifying and extend the range of the LF signal, generated by the vehicle and used to communicate with the key, it is possible to open and to start the vehicle even if the owner is far away the vehicle, all without any suspect from the key owner.

This problem has been described in detail in a publication by the authors Aurelien Francillon, Boris Danev, Srdjan Capkun of ETH Zürich having the title "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Vehicles".

In Figure 1 there is shown a mobile device, such as a key which can be used in PKE-Systems. In summary the PKE-System usually comprises the following steps in order to open and to start a car:

- triggering the system (e.g. touching the door handles), the vehicle turn on the LF antenna and sends the commands to the Mobile Device (key); and
- the key is awake through LF signal (***4,5***) and answers (***1,2,3***) via UHF directly to the vehicle with the right command to unlock the door.

The same applies when the start/stop button inside the vehicle for the Passive Keyless Go is pushed.

The LF is a short range communication, usually not more than 1-2m, meanwhile the UHF range is up to 100m. This is illustrated in figure 2.

The relay attack consists to extend the LF range ***X***, so you can open and start the vehicle even if the key owner is far away but still in the range ***Z*** of the UHF as it is also described in the above mentioned publication.

To make an illustrative example: the owner sits in a restaurant and the vehicle just parked outside the restaurant. The thief with the relay, within the range ***X***, touches the door handle, the vehicle starts the communication procedure, the relay extends the LF range, the remote key is awake from the LF signal and answers via UHF signal. The vehicle unlocks the door, the thief enters, push the start button, the LF starts again the communication, extended by the relay, the key answers, and the vehicle engine starts.....and the vehicle is gone!

SUMMARY OF THE INVENTION

Starting from this prior art it is an object of the present invention to provide a locking system having a higher security against such relay attacks.

This object is solved by claim 1. Therefore a passive entry system, in particular for a motor vehicle comprising:

- a mobile device to be carried by a user, said mobile device comprising a low-frequency transceiver for short range communication, an ultra-high-frequency transceiver for long range communication and information concerning access, such as an access code, which is transmittable by said transceivers; and
- a locking device which is to be unlocked by the mobile device, said locking device comprising a low-frequency transceiver for short-range communication and an ultra-high frequency transceiver for long range communication to receive said information concerning access, such as the access code.

The transceivers of the mobile device communicates with the transceivers of the locking device and exchange information concerning access, such as said access code, to the locking system via the respective transceivers. The communication range of the ultra-high-frequency transceiver of the mobile device is limited to a short range in a normal operating mode of the mobile device.

The limitation of the range has the advantage that communication of the ultra-high-frequency transceiver becomes limited to a restricted range. Therefore the signal from said transceiver will only be sent within this short range, which means that the mobile device has to be physically close to the locking device in order to send the information with which the locking device will be unlocked to the locking device. In case the mobile device is far away from the car and receives a fraud signal that originates from the car and has been amplified by a fraud relay, the mobile device may send an answer, for example a code to unlock the locking device, to this signal, but the answer will not reach the locking device.

The term limitation is preferably to be understood as physical limitation which means that the mobile device is only able to send the access information only within a short physical range such as less than 10 meters or less than 2 meters for example.

Preferably the mobile device comprises means such as a button, to activate the transmission of the information concerning access, wherein upon a manual actuation of said means of the mobile device the condition of the mobile device is changeable from said normal operating mode to a manual mode, wherein in said manual mode the long range communication of the ultra-high-frequency transceiver of the mobile device is active such that access information is transmittable over the long range.

Hence the mobile device can have two operating modes. In the normal operating mode the mobile device and the locking device are protected against relay attacks since the long range communication is deactivated. In the manual mode long range communication is activated and long range exchange of access information will take place upon manual and deliberate actuation of the mobile device by the user.

Typical values of low-frequency are usually 125 kHz and of high-frequency are usually 315 MHz or 433 MHz or 868 MHZ or 915 MHz.

Further embodiments of the invention are laid down in the dependent claims.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the invention are described in the following with reference to the drawings 3 to 6, which are for the purpose of illustrating the present preferred embodiments of the invention and not for the purpose of limiting the same. In the drawings,

Fig. 1 shows a schematic view of a mobile device, such as a key to access a car,
Fig. 2 shows a schematic view of an overall system of a relay attack as described prior art chapter,
Fig. 3 shows a schematic view of an overall system according to the present invention;
Fig. 4 shows a first embodiment of a mobile device according to the present invention;
Fig. 5 shows a second embodiment of a mobile device according to the present invention; and
Fig. 6 shows a third embodiment of a mobile device according to the present invention.

DESCRIPTION OF PREFERRED EMBODIMENTS

Preferred embodiments of the invention are described in the following with reference to the drawings or figures, respectively, which are for the purpose of illustrating the present preferred embodiments of the invention and not for the purpose of limiting the same.

The way to solve this kind of relay attacks on PKE/GO system, is putting some countermeasure on the communication between the key and the vehicle and not vice versa as attempted until now.

The new approach is to limit the communication range ***Z*** as indicated in figure 2 from the key to vehicle via UHF in the PKE/GO system. Therefore the communication range of the ultra-high-frequency transceiver of the mobile device is limited to a short range in a normal operating mode of the mobile device.

This limitation of the communication range could be obtained applying one of the following strategies:

a) reducing key transmission power;
b) increasing the transmission power;
c) adapting key antenna matching network;
d) using different antenna type;
e) using different antenna design;
f) using different antenna gain;
g) any combinations of the above strategies;
h) or any other solution to reduce and limit the communication range.

In this manner, at any requests from the vehicle via LF signal, via relay or not, the key answers only adopting one or more of the above strategies, limiting the UHF range to less than $Y = X+W$ meters.

The mobile unit, preferably a key, can also be operated in a manual mode which is applicable when the user intends to unlock the locking system (e.g. the car) manually. For that reason the mobile unit comprises at least one button which can be activated by the user. When the user presses said button, the above strategies are not applied. Hence the normal operating mode of the mobile device will be changed into a manual mode, resulting in the normal use of the key, with UHF range ***Z***. With other words: Upon a manual actuation the mobile device the condition of the mobile device is changeable from said normal operating mode to a manual mode, wherein in said manual mode the long range communication of the ultra-high-frequency transceiver of the mobile device is activatable. Hence the user can manually unlock the car since the transceiver of mobile unit communicates without a limitation of the range of the ultra-high-frequency channel. This is illustrated in the below.

The invention is valid for Passive Keyless Entry and/or Passive Keyless Go.

According to preferred embodiments the invention can be implemented in the embodiments as described in the following. Preferably the invention can be implemented in a purely hardware embodiment or in a purely software/firmware embodiment or an embodiment in which hardware as well as software/firmware are adapted to the invention. These embodiments will be described in the following with reference to the drawings:

First Embodiment:

In the first embodiment the limitation the range of the ultra-high-frequency transceiver of the mobile device is limited to a short range in a normal operating mode of the mobile device is provided by means of hardware components.

Figure 4 illustrates a possible embodiment, in particular said first embodiment, of a mobile device in which the range of the ultra-high-frequency transceiver is limited accordingly.

The solutions, using only hardware implementation to limit the communication range ***Z*** from the key to vehicle via UHF, are preferably obtained by:

a) reducing key transmission power;
   - automatic switch (***2c***) on passive RF path with HW attenuator inside (***2a***) using the same antenna inside (***1***);
   - automatic switch (***2c***) on passive RF path with HW attenuator inside (***2a***) using different antenna inside (***1***);

b) increasing the transmission power;
   - automatic switch (***2c***) on functional RF path with HW amplifier inside (***2b***) using the same antenna inside (***1***);
   - automatic switch (***2c***) on functional RF path with HW amplifier inside (***2b***) using different antenna inside (***1***);

c) adapting key antenna matching network;
   - automatic switch (***2c***) on passive RF path with component (resistors, capacitors, inductors) inside (***2a***) with different values using the same antenna inside (***1***);
   - automatic switch (***2c***) on passive RF path with component (resistors, capacitors, inductors) inside (***2a***) with different values using different antenna inside (***1***);

d) using different antenna type;
   - automatic switch (***2c***) either passive or functional RF path using one or more different antenna types inside (***1***);

e) using different antenna design;
   - automatic switch (***2c***) either passive or functional RF path using one or more different antenna design inside (***1***);

f) using different antenna gain;
   - automatic switch (***2c***) either passive or functional RF path using one or more different antenna gain inside (***1***).

g) using any combinations of the above strategies.

Second Embodiment:

In the second embodiment the limitation the range of the ultra-high-frequency transceiver of the mobile device is limited to a short range in a normal operating mode of the mobile device is provided by means of software components, hence by means of a programmed software solution.

Figure 5 illustrates a possible embodiment, in particular said second embodiment, of a mobile device in which the range of the ultra-high-frequency transceiver is limited accordingly.

Using the right software device settings (***3a, 3b***) in the control unit (***3***) is possible to adjust the UHF power transmission:

- By LF request (***4,5***), the control unit (***3***) uses passive software/firmware settings (***3a***), in order to have limited UHF range ***Y***;
- By pushing one of the key buttons (***6,7***), the control unit (***3***) uses functional software/firmware settings (***3b***), in order to have functional UHF range ***Z***;

This implementation could be applied on the existing mobile device (key), without any hardware modifications.

Third Embodiment:

In the third embodiment the limitation the range of the ultra-high-frequency transceiver of the mobile device is limited to a short range in a normal operating mode of the mobile device is provided by means of software components and hardware components.

Figure 6 illustrates a possible embodiment, in particular said third embodiment, of a mobile device in which the range of the ultra-high-frequency transceiver is limited accordingly.

The "mixed" implementation is the most complete solution from optimization point of view, providing more flexibility in term of range ***Y*** selection.

This is achieved by combining strategies described in embodiments 1 and 2.

CLAIMS

1. Passive entry system, in particular for a motor vehicle, comprising:

a mobile device to be carried by a user, said mobile device comprising a low-frequency transceiver for short range communication, an ultra-high-frequency transceiver for long range communication and information concerning access, such as an access code, which is transmittable by said transceivers; and

a locking device which is to be unlocked by the mobile device, said locking device comprising a low-frequency transceiver for short-range communication and an ultra-high frequency transceiver for long range communication to receive said information concerning access, such the access code,

wherein the transceivers of the mobile device communicates with the transceiver of the locking device and exchange information concerning access, such as said access code, to the locking system via the respective transceivers, characterized in that

the communication range of the ultra-high-frequency transceiver of the mobile device is limited to a short range in a normal operating mode of the mobile device.

2. Passive entry system according to claim 1, characterized in that the mobile device comprises means such as a button, to activate the transmission of the information concerning access, wherein upon a manual actuation of said means of the mobile device the condition of the mobile device is changeable from said normal operating mode to a manual mode, wherein in said manual mode the long range communication of the ultra-high-frequency transceiver of the mobile device is active such that access information is transmittable over the long range.

3. Passive entry system according to any of the preceding claims, characterized in that the communication range is limited to a short range in case communication will be initiated by the transceiver of the locking device in particular on the vehicle, wherein said communication is preferably a request of the locking device to the mobile device to send information concerning access.

4. Passive entry system according to any of the preceding claims, characterized in that said limitation of the range of the mobile device is provided by means of

reducing transmission power of the transceiver of the mobile device by changing value and/or number of electronic and/or software parameters in its normal operating mode and/or

increasing transmission power of the transceiver of the mobile device by changing value and/or number of electronic and/or software parameters in in its in manual mode and/or

adapting the antenna matching network of the mobile device by changing value and/or number of electronic components and/or

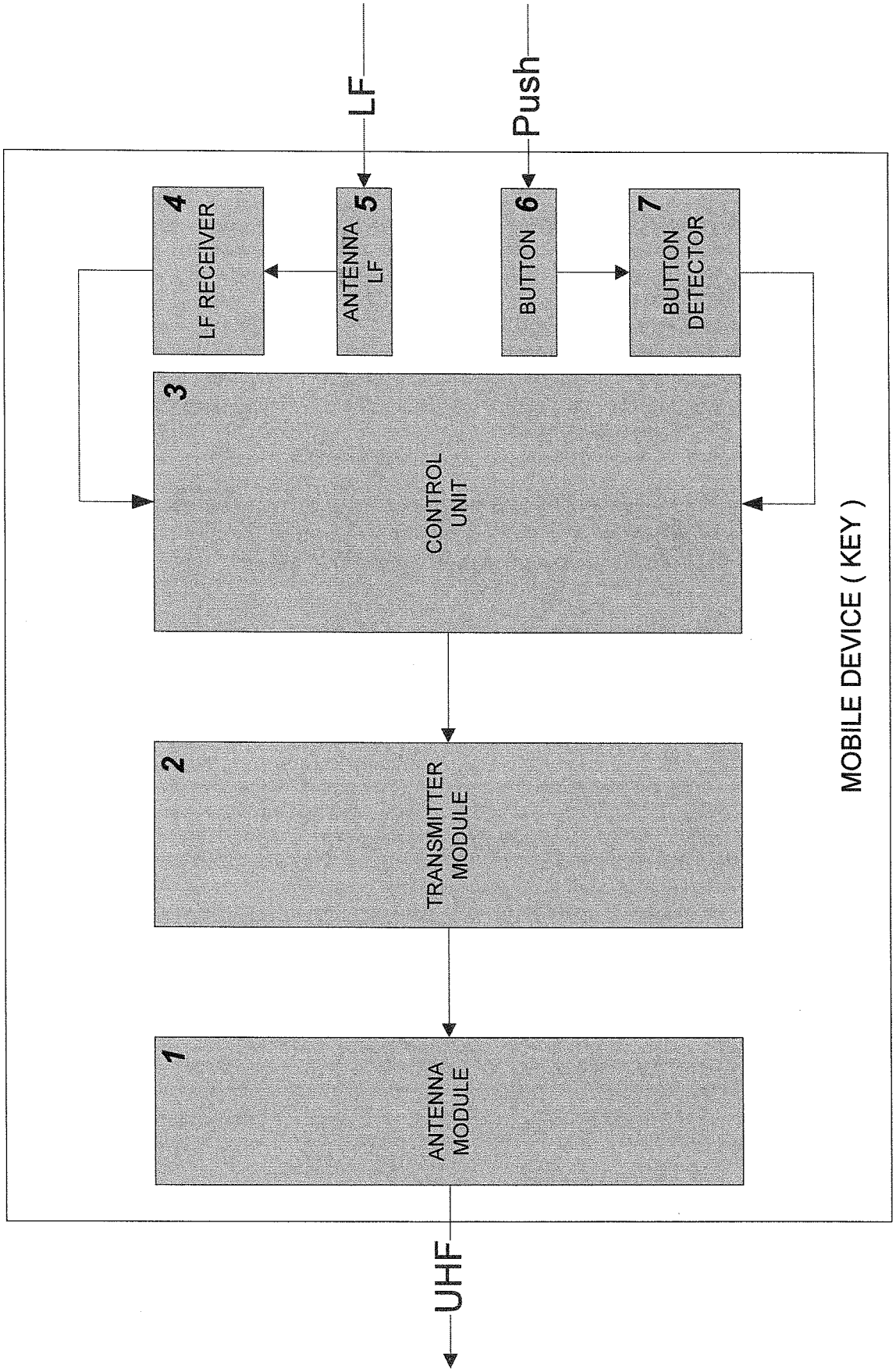
using different antenna types of the mobile device and/or

using different antenna design of the mobile device and/or by using different gain.

5. Passive entry system according to any of the preceding claims, characterized in that said limitation of the range of the mobile device is provided by means of a programmed software solution.

6. Passive entry system according to any of the preceding claims, characterized in that the long range is between 10 meters and 200 meters and in that the short range is between 0 meters and 10 meters, preferably between 0 meters and 5 meters, most preferably between 0 meters and 2 meters.

Fig. 1


LF
Push
4
LF RECEIVER
5
ANTENNA LF
6
BUTTON
7
BUTTON DETECTOR
3
CONTROL UNIT
2
TRANSMITTER MODULE
1
ANTENNA MODULE
MOBILE DEVICE (KEY)
UHF

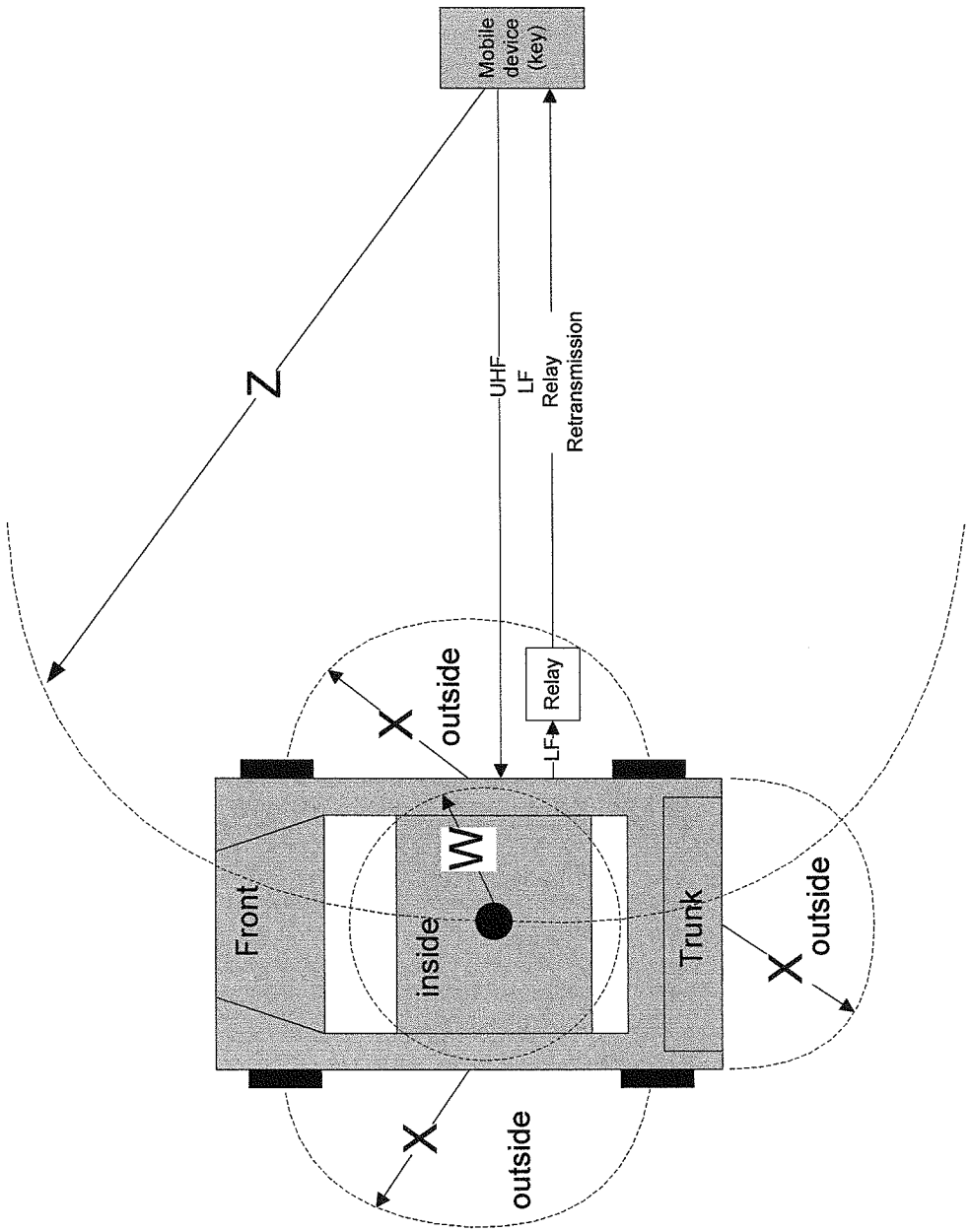

Mobile device (key)
Z
UHF
LF
Relay
Retransmission
Relay
LF
X
outside
W
Front
inside
Trunk
X
outside
X
outside

Fig. 2

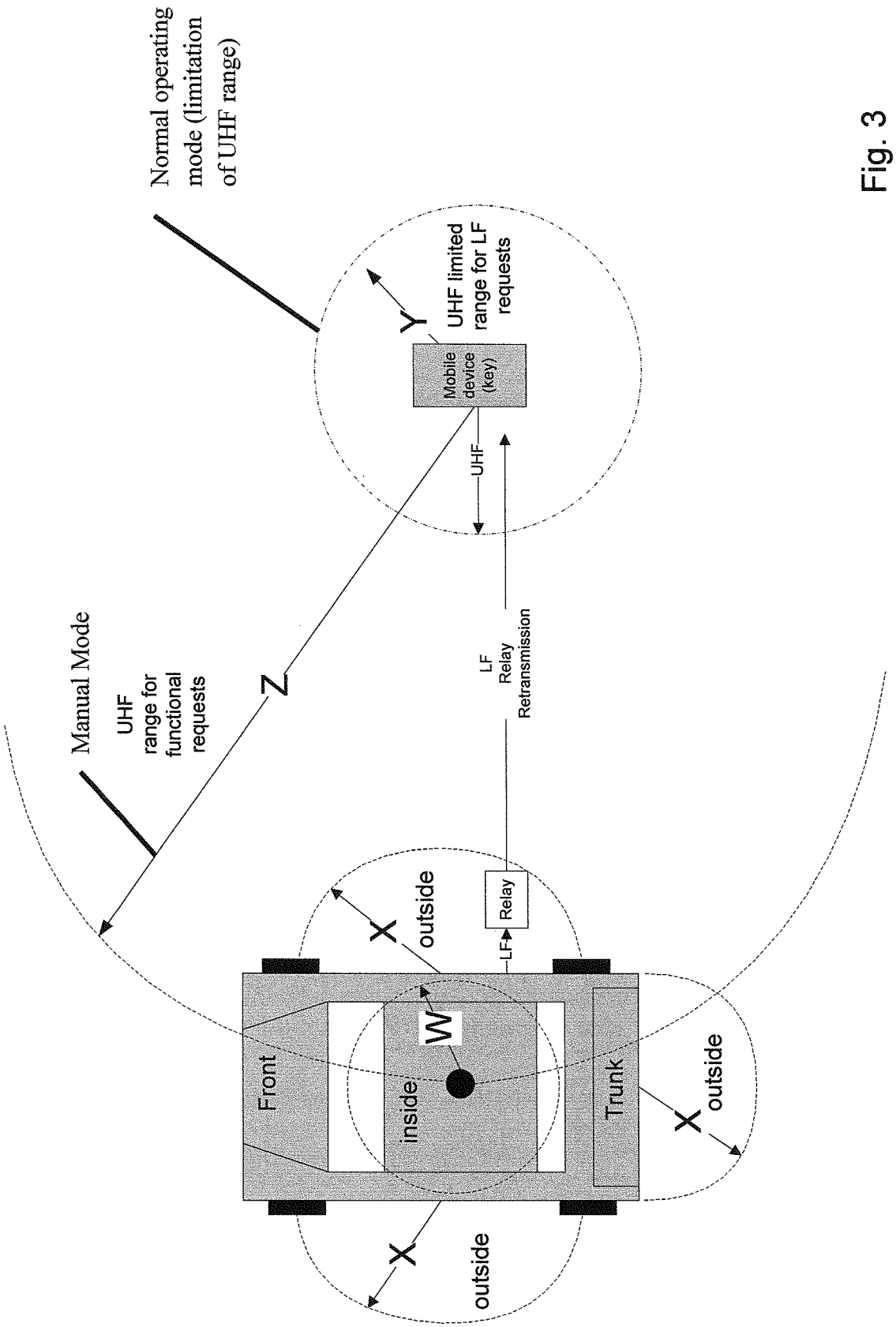

Normal operating mode (limitation of UHF range)
UHF limited range for LF requests
Y
Mobile device (key)
UHF
Manual Mode
UHF range for functional requests
Z
LF Relay Retransmission
Relay
LF
X
outside
Front
inside
W
Trunk
X
outside
X
outside

Fig. 3

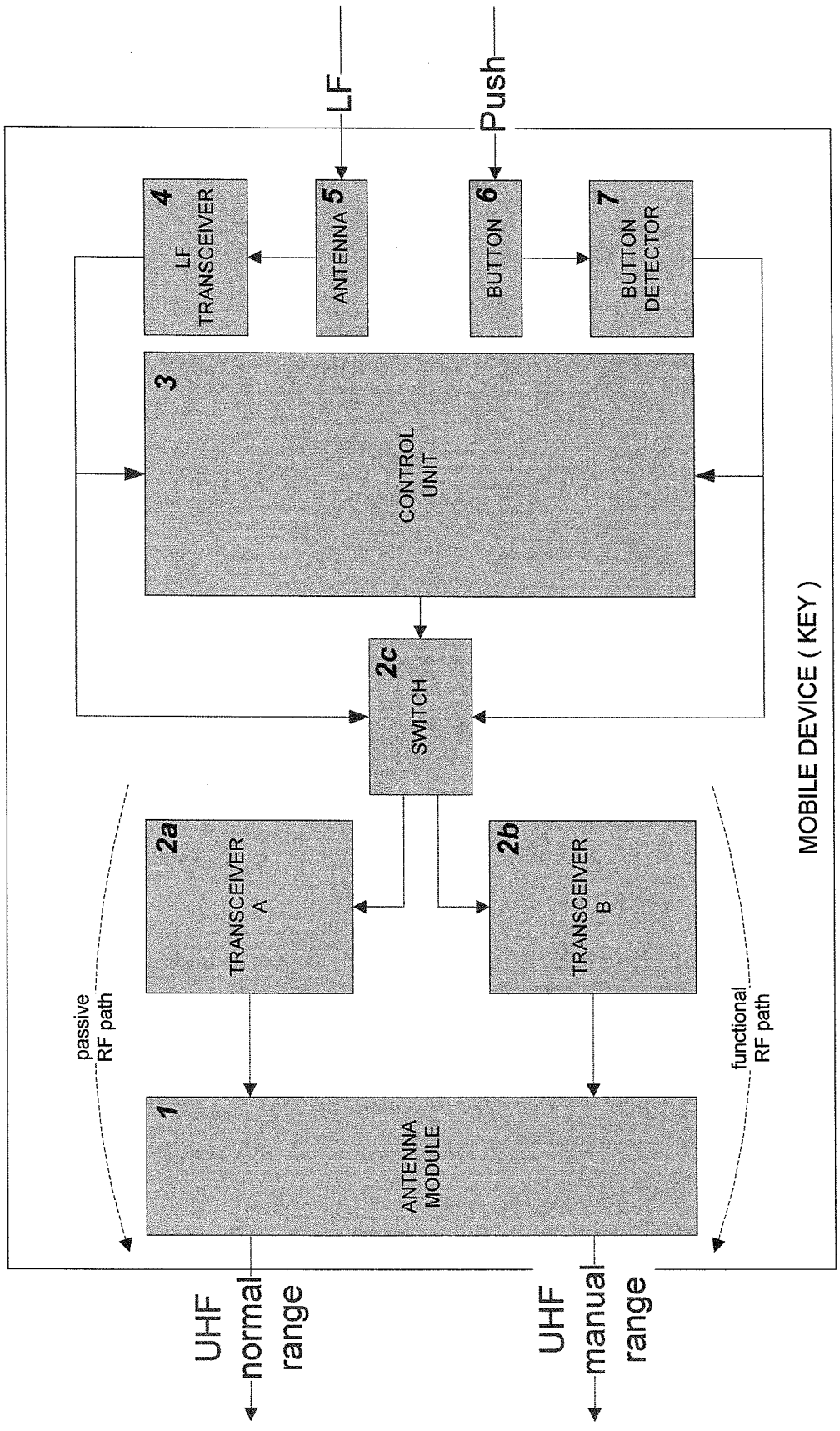
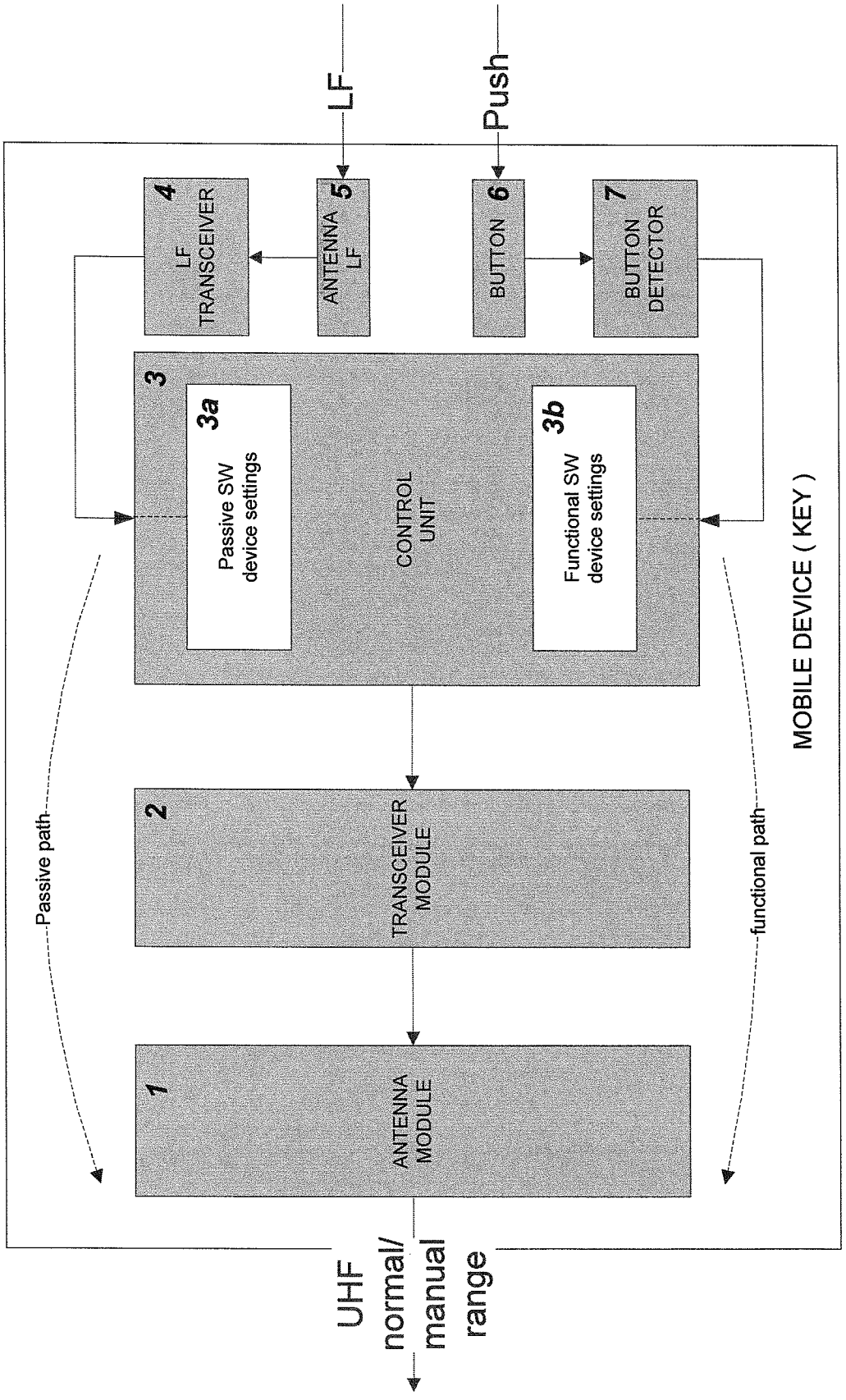

LF
Push
4
LF TRANSCEIVER
5
ANTENNA
6
BUTTON
7
BUTTON DETECTOR
3
CONTROL UNIT
2c
SWITCH
2a
TRANSCEIVER A
2b
TRANSCEIVER B
1
ANTENNA MODULE
passive RF path
functional RF path
MOBILE DEVICE (KEY)
UHF normal range
UHF manual range

Fig. 4

Fig. 5


LF
Push
4
LF TRANSCEIVER
5
ANTENNA LF
6
BUTTON
7
BUTTON DETECTOR
3
3a
Passive SW device settings
CONTROL UNIT
3b
Functional SW device settings
2
TRANSCEIVER MODULE
1
ANTENNA MODULE
Passive path
functional path
MOBILE DEVICE (KEY)
UHF normal/ manual range

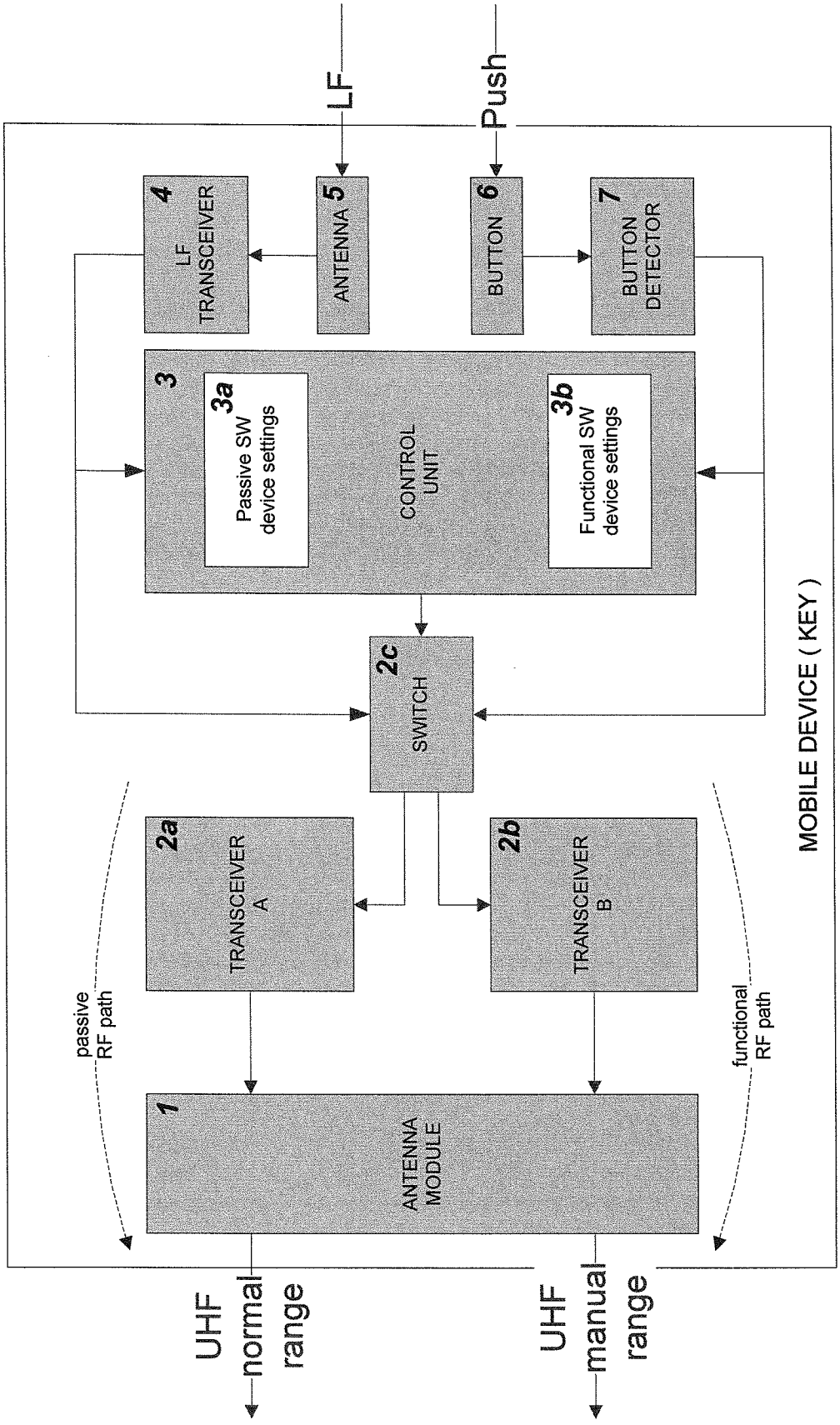

LF
Push
4
LF TRANSCEIVER
5
ANTENNA
6
BUTTON
7
BUTTON DETECTOR
3
3a
Passive SW device settings
CONTROL UNIT
3b
Functional SW device settings
2c
SWITCH
2a
TRANSCEIVER A
2b
TRANSCEIVER B
1
ANTENNA MODULE
passive RF path
functional RF path
MOBILE DEVICE (KEY)
UHF normal range
UHF manual range

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/069520

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07C9/00 B60R25/00 E05B49/00
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)
G07C B60R E05B

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 10 2010 006149 A1 (WEBASTO AG [DE]) 4 August 2011 (2011-08-04) abstract; claims 1,3,5,7; figure 1 paragraphs [0001], [0004], [0005], [0011], [0013] - [0020], [0040] - [0043] -----	1-6
A	US 2006/255911 A1 (TAKI NAOKI [JP] ET AL) 16 November 2006 (2006-11-16) abstract; claims; figures paragraph [0010] - paragraph [0011] paragraph [0023] - paragraph [0047] -----	1-6
A	DE 103 34 625 A1 (SIEMENS AG [DE]) 3 March 2005 (2005-03-03) abstract; claims; figure paragraphs [0001], [0006] - [0018], [0021] - [0030] -----	1-6

-/--

[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
11 December 2012	02/01/2013

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	Rother, Stefan

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/069520

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 10 2004 052904 A1 (SIEMENS AG [DE]) 1 June 2006 (2006-06-01) abstract; claims; figure paragraph [0028] - paragraph [0035] -----	1-6
A	DE 101 49 344 A1 (KIEKERT AG [DE]) 10 April 2003 (2003-04-10) abstract; claims; figure -----	1
A	DE 103 01 146 A1 (BOSCH GMBH ROBERT [DE]) 22 July 2004 (2004-07-22) abstract; figure 1 paragraph [0012] - paragraph [0018] -----	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2012/069520

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 102010006149 A1	04-08-2011	CN 102448748 A	09-05-2012
		DE 102010006149 A1	04-08-2011
		US 2012282913 A1	08-11-2012
		WO 2011091776 A1	04-08-2011
US 2006255911 A1	16-11-2006	JP 4389838 B2	24-12-2009
		JP 2006316455 A	24-11-2006
		US 2006255911 A1	16-11-2006
DE 10334625 A1	03-03-2005	DE 10334625 A1	03-03-2005
		FR 2858347 A1	04-02-2005
		US 2005024181 A1	03-02-2005
DE 102004052904 A1	01-06-2006	NONE	
DE 10149344 A1	10-04-2003	NONE	
DE 10301146 A1	22-07-2004	CN 1692378 A	02-11-2005
		DE 10301146 A1	22-07-2004
		EP 1595231 A1	16-11-2005
		KR 20050092411 A	21-09-2005
		US 2006255909 A1	16-11-2006
		WO 2004068419 A1	12-08-2004