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

(11) EP 3 825 205 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
26.05.2021 Bulletin 2021/21

(51) Int Cl.:
B61L 15/00 *(2006.01)* ***B61L 23/34*** *(2006.01)*

(21) Application number: **20208472.9**

(22) Date of filing: **18.11.2020**

(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
KH MA MD TN

(30) Priority: **20.11.2019 IN 201941047414**

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

(72) Inventor: **GANESAN, Muniandi**
626001 VIRUDHUNAGAR, Tamilnadu (IN)

(74) Representative: **Lavoix**
2, place d'Estienne d'Orves
75441 Paris Cedex 09 (FR)

(54) RAILWAY VEHICLE, DISTRIBUTED CONTROL SYSTEM, AND METHOD FOR MANAGING OPERATIONS OF RAILWAY VEHICLES IN A RAILWAY NETWORK

(57) A railway vehicle (100) suitable to operate in a railway network (150), characterized in that it comprises at least one on-board control system (200) configured:
- to exchange one or more first messages with at least one off-board control system (250) of the railway network using a first communication path (10) having a first communication range; and
- to exchange one or more second messages with at least another railway vehicle (101) operating in the same railway network and/or with another unit of the railway vehicle (100) using a second communication path (20) having a second communication range shorter than said first communication range; and
- to exchange one or more third messages with the at least another railway vehicle (101) of a plurality of vehicles operating in the same railway network (150) using a third communication path (30) having a third communication range shorter than the second communication range.

The invention provides also a distributed control system comprising at least a first and a second railway vehicles (100), and a method (400) for managing operations of a plurality of railway vehicles via exchange of said first, second and third messages.

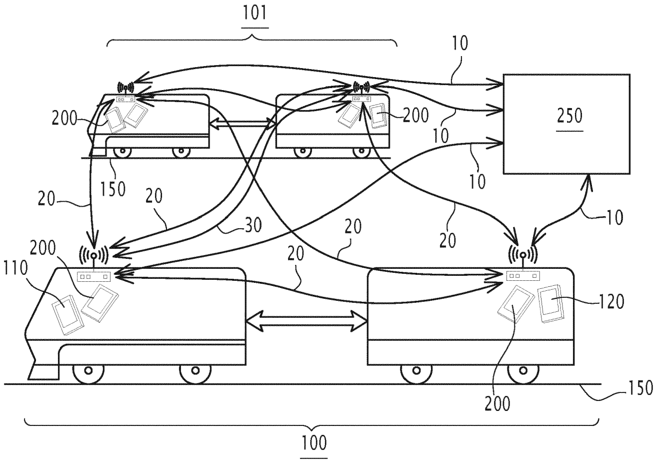

FIG.1

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The present invention relates in general to the field of traffic management in a railway network; more in particular it concerns a railway vehicle, a distributed control system and a method for managing operations of railways vehicles in a railway network, in particular as regard to prevention of collisions and possibility of virtual coupling between vehicles.

[0002] As known, railways networks are very complex systems formed by many components and devices which must be properly coordinated, continuously monitored, and timely operated, in order to ensure the correct and efficient functioning of the traffic over the whole railway network, while satisfying the highest standards of safety for the fleet of operating vehicles, which is a very critical aspect in the railroad industry.

[0003] Nowadays, a centralized and safe movement of the "fleet of trains" is managed via a Radio Block Center ("RBC") subsystem through a proper "Movement Authority" which is in operative communication, directly or indirectly, with the various trains, and operates along the track with the help of several track side devices, such as track circuits, axle counters, interlocking subsystems, signaling devices, gate crossings, et cetera.

[0004] Although such solution allows to properly manage a fleet of trains moving in a railway network, an increasing trend in the railway field foresees the reduction of the number of track side devices, due for example to their non-negligible costs for realization, installation and maintenance.

[0005] At the same time, the concept of virtually coupled vehicles, e.g. remote trains operatively coupled and managed in a coordinated way as they formed a unique convoy, is evolving and attracting more and more interest, which concept is in principle in antithesis with safety considerations related to anti-collision between vehicles.

[0006] Clearly, for any of the above aspects related to anti-collision, to virtual coupling, or to a more general traffic management, the possibility of having a reliable, trusted, safe and timely communication with and among the various trains operating within the same railway network is of paramount importance.

[0007] The present invention is purposively aimed at providing a solution which allows to integrate and balance at the same time the contrasting goals of realizing anti-collision and virtual coupling of railway vehicles, while managing traffic in a railway network, according to a reliable, safe and trusted communication scheme.

[0008] In particular, such aimed is achieved by a railway vehicle suitable to operate in a railway network, characterized in that it comprises at least one on-board control system configured:

- to exchange one or more first messages with at least one off-board control system of the railway network using a first communication path having a first communication range; and
- to exchange one or more second messages with at least another railway vehicle of a plurality of vehicles operating in the same railway network and/or with another unit of the railway vehicle using a second communication path having a second communication range shorter than said first communication range; and
- to exchange one or more third messages with at least another railway vehicle of a plurality of vehicles operating in the same railway network using a third communication path having a third communication range shorter than said second communication range.

[0009] The above mentioned aim is also achieved by a distributed control system for managing a fleet of railway vehicles operating in a railway network, characterized in that it comprises:

- at least a first railway vehicle and a second railway vehicle as above indicated, and in particular ad described and especially according to any of the relevant appended claims 1 to 8;
- at least one off-board control system in operative communication with said first railway vehicle and said second railway vehicle at least via the respective first communication path.

[0010] Further, the present invention provides also a method for managing operations of a plurality of railway vehicles operating in a railway network, characterized in that it comprises, in whichever suitable order, at least the following steps:

- exchanging, between a control system installed on-board of a first railway vehicle of said plurality of railway vehicles and at least one off-board control system of the railway network, one or more first messages using a first communication path having a first communication range;
- exchanging, between said first railway vehicle and at least another railway vehicle of the plurality of vehicles and/or another unit of the first railway vehicle, one or more second messages using a second communication path having a second communication range shorter than said first communication range;
- exchanging, between said first railway vehicle and at least another railway vehicle of a plurality of vehicles operating in the same railway network, one or more third messages using a third communication path having a third communication range shorter than said second communication range.

[0011] Further characteristics and advantages will become apparent from the description of some preferred but not exclusive exemplary embodiments of a railway vehicle, a distributed control system and a method according to the invention, illustrated only by way of non-limitative examples with the accompanying drawings, wherein:

Figure 1 is a block diagram schematically illustrating two railway vehicles in communication with each other and with an off-board control center, according to the invention;
Figure 2 is a block diagram schematically illustrating an exemplary distributed control system according to the invention;
Figure 3 is a flow chart schematically representing a method for managing operations of railway vehicles operating in a railway network, according to the present invention.

[0012] It should be noted that in order to clearly and concisely describe the present disclosure, the drawings may not necessarily be to scale and certain features of the disclosure may be shown in somewhat schematic form.

[0013] Further, when the term "adapted" or "arranged" or "configured" or "shaped", is used herein while referring to any component as a whole, or to any part of a component, or to a combination of components, it has to be understood that it means and encompasses correspondingly either the structure, and/or configuration and/or form and/or positioning.

[0014] In particular, for electronic and/or software means, each of the above listed terms means and encompasses electronic circuits or parts thereof, as well as stored, embedded or running software codes and/or routines, algorithms, or complete programs, suitably designed for achieving the technical result and/or the functional performances for which such means are devised.

[0015] A railway vehicle, a distributed control system and a method for managing operations of railway vehicles in a railway network, according to the present invention, are schematically illustrated in figures 1, 2 and 3, therein indicated by the corresponding overall reference numbers 100, 300 and 400 respectively.

[0016] As illustrated in figure 1, the railway vehicle 100 according to the present invention comprises at least one on-board control system, indicated by the overall reference number 200, which is configured to exchange one or more first messages with at least one off-board control system 250, using a dedicated first communication path, schematically indicated in figures 1 and 2 by the reference number 10, having a first communication range.

[0017] In figure 1, the at least one off-board control system 250, associated to the railway network 150 inside which the vehicle 100 is operating, is illustrated as a remote central control center 151 supervising the entire railway network 105 or a portion thereof.

[0018] As those skilled in the art may easily appreciate, the at least one off-board control system 250 may include, in addition or in alternative to the control center 151, one or more trackside control systems, for example associated each to supervise a section of the railway network 105, and for instance placed at corresponding stations.

[0019] In the exemplary embodiment illustrated in figure 2, the at least one off-board control system is depicted as comprising for example the centralized control center 151 and a trackside control system 160, and both comprises for example a respective database 161; a control and processing unit 162, a communication interface module 163, and a Human Machine Interface 165.

[0020] Conveniently, in the railway vehicle 100 according to the present invention, the on-board control system 200 is further configured:

- to exchange one or more second messages with at least another railway vehicle 101 of a plurality of vehicles operating in the same railway network 150, and/or with another unit of the own railway vehicle 100, using a dedicated second communication path, indicated in figures 1 and 2 by the reference number 20, having a second communication range shorter than the first communication range; and further
- to exchange one or more third messages with at least another railway vehicle 101 of a plurality of vehicles operating in the same railway network 150, preferably exclusively with said at least another railway vehicle 101 of the plurality of vehicles operating in the railway network 150, using a dedicated third communication path, indicated in figures 1 and 2 by the reference number 30; the third communication path has a third communication range shorter than said second communication range.

[0021] In figure 1, the first vehicle 100 and the another vehicle 101 are shown, for ease of illustration, as comprising each only two units, e.g. a head unit 110 and a tail unit 120; as those skilled in the art would easily appreciated, the term railway vehicle herein used encompasses any suitable type of railway vehicle, such as passengers or freight trains, which can be composed by any number of locomotives or equivalent traction units, and associated one or more carriages, railcars, vehicles, or the like.

[0022] Further, within the frame of the present invention, the at least another vehicle has to be substantially equivalent to the reference or own vehicle 100, and it has been indicated by the reference number 101 only for the sake of a clearer description.

[0023] According to an exemplary embodiment, schematically illustrated in figure 2, the on-board control system 200 includes, for instance, at least a control and processing unit 1, an associated communication interface or module 2, a localizing system 3 for localizing the actual position of the own railway vehicle 100 in the railway network 150, a further computerized unit, for instance a European Vital Computer (EVC) 4 which provides to the unit 1 movement authority information for the own vehicle 100 which is received for instance from the centralized control center 151, a database 5, and a Human Machine Interface 6 used for monitoring the operations linked with the railway vehicle 100.

[0024] According to a possible embodiment, the database 5, or block database, contains data related to the railway network, and in particular, for instance, zone numbers, unique block identification number(s), absolute location kilometric point (s), list of blocks in both directions of the tracks, list of blocks (incremental distance, angle) in both directions.

[0025] For example, data stored can be in the following form: Zone number, block identifier or ID, location kilometric point, list of block identifiers of IDs in up direction, list of blocks (distance, angle) in up direction, list of block identifiers or IDs in down direction, list of blocks (distance, angle) in down direction.

[0026] The following is a numerical example of the above form: Zone1, 8, 1550, 9|10|11, (50,0)|(20,+20)|(30,+20), 7,(30,0)

[0027] This database 5 can be constructed/updated using the inputs from the localizing system 3, which provides to the unit 1 data suitable for localizing the vehicle 100 within the physical or virtual block(s) of the railway network 105. In particular, the localizing system 3, via one or more of its sensors, such as odometers/accelerometers, provides data about the actual speed, acceleration et cetera, which are required to precisely calculate the movement of a vehicle within 100 the railway network 105.

[0028] With the data received from the localizing system 3 and those available from the database 5, the control and processing unit 1 is able to locate the actual position of the own vehicle 100 and to predict its movement path quite accurately based on the braking distance along with the route assigned to vehicle itself.

[0029] The control and processing unit 1 of the own vehicle 100 sends/receives the telemetry of each relevant block ID and the incremental distance from it, to/from nearby vehicles within the short-range communication distance of the path 20. The telemetry includes, for instance, the speed/acceleration, the movement path in terms of the list of blocks within the braking distance along with the assigned route to the nearby vehicles.

[0030] Further, the control and processing unit 1 of the own vehicle 100 sends/receives the telemetry of each relevant block ID and the incremental distance from the block, to/from nearby vehicles within the "very short-range communication distance of the path 30. This telemetry includes for instance the speed/acceleration, the movement paths of relevant vehicles.

[0031] The control and processing unit 1 can be of concentrated or distributed type, and it can be constituted by, or comprise, any suitable processor-based device, e.g. a processor of a type commercially available, suitably programmed and provided to the extent necessary with circuitry, in order to perform the innovative functionalities devised for the railway vehicle 100 according to the present invention.

[0032] According to the invention, the first communication path 10, which covers the distance range of an entire railway network zone, for example, 500 km, is used in particular for exchanging messages related to the management of identifying keys/IDs for uniquely identifying each vehicle 100, 101 of the plurality of vehicles operating in the railway network, between the on-board control system 200 and in particular the processing unit 1 and one or more off-board control systems, such as the trackside control system 160 represented in figure 2.

[0033] In particular, the control and processing unit 1, is configured for generating a first identifier or key SK suitable to be stored and kept secret in the own vehicle 100, e.g. in a memory of the unit 1 or in the database 5, and a second public identifier or key PK associated with the first secret identifier or key SK. The second identifier key PK is transmitted, via the interface communication module 2, to at least one off-board control system, e.g. the centralized control center 151 and /or the trackside control system 160, via the first communication path 10, where it is publicly accessible by the other railway vehicle(s) 101 operating in the railway network 150, for uniquely identifying the own vehicle 100.

[0034] For instance, each public identifier or key PK sent by a railway vehicle 100 can be stored in an off-board database 161 installed at the remote control center 151, and/or in any off-board database 161 located in the trackside control system 160 installed along the railway network 150.

[0035] When each railway vehicle sends its public key PK to the off-board control system 160 (or to the control center 151), it can receive back the corresponding public identifier or key PK of the control system 160 itself (or of the control center 151) so as to establish dedicated communication sessions with it; further, via the same off-board control system, each vehicle can receive the public identifier of keys PKs of other vehicles.

[0036] According to an embodiment of the railway vehicle 100, the control and processing unit 1 is adapted to encrypt at least one, preferably all, the one or more second and third messages.

[0037] The on-board control system 200, and in particular for example the control and processing unit 1, is adapted to generate second messages, preferably encrypted, which include information related to and suitable for managing and executing a collision prevention intervention between the own railway vehicle 100 and one or more other vehicles, such as the vehicle 101 illustrated in figure 1, operating in the same railway network 150.

[0038] In particular, the second messages are suitable to be exchanged with the at least another vehicle 101, and/or with the another unit of the own railway vehicle 100, using the second communication path 20, for instance via the interface communication module 2.

[0039] Typically, the second communication path 20 covers the distance range of more than the braking distance at maximum speed of a vehicle plus the length of both vehicles, and is for example in the order of 10 km.

[0040] In practice, the second or short range communication path 20 is in particular dedicated for exchanging messages in the context of collision avoidance. As nearby vehicles 101 are not known in advance, the relevant second messages are signed as generic messages using the security key SK of a sending vehicle 100 and incorporate the identity (ID) of the sending vehicle 100 itself. These messages can be verified using the related public key PK of the sending vehicle 100 by the on-board control system 200 of the receiving vehicle 101.

[0041] According to an embodiment of the railway vehicle 100, the on-board control system 200, and in particular its control and processing unit 1, is configured to disable the third communication path 30 when a collision prevention intervention between the own railway vehicle 100 and the least another railway vehicle 101 of the plurality of vehicles operating in the railway network 150 is under execution.

[0042] According to a possible embodiment of the railway vehicle 100, the on-board control system 200, and in particular for instance its control and processing unit 1, is adapted to generate third messages, preferably encrypted which include information for virtual coupling of the own railway vehicle 100 with at least another railway vehicle 101 of the plurality of vehicles 100 operating in the same railway network 150, in the vicinity of the own vehicle 100.

[0043] In particular, the preferably encrypted third messages are suitable to be exchanged with the at least another vehicle 101 operating in the vicinity of the own vehicle 100, using the third communication path 30, for instance via the interface communication module 2.

[0044] In particular, the third or very short-range communication path 30, which covers for example a distance up to 1 km, is preferably exclusively dedicated for exchanging messages in the context of virtual coupling between a leading vehicle 100 and a trailing one out of a plurality of vehicles operating in the railway network 105. To this end, each third message sent by a vehicle 100 is signed using the public key "PK" of the other vehicle 101 under mutual virtual coupling. The third message can be verified by using the security key SK of the receiving vehicle 101 under mutual virtual coupling.

[0045] According to an embodiment of the railway vehicle 100, when the own railway vehicle 100 engages in virtual coupling with at least another and nearby vehicle 101 using the third communication path 30, the on-board control system 200, and in particular its control and processing unit 1, is configured to overrule any on-going collision prevention intervention with such another vehicle, while keeping the second communication path 20 active, together with the first communication path 10 as well, in order to promptly face any issue arising from the on-going virtual coupling or with any other railway vehicle.

[0046] According to an embodiment, the above mentioned another part of the own railway vehicle 100 comprises a second on-board control system 200, wherein the first on-board control system is positioned at a front part of the own railway vehicle 100, e.g. the head unit 110, which can be a locomotive, and the second on-board control system 200 is positioned at a rear part for the own vehicle 200, e.g. the tail vehicle 120 thereof, which can be for example a second locomotive or any suitable car.

[0047] The second on-board control system is substantially identical to the first on-board control system 200, and therefore the description related to the first on-board control system 200 applies likewise to the second control system 200. In particular, the first and second on-board control systems 200 are in operative communication with each other via the second communication path 20, using for instance the respective communication interface module 2.

[0048] Further, likewise the first on-board control system 200, the second on-board control system 200 links in operative communications and exchanges, for instance via its communication interface 2: corresponding first messages with at least one off-board control system, such as the control center 151 and/or any trackside control system 160, using the first communication path 10; corresponding second and third messages with and any further railway vehicle 101, using the second communication path 20 and the third communication path 30, respectively.

[0049] In this way each railway vehicle 100 according to the present invention, is able to communicate with various off-board control systems, and with other railway vehicles 101 preceding and trailing the own vehicle 100 along a route of the railway network 150.

[0050] In practice, according to the present invention, a distributed control system 300 for managing operations of railway vehicles operating in a railway network 150, is realized and comprises at least: a first railway vehicle 100 and a second railway vehicle 100 equipped each with the at least one, preferably two, on board control system(s) 200, previously described, and which are linked in mutual communication using the second communication path 20; and at least one off-board control system, such as the control center 151 and/or any trackside control system 160, in operative communication with the first railway vehicle 100 and the second railway vehicle 100 at least via the respective first communication path 10.

[0051] The third communication path 30 is used for inter-train communication between the railway vehicle 100 and the other railway vehicle 101.

[0052] Figure 3 illustrates a method 400 for managing operation of a plurality of railway vehicles 100, of the type previously described, operating in the railway network 150, the method 400 being characterized in that it comprises, in whichever suitable order, at least the following steps:

- 405: exchanging, between a control system 200 installed on board of a first railway vehicle 100 and at least an off-board control system of the railway network 150, e.g. the control center 151 and/or any trackside control system 160, one or more first messages using a first communication path 10 having a first communication range;
- 410: exchanging, between said first railway vehicle 100 and at least another railway vehicle 101 of the plurality of vehicles operating in the same railway network 150 and/or another unit of the first railway vehicle 100, one or more second messages using a second communication path 20 having a second communication range shorter than said first communication range;
- 415: exchanging, between said first railway vehicle 100 and at least another railway vehicle 101 of the plurality of vehicles operating in the same railway network 150, one or more third messages using a third communication path 30 having a third communication range shorter than said second communication range.

[0053] In particular, the step 405 of exchanging first messages comprises generating a first secret identifier or key SK suitable to be kept stored at the first vehicle 100, and a second public identifier or key PK uniquely associated with the first secret identifier SK; the second identifier or key PK is suitable to be transmitted to and stored in said at least one off-board control system, using the first communication path 10 and being publicly accessible for uniquely identifying the first railway vehicle 100, by other vehicles, and/or off-board control systems.

[0054] In practice, according to the invention, public (PK) and private (SK) keys are generated by individual vehicles 100, for example based on blockchain technology. The private key (SK) is kept by each individual vehicle 100, while the public key is sent to for being shared, in one or more off-board control systems, such as the depicted control system 160, within the long communication range of the path 10, and/or to the centralized control center 151. Hence, the relevant trackside control system 160 acts as a public key management node, has the information about all public keys, and it can confirm the uniqueness of each key-vehicle 100.

[0055] According to an embodiment, the step 410 of exchanging one or more second messages and/or the step 415 of exchanging one or more third messages comprises preferably encrypting at least one of said one or more second and/or third messages.

[0056] In particular, the step 410 of exchanging one or more second messages comprises generating and preferably encrypting second messages which include information related to and suitable for managing a collision prevention intervention between the first railway vehicle 100 and the at least another vehicle 101; to this end, the encrypted second messages are suitable to be exchanged with the at least another vehicles 101 and/or with the another unit of the first railway vehicle 100, namely a second on-board control system 200 thereof, using the second communication path 20.

[0057] In particular, concerning the avoidance of collision between nearby vehicles, the on board control system 200 of a railway vehicle 100, located at the head and/or tail thereof, receives via the short-range communication path 20, the localization reports from all the nearby vehicles 101, which reports include for example the braking distance of a relevant vehicle at maximum speed. In case, both nearest vehicles generate the consensus for entering into a collision prevention mode, and execute required operations, for example they both apply the brakes to avoid the collision and perform an incident reporting. In this interval, the very short-range communication path 30 will be inactive during "vehicles collision avoidance", and only the short and long-range communication paths 20, 10 are used.

[0058] According to an embodiment, the method 400 comprises a step 420 of disabling the third communication path 30 when a collision prevention intervention between the first railway vehicle 100 and the at least another railway vehicle 101 is under execution.

[0059] Likewise, the step 415 of exchanging one or more third messages comprises generating and preferably encrypting third messages which include information for virtual coupling of the first railway vehicle 100 with said at least another nearby railway vehicle 101 of the plurality of vehicles operating in the same railway network 150, the encrypted third messages being suitable to be exchanged with the at least one nearby vehicle 101 using the third communication path 30.

[0060] In particular, if two vehicles are engaging in virtual coupling, collision avoidance is overruled by the virtual coupling operation. In this case, for instance, the trailing vehicle 101 tracks the leading train using very short-range communication path 30, and all the three-communication paths (long 10, short 20, and very-short 30) are active to ensure a smooth transition to a collision avoidance procedure in case of issues while executing the ongoing virtual coupling.

[0061] In particular, virtual coupling is preferably enabled only when two vehicles 100 are moving in the same direction and the same blocks of railway network 150 for a reasonable distance/time, for example 20 kms/10 minutes.

[0062] Concerning encryption, for instance for messages exchanged via the very short-range communication paths or links 30, the corresponding separate public and private keys are generated and the public keys are exchanged between two vehicles 100 via the dedicated short-range communication path or link 30 as previously indicated.

[0063] For example, a security key (SK) with the size of 32 bytes or 256 bits can be generated using any random number generator comprised in or associated with the own control and processing unit 1 and is kept secret. In practice, each vehicle 100 contains its own key management node which manages its private and secret keys used for communicating messages among the vehicles 100. Then, a related public key PK, for example having the size of 64 bytes or 512 bits is generated from the previously generated security key (SK) using Ecliptic Curve Digital Signature Algorithm (ECDSA) by the relevant on-board control system 200, namely *PK = ECDSA(SK).*

[0064] The public keys from various vehicles 200 are managed at the key management master node of the trackside control system, such as the system 160, by pairing the vehicle ID with its related public key PK).

[0065] Then, a secured message is created by calculating for example the SHA-256 (Secure Hash Algorithm-256) of a message at first, and then generating 160-bit hash using RIPEMD-160 (RACE Integrity Primitives Evaluation Message Digest). The SHA-256 generates an almost-unique 256-bit (32-byte) signature for a message which is required for the security of the message. RIPEMD-160 is a 160-bit cryptographic hash function which is required for maintaining uniformity. Finally, signature is a 160-bit hash value of a 256-bit hash of message, namely Hash of message = RIPEMD-160(SHA-256(message)).

[0066] Accordingly, any length of message is converted into uniform 160 bits. Then, the hash of the message is encrypted using the relationship SK/PK. This encrypted hash is the signature of the message, namely Signature = Encryption (Hash of message, SK/PK).

[0067] This "signature" is sent along with "message" by each on-board control system 200 to other on-board control systems 200 or to off-board control system located at the control center 151 or else.

[0068] For verifying a message, at first step the Hash of the message is recreated and then the signature is decrypted decrypt the using relevant public key (PK) (for encryption with SK)/SK (for encryption with PK) to create decrypted hash, namely Hash of message = RIPEMD-160(SHA-256(message)), Decrypted Hash of message = Decryption (Signature, PK/SK). If hash of message and decrypted hash of message are same, the message is verified as the correct one and can be used.

[0069] The message, as for example represented in the below table, exchanged between the on-board control system 200 and an off-board trackside control system 160, is also used to change the key. It is to be noted that the public key of the receiver is used for message encryption such that only the respective receiver can decrypt the public key (PK) of sender using its secret key (SK). The receiver ID is filled with zeros when there are anonymous receivers, i.e. a message broadcasted, to all the nearby vehicles. Any on-board control system 200 can decrypt the message using sender's public key (PK), which can be collected from an off-board trackside control system 160.

Hash code of Message (128 bits)	Time Stamp (Sec) (32 bits)	*Receiver Identification Hash Code (32 bits)*	*Sender Identification Hash Code (32 bits)*	Encryption with (PK) of Receiver / (SK) of Sender			Hash code of Next Message (128 bits)
				Message Type (4 bits)	Data Size (32 bits)	Scrambled Data with clues (Variable size)	
MD5 checksum of message	Time	Zeros (or) Receiver ID	Sender ID	1- Change Key	512 or Message size	New PK from Sender - 512 bits or Message	Zeros (or) MD5 checksum of next message

[0070] According to an embodiment, the method 400 comprises the steps of:

- 425: engaging virtual coupling between the first railway vehicle 100 and the at least another nearby vehicle 101 of the plurality of vehicles operating in the railway network, using the third communication path 30: and

- 430: overruling any collision prevention intervention between the first railway vehicle 100 and the at least another nearby vehicle 101 under virtual coupling, while keeping the second communication path 20, as well as the first communication path 10, active.

[0071] In practice, when a railway vehicle 100 starts its operations in a day, it is assigned with a unique ID and initial zone number from the control center 151, which ID is sent to the computerized unit 4 of the on board control system 100, e.g. the one at the head of the vehicle 100. The onboard control system 200 generates an initial pair of associated security and public keys (SK, PK), and the public key is sent to the control center 151. At the same time, the off-board trackside control system 160 also generates its pair of security and public keys (SK, PK) and sends its public PK to the control enter 151 during the initialization for the day. Finally, the control center 151 shares the public PKs from the on-board control system 100 and the off-board trackside control system 160 with each other during the initialization. Accordingly, a "permissioned" network is created between the on-board control system 100 and the off-board trackside control system 160. In order to avoid the unauthorized usage of PK, PK is sent as scrambled data with the attached clues for descrambling, such as for instance, swapping of every multiple of 4th bit and the prior bit, or similar.

[0072] Since the public keys need to be known substantially at control system level, one of each of the on-board control system(s) 200 of the vehicle 100 generates a new key pair and communicates with the off-board trackside control system 160 to change its current key, e.g. at each relevant station. At the same time, the off-board trackside control system 160 also creates a new key pair for each vehicle 100, i.e. the transaction between an on-board control system 100 and the off-board trackside control system 160 will be maintained as unique key pairs, even though only one off-board trackside control system 160 is present in the respective zone of the railway network 150.

[0073] In this way, the associated new keys of the on-board control systems 200 and of the trackside control system 160 are not known to the centralized control center 151 immediately.

[0074] The same process is repeated for each new vehicle 100 which is initialized via the centralized control center 151, or at each station.

[0075] An important aspect is that public key PK of the receiver is used for message encryption such that only the respective receiver can decrypt the PK of sender using its security key SK.

[0076] In case of possible collision, the on-board control system 100, for example at the head of the vehicle 100, transmits the *unique ID* and initial *zone number* to the on-board control system 100 at the tail of the vehicle using the public key (PK) of the tail vehicle (or vice versa). This information is required to communicate with the off-board trackside control system 160. The own localizing system 3 provides to the control and processing unit 1 the block identifier or ID for the forthcoming block of the railway network 105 along with the incremental distance from it, as well as data related to the actual speed/acceleration of the vehicle 100. Further, the control and processing unit 1 receives the Movement Authority information form the associated computerized unit 4 (EVC) which contains the route information. The same information about Movement Authority is transmitted to the other control system 200 at the tail (or viceversa) of the same vehicle 100. Based on the current location and Movement Authority, the on-board control system 100, and in particular its control and processing unit 1, calculates the list of blocks within the braking distance plus a safety margin distance, which is configurable, along with the time in the assigned route. This information is telemetered using the short range communication path 20, thus such message can be captured only by nearby vehicles 101 operating within the short range distance. Likewise, the on-board control system 200 of the own vehicle 100 also receives the telemetry of the block ID and incremental distance from the block, from nearby vehicles operating within the short-range communication distance, along with information about their speed/acceleration, movement path in terms of the list of blocks within the braking distance along the assigned route.

[0077] Based on the block ID and incremental distance from other vehicles, the distance between the head of a first vehicle 100 and the tail of a preceding second vehicle 100 is calculated using for example the block database 5 and the respective route information. If the calculated distance exceeds the combined braking distances, it will be treated as a possible collision scenario. Furthermore, the overlapping point between the two vehicles the distance of collision, time of the collision, collision type (head/tail/side), are calculated. It is possible to have a collision, if one of the vehicles is approaching another one. If both vehicles are leaving in opposite direction, then, the movements are declared as collision-free. Once the possible collision scenario is confirmed, then the appropriate actions are triggered as for example described in the following table, for two trains:

One train	Another train	Action for One train in case of possible collision	Action for Another train in case of possible collision
Approaching	Approaching	- Reduce the speed - Apply Emergency Brake (EB)/ Service Brake (SB) through EVC Alert CCC, EVC Get updated Movement Authority from EVC or train suggests the alternate path based on block database for safe stopping.	- Reduce the speed, - Apply EB/SB through EVC - Alert CCC, EVC - Get updated Movement Authority from EVC or train suggests the alternate path based on block database for safe stopping.
Approaching	Leaving	Reduce the speed of the following train, Apply SB	Increase the speed of the lead train Apply SB
Leaving	Approaching	Reduce the speed of the following train, Apply SB	- Increase the speed of the lead train Apply SB

(continued)

One train	Another train	Action for One train in case of possible collision	Action for Another train in case of possible collision
Leaving	Leaving	No Action is required	No Action is required

[0078] Concerning virtual coupling between railway vehicles, it is possible to establish "Virtual Coupling" between two static/running vehicles, or between a running leading vehicle and a static following vehicle. It is also possible to establish virtual coupling only to stop a running following vehicle closer to a static leading vehicle, i.e. the targeted speed of the following vehicle is zero and the stopping distance is less than 1 km in the same track. As collision avoidance and virtual coupling are basically in contrast to each other, virtual coupling can be activated only when the direction of travel is same for both running vehicles.

[0079] In particular, the possible pair of trains are identified for virtual coupling during the route generation by the centralized control enter 151. During the running, if the lead vehicle identifies the following vehicle, or vice versa, through the short range communication 20, they can exchange the messages related to authentication of virtual coupling by sharing the route information. Hence, both trains compare the assigned route which is received using the short range communication 20. Consensus for virtual coupling has to be expressed mutually by both vehicles.

[0080] Based on the consensus, both trains generate the dedicated PK, SK pair of keys so as to communicate the message(s) using the very short-range communication path or link 30. This pair of keys is not shared with any trackside control system. These keys are sent by a vehicle as a message signed with the public key PK of the other vehicle. Once such keys are available at both trains, the virtual coupling link is established and both vehicles will start the exchange of high-speed telemetry data using the third communication path 30. The information about ongoing virtual coupling is also media available at the computerized unit(s) 4 and the centralized control center 151. At the same time, as previously indicated, the collision Avoidance functionality is disabled between the two vehicles under virtual coupling. However, the collision monitoring will run in the background using the short range communication data as a fallback option in case of issues.

[0081] The "trailing vehicle 101" gets the dynamic movement authority based on its speed as the objective to follow so as to maintain a constant distance, for instance up to maximum 1km, from the preceding vehicle. If one of the two vehicles virtually coupled is out of the range of the third communication path 30, signals are lost and the established virtual coupling link will be disabled. This will lead the on-board control system 200 to enter into a "Collision Avoidance" mode and to execute for example the actions indicated in the above table.

[0082] Hence, it is evident from the foregoing description and appended claims that the railway vehicle 100, control system 300, and method 400 according to the present invention, achieve the intended aim and objects, since they allow to properly manage operations of railways vehicles in a railway network, and in particular to properly coordinate at the same type operations for avoiding collision and virtual coupling between vehicles. To this end, communication among the various parts, is executed using dedicated channels and according to a secured and trustable way.

[0083] The railway vehicle 100, distributed control system 300, and method 400 thus conceived are susceptible of modifications and variations, all of which are within the scope of the inventive concept as defined in particular by the appended claims.

[0084] All the details may furthermore be replaced with technically equivalent elements.

Claims

1. A railway vehicle (100) suitable to operate in a railway network (150), **characterized in that** it comprises at least one on-board control system (200) configured:

- to exchange one or more first messages with at least one off-board control system (250) of the railway network (150) using a first communication path (10) having a first communication range; and
- to exchange one or more second messages with at least another railway vehicle (101) of a plurality of vehicles operating in the same railway network (150) and/or with another unit of the railway vehicle (100) using a second communication path (20) having a second communication range shorter than said first communication range; and
- to exchange one or more third messages with at least another railway vehicle (101) of a plurality of vehicles operating in the same railway network (150) using a third communication path (30) having a third communication range shorter than said second communication range.

2. A railway vehicle (100) according to claim 1, wherein said at least one on-board control system (200) includes a control and processing unit (1) arranged to encrypt at least one of said one or more second and third messages.

3. A railway vehicle (100) according to claim 2, wherein said control and processing unit (1) is configured for generating a first identifier (SK) suitable to be kept stored secretly at the railway vehicle (100), and a second public identifier (PK), associated with the first secret identifier (SK), the second identifier (PK) being suitable to be transmitted to and stored in said at least one off-board control system (250) via said first communication path (10) and being publicly accessible for uniquely identifying the railway vehicle (100).

4. A railway vehicle (100) according to any of the preceding claims, wherein the on-board control system is configured to generate second messages which include information related to and suitable for executing a collision prevention intervention between the railway vehicle (100) and the at least another railway vehicle (101) operating in the same railway network (150), said second messages being suitable to be exchanged with the at least another railway vehicle (101) and/or with the another unit of the railway vehicle (100) via the second communication path (20).

5. A railway vehicle (100) according to claim 4, wherein the on-board control system is configured to disable said third communication path (30) when a collision prevention intervention between the railway vehicle (100) and at least another railway vehicle is under execution.

6. A railway vehicle (100) according to any of the preceding claims,, wherein the on-board control system is adapted to generate third messages which are encrypted and include information for virtual coupling of the railway vehicle (100) with at least one nearby vehicle (101) operating in the same railway network (150), said encrypted third messages being suitable to be exchanged with the at least one nearby vehicle via the third communication path (30).

7. A railway vehicle (100) according to claim 6, wherein, when the railway vehicle (100) engages in virtual coupling with at least one nearby vehicle via said third communication path (30), the on-board control system is configured to overrule any collision prevention intervention while keeping the second communication path (20) active.

8. A railway vehicle (100) according to any of claims 1 to 7, wherein the at least one on-board control system (200) comprises a first on-board control system (200) positioned at a front part of the railway vehicle (100) and a second on-board control system (200), substantially identical to said first on-board control system (200), which is positioned at a rear part for the railway vehicle , said first and second on-board control systems (200) being in operative communication with each other via the second communication path (20), the second on-board control system (200) being in operative communication with the at least one off-board control system (250) via its first communication path (10) and being in operative communication with a further railway vehicle via its second and/or third communication path (30).

9. A distributed control system (300) for managing a fleet of railway vehicles operating in a railway network (150), **characterized in that** it comprises:

- at least a first railway vehicle (100) and a second railway vehicle (100) according to any of the claims 1 to 8;
- at least one off-board control system (250) in operative communication with said first railway vehicle (100) and said second railway vehicle (100) at least via the respective first communication path (10).

10. A method (400) for managing operations of a plurality of railway vehicles operating in a railway network, **characterized in that** it comprises, in whichever suitable order, at least the following steps:

- (405): exchanging, between a control system installed on-board of a first railway vehicle (100) of said plurality of railway vehicles and at least one off-board control system (250) of the railway network (150), one or more first messages using a first communication path (10) having a first communication range;
- (410): exchanging, between said first railway vehicle (100) and at least another railway vehicle (101) of the plurality of vehicles and/or another unit of the first railway vehicle (100), one or more second messages using a second communication path (20) having a second communication range shorter than said first communication range;
- (415): exchanging, between said first railway vehicle (100) and at least another railway vehicle (101) of the plurality of vehicles operating in the same railway network, one or more third messages using a third communication path (30) having a third communication range shorter than said second communication range.

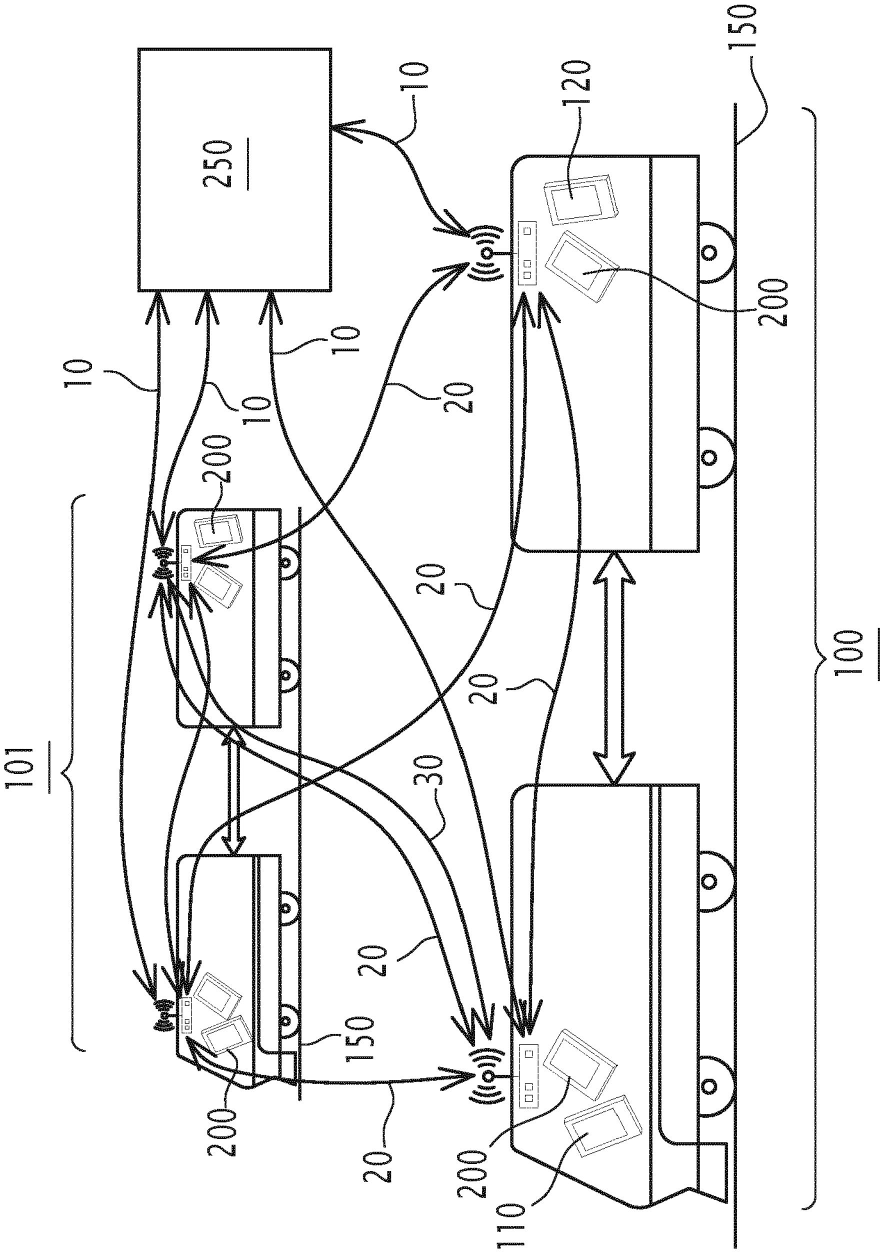
250
10
10
10
10
10
20
20
20
20
20
30
200
200
200
200
101
100
110
120
150
150

FIG.1

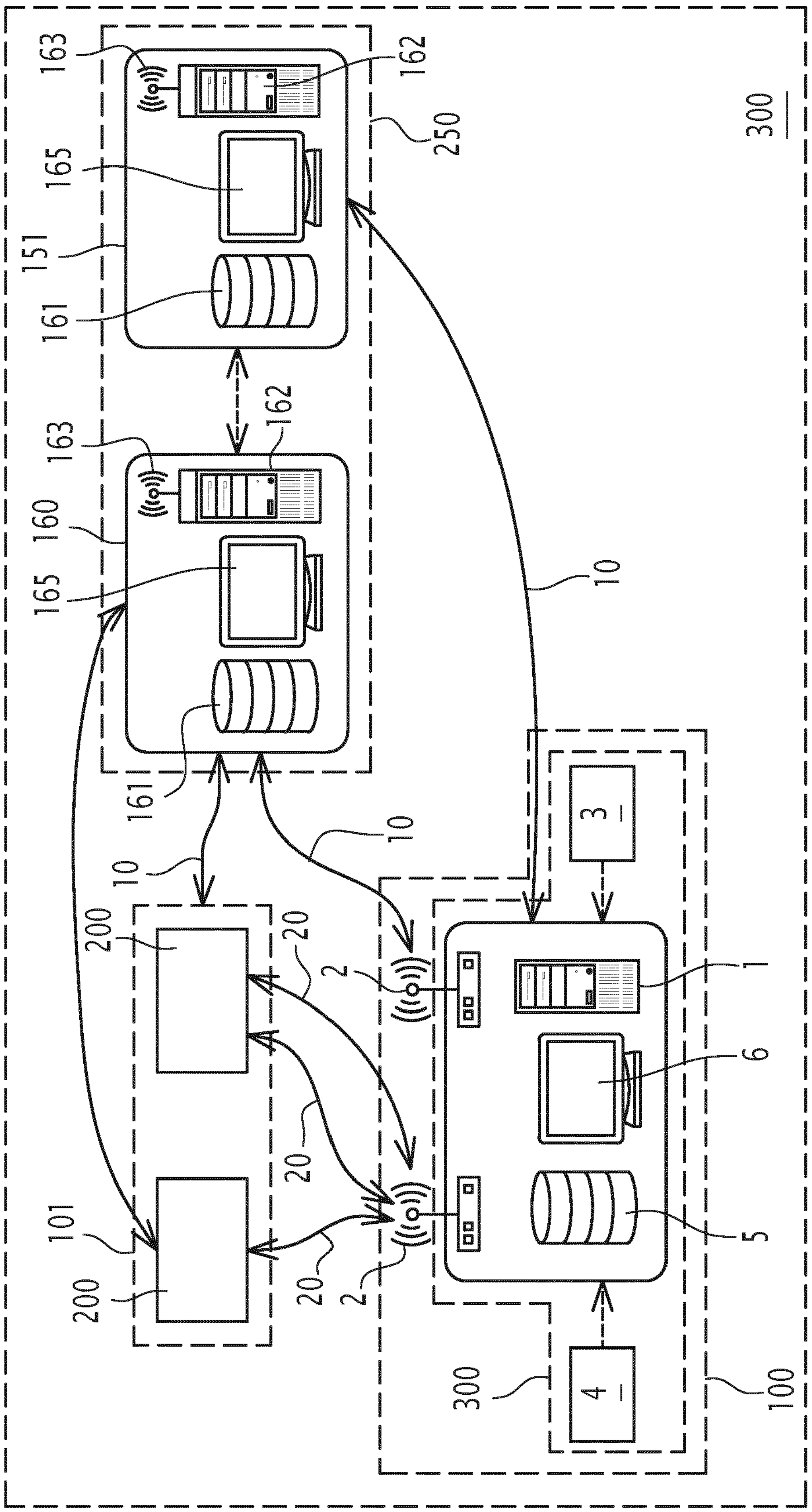
163
162
165
151
161
250
300
163
162
160
165
161
10
10
10
200
20
2
1
6
20
20
101
5
200
20
2
3
4
300
100

FIG.2

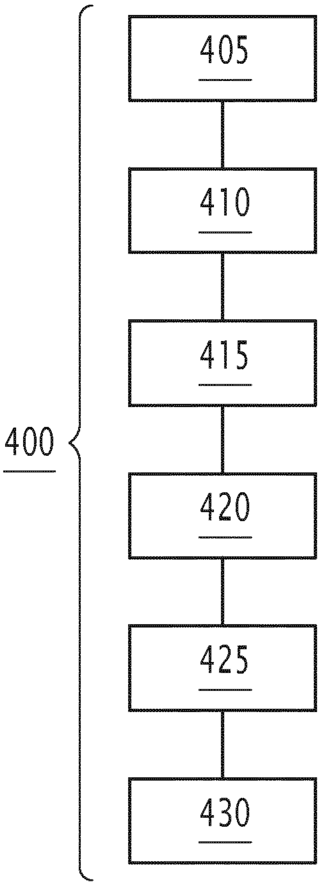

FIG.3

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 20 20 8472

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	US 2011/172856 A1 (KULL ROBERT C [US]) 14 July 2011 (2011-07-14)	1-4,6-10	INV. B61L15/00 B61L23/34
A	* paragraphs [0024] - [0026]; figure 1 * * paragraphs [0027] - [0031]; figure 2 * * paragraph [0032]; figure 3 * * paragraphs [0034], [0035] * * paragraph [0050]; figure 5 * -----	5	
X	US 2018/159936 A1 (KIRSCHNER MARK [US] ET AL) 7 June 2018 (2018-06-07)	1-3,8-10	
A	* paragraphs [0044], [0047], [0049], [0052] - [0055]; figure 1 * -----	4-7	
A	EP 3 219 575 A1 (ALSTOM TRANSP TECH [FR]) 20 September 2017 (2017-09-20) * paragraphs [0008] - [0010] * * paragraphs [0024], [0029], [0034], [0037] - [0039], [0042]; figures 1,2 * -----	1-3,8-10	

TECHNICAL FIELDS SEARCHED (IPC)

B61L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	6 April 2021	Martínez Martínez, J

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

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 20 20 8472

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.

06-04-2021

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011172856 A1	14-07-2011	AU 2010340289 A1 BR PI1010174 A2 CA 2761014 A1 US 2011172856 A1 WO 2011084251 A2	24-11-2011 29-03-2016 14-07-2011 14-07-2011 14-07-2011
US 2018159936 A1	07-06-2018	NONE	
EP 3219575 A1	20-09-2017	NONE	

EPO FORM P0459

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