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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 June 2006 (29.06.2006)

PCT

(10) International Publication Number
WO 2006/067673 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/IB2005/054208

(22) International Filing Date:
13 December 2005 (13.12.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
04106746.3 20 December 2004 (20.12.2004) EP

(71) Applicant *(for DE only)*: **PHILIPS INTELLECTUAL PROPERTY & STANDARDS GMBH** [DE/DE]; Steindamm 94, 20099 Hamburg (DE).

(71) Applicant *(for AE, AG, AL, AM, AT, AU, AZ, BA, BB, BE, BF, BG, BJ, BR, BW, BY, BZ, CA, CF, CG, CH, CI, CM, CN, CO, CR, CU, CY, CZ, DK, DM, DZ, EC, EE, EG, ES, FI, FR, GA, GB, GD, GE, GH, GM, GN, GQ, GR, GW, HR, HU, ID, IE, IL, IN, IS, IT, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MC, MD, MG, MK, ML, MN, MR, MW, MX, MZ, NA, NE, NG, NI, NL, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD only)*: **KONINKLIJKE PHILIPS ELECTRONICS N. V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

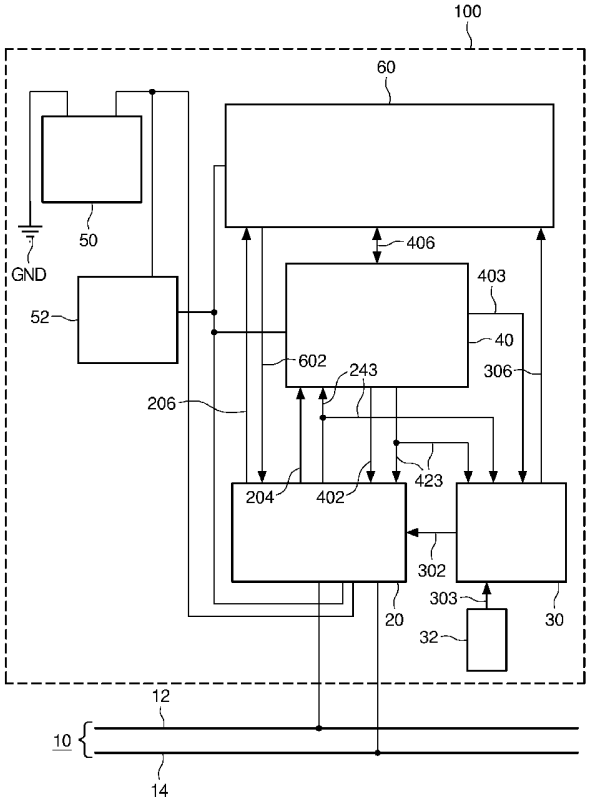
(75) Inventor/Applicant *(for US only)*: **ELEND, Bernd** [DE/DE]; c/o Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen (DE).

(74) Agent: **VOLMER, Georg**; Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen (DE).

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

[Continued on next page]

(54) Title: BUS GUARDIAN AS WELL AS METHOD FOR MONITORING COMMUNICATION BETWEEN AND AMONG A NUMBER OF NODES, NODE COMPRISING SUCH BUS GUARDIAN, AND DISTRIBUTED COMMUNICATION SYSTEM COMPRISING SUCH NODES



(57) Abstract: In order to provide a bus guardian (30) for monitoring communication between and among a number of nodes (100), in particular between and among a number of electronic control units, the bus guardian (30) being designed for monitoring at least one cyclic time-triggered communication media access schedule for transmitting messages between and among the nodes (100) across at least one communication media (10), in particular across at least one channel (12) and across at least one optional further channel (14), and being assigned to at least one communication controller (40), the communication controller (40) comprising the communication media access schedule, wherein the bus guardian (30) as well as a corresponding method require neither any a priori knowledge of the communication schedule nor any configuration parameter and monitor the communication media access schedule of the communication controller (40) even during start-up of the communication, it is proposed that that the bus guardian (30) is able to learn, in particular within the first cycle, about said communication media access schedule, and that the bus guardian (30) makes use of the learned knowledge with respect to at least one possible schedule violation (SV1, SV2, SV3), in particular with respect to at least one deviation from said communication media access schedule, for example during start-up of the communication.

WO 2006/067673 A2

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

BUS GUARDIAN AS WELL AS METHOD FOR MONITORING COMMUNICATION BETWEEN AND AMONG A NUMBER OF NODES, NODE COMPRISING SUCH BUS GUARDIAN, AND DISTRIBUTED COMMUNICATION SYSTEM COMPRISING SUCH NODES

The present invention relates in general to the architecture for communication systems, wherein for error containment in the time domain at least one bus guardian is used for each node of the communication system.

The present invention in particular relates to a bus guardian for monitoring communication between and among a number of nodes, in particular between and among a number of electronic control units, the bus guardian

- being designed for monitoring at least one cyclic time-triggered communication media access schedule for transmitting messages between and among the nodes across at least one communication media, in particular across at least one channel and across at least one optional further channel, and
- being assigned to at least one communication controller, the communication controller comprising the communication media access schedule.

The present invention further relates to a method for monitoring such communication.

In time-triggered communication systems, which for example can be used for message exchange in safety-relevant applications in vehicles, a situation in which one of the nodes due to a local malfunction temporarily or permanently impedes communication between the nodes of the communication system, is not tolerable.

In order to avoid such not tolerable situations in such time-triggered communication systems, a bus guardian as defined above in the chapter "Technical field" has been proposed; the function of such conventional bus guardian is known in the prior art for instance from communication systems for X-by wire applications, for

example from FlexRay communication systems.

In this context the bus guardian avoids that a communication controller of one of the nodes of the communication system sends data at points in time, when it is not expected to do so, thereby blocking the communication media; as a consequence of such unexpected sending and thus blocking, no other communication controller of another node would be able to transmit data (so-called "babbling idiot" failure).

To avoid such "babbling idiot" failure, the prior art provides a certain set of supervision functions, which all need to be configured. Thus, according to the prior art, a costly configuration data interface to a microcontroller, in particular to the communication controller, is necessary to adjust the parameters.

Exemplary systems matching the above description are disclosed

- in the prior art article "FlexRay International Workshop", April 16, 17, 2002, Munich, Protocol Overview by Florian Bogenberger, Dr. Bernd Müller and Thomas Führer; cf. http://www.dismi.unimo.it/Pavan/Sistemi%20Elettronici%20Industriali/protocollo_flexray.pdf),
- in prior art document EP 1 355 461 A2,
- in prior art document GB 2 386 804 A, and
- in prior art document US 2004/0081079 A1.

The prior art article "A Prototype Implementation of a TTP/C Controller" by Hermann Kopetz, René Hexel, Andreas Krüger, Dietmar Millinger, Roman Nossal, Andreas Steininger, Christopher Temple, Thomas Führer, Roman Pallierer and Markus Krug (cf. http://www.decomsys.com/publications/dm_rn_rp_prototypeimpl_ttpc_contr.pdf) discloses a prototype implementation of a T[ime]T[riggered]P[rotocol] named TTP/C. In this context, bus guardians play a key role in ensuring the required fail silent behaviour of the TTP module.

Apart from that, prior art document EP 1 355 460 A2 refers to a method for monitoring a communication media access schedule as described in the technical field above. However, for sufficient supervision the bus guardian according to prior art

document EP 1 355 460 A2 needs a priori knowledge, implemented in the form of one or more configuration parameters.

Despite all efforts as described above, the problem remains that conventional bus guardians need a costly data interface to protect the communication media from timing failures of the communication controller.

Starting from the disadvantages and shortcomings as described above and taking the prior art as discussed into account, an object of the present invention is to provide a bus guardian as well as a corresponding operating method

- requiring neither any a priori knowledge of the communication schedule nor any configuration parameter and
- monitoring the communication media access schedule of the communication controller even during start-up of the communication.

The object of the present invention is achieved by a bus guardian comprising the features of claim 1 as well as by a method comprising the features of claim 7. Advantageous embodiments and expedient improvements of the present invention are disclosed in the respective dependent claims.

The present invention is principally based on the idea to provide a bus guardian, in particular a FlexRay bus guardian, which has

- neither a configuration parameter set through special interface
- nor any a priori knowledge of the communication schedule.

In other words, the bus guardian does neither require any configuration, in particular any advance configuration or any pre-configuration, nor the implementation of a costly data interface but nevertheless grants supervision functionality, for example protects the communication media from timing failures of the communication controller.

This may be achieved in that the bus guardian is designed to learn within the first cycle about said communication media access schedule; this learned knowledge may be used regarding at least one possible schedule violation, in particular in order to differentiate or distinguish between at least one allowed deviation and at least one forbidden deviation caused by a failure of the communication controller during start-up.

A possible embodiment of a cycle of said communication media access schedule is a communication cycle comprising a periodic data transfer mechanism. Structure and timing of said communication cycle can for example be statically defined. Thus, the communication cycle may comprise a static segment only, i.e. a segment of the communication cycle where messages, in particular frames, are transmitted according to at least one statically defined T[ime]D[ivision]M[ultiple]A[ccess] scheme.

However, it is even possible that the communication cycle comprises beside the static segment also a dynamic segment, i.e. a segment where messages, in particular frames, are transmitted according to at least one mini-slotting algorithm. A communication cycle comprising static segments as well as dynamic segments is able to transmit state information as well as event information.

During start-up of the communication procedure the C[ommunication]C[ontroller] takes care of the start-up communication and may

- succeed to start up communication, i.e. sends appropriate communication elements,
- succeed to integrate into a communication schedule, i.e. performs clock synchronisation operation,
- notice by its own mechanism if the communication controller does not succeed to integrate into a communication schedule, for example due to wrong configuration.

Consequently, the bus guardian can advantageously rely on that the first (complete) communication cycle either is performed correctly by the C[ommunication]C[ontroller] or is aborted by the C[ommunication]C[ontroller]. Thus, the bus guardian can rely on the first communication cycle by the C[ommunication]C[ontroller] and learn about the communication schedule.

After learning in the first complete communication cycle(s) and with optionally taking some FlexRay protocol configuration constraints for plausibility checks into account, the bus guardian is able to perform its full operation and protect the media from faulty access.

To this aim, according to an advantageous embodiment of the present invention, the bus guardian is provided

- with at least one clock signal from at least one clock unit being

assigned to and/or comprised in the bus guardian and/or

- with at least one reset signal from any state and/or
- with at least one arming signal, in particular with at least one bus guardian ARMing signal, from the communication controller; said arming signal is advantageously the first trigger signal after starting the communication and designed for synchronising the bus guardian and the communication controller.

The present invention further relates to a node, in particular to an electronic control unit, of a distributed communication system with a number of nodes being interconnected by the communication media, in particular by one or more communication channels, the node comprising one or more bus guardians as described above.

Thus, the present invention supports the idea of having decentralised or peripheral bus guardians in each communication node. Since according to a preferred embodiment of the present invention the clock synchronisation and error detection mechanisms within the communication controller are able to detect slight deviations, for example clock drift over temperature, in the nominal communication schedule, the bus guardian only has to intervene at coarse deviations, for example at a clock stop.

The communication media is advantageously a physical connection between at least two nodes, in particular between at least two communication controllers. A possible embodiment of the communication media is for example a redundant bus comprising two channels connecting said at least two nodes.

By means of the communication media, messages, in particular frames, are transmitted between and among the nodes, in particular between and among the respective communication controllers of the nodes. In this context, a frame comprises all information being transmitted in the time during which a communication controller may access the communication medium on the channel(s).

According to a preferred embodiment of the present invention, the node comprises at least one bus driver, in particular at least one transceiver unit, for example being comprised of at least one sender unit and of at least one receiver unit, the bus driver being connected to the communication controller, to the bus guardian as well as to the communication media.

Said bus driver advantageously connects the communication controller to

the communication media. To prevent the communication media from timing failures of the communication controller, according to a preferred embodiment said bus driver can be controlled, in particular enabled and disabled, by the bus guardian.

For this reason, the bus driver may be provided

- with at least one signal, in particular with at least one transmit data input signal (so-called TxD signal), being transmitted from the communication controller, and/or
- with at least one transmit signal, in particular with at least one transmit data enable signal (so-called TxEN signal: low active), being transmitted from the communication controller also to the bus guardian and/or
- with at least one control signal, in particular with at least one bus guardian enable input signal (so-called BGEN signal: high active), being transmitted from the bus guardian.

Moreover, according to a preferred embodiment, the bus driver is designed for

- transmitting and receiving the messages via the communication media,
- transmitting at least one signal, in particular at least one receive data output signal (so-called RxD signal), to the communication controller and
- transmitting at least one receive signal, in particular at least one receive data enable output signal (so-called RxEN signal), to the communication controller as well as to the bus guardian.

Furthermore, according to a preferred embodiment, the node comprises at least one host unit, which can be implemented as the part of the node where at least one application software is executed. The host unit may be separated from the communication system or communication network by at least one C[ontroller]H[ost]I[nterface] which is arranged between the host unit and the communication controller.

The present invention further relates to a distributed fault-tolerant and/or time-triggered communication system or communication network with at least two nodes or electronic control units as described above.

Moreover, the present invention relates to a computer program

- being able to run on at least one computer, in particular on at least one microprocessor, for example on the communication controller as described above, and
- being programmed in order to execute a method as described above.

According to a preferred embodiment of the present invention, the computer program can be stored on at least one R[ead]O[nly]M[emory] module, on at least one R[andom]A[ccess]M[emory] module or on at least one flash memory module.

The present invention finally relates to the use of at least one bus guardian as described above and/or of at least one node as described above and/or of at least one distributed communication system as described above and/or of the method as described above and/or of at least one computer program as described above for ensuring error containment in the time domain of the node, in particular for synchronizing clocks of the communication system transmitting messages between and among the nodes across the communication media, for example in an at least dual-channel environment, wherein differences in offset of the clocks as well as differences in rate of the clocks can be corrected.

As already discussed above, there are several options to embody as well as to improve the teaching of the present invention in an advantageous manner. To this aim, reference is made to the claims respectively dependent on claim 1, on claim 3, on claim 7 and on claim 13; further improvements, features and advantages of the present invention are explained below in more detail with reference to preferred embodiments by way of example and to the accompanying drawings where

Fig. 1 schematically shows an embodiment of an electronic control unit or node according to the present invention, the electronic control unit or node working according to the method of the present invention;

Fig. 2 schematically shows the steps of the method of the present invention according to which the electronic control unit or node of Fig. 1 works;

Fig. 3A schematically shows a first embodiment of a fault-tolerant time-triggered network system according to the present invention, the network system comprising several electronic control units or nodes of Fig. 1;

Fig. 3B schematically shows a second embodiment of a fault-tolerant time-triggered network system according to the present invention, the network system comprising several electronic control units or nodes of Fig. 1.

The same reference numerals are used for corresponding parts in Fig. 1 to Fig. 3B.

In order to avoid unnecessary repetitions, the following description regarding the embodiments, characteristics and advantages of the present invention relates (unless stated otherwise)

- to the bus guardian 30 (cf. Fig. 1) according to the present invention, i.e. there is no need of configuring this bus guardian 30,
- to the electronic control unit or node 100 (cf. Fig. 1) according to the present invention,
- to the first embodiment of the distributed network system 200 (cf. Fig. 3A) according to the present invention as well as
- to the second embodiment of the distributed network system 200' (cf. Fig. 3B) according to the present invention,

all embodiments being operated according to the method (cf. Fig. 2) of the present invention.

Fig. 1 depicts a communication node, namely an E[lectronic]C[ontrol]U[nit] 100; two or more of such communication nodes 100 are connected in a communication system, namely in a FlexRay communication system 200, 200' as illustrated in Figs 3A, 3B.

The node 100 comprises basically five subsystems, namely

- a power supply unit or battery 50 with a voltage regulator 52 assigned to this power supply unit 50,

- a host unit 60,
- a communication controller 40,
- a bus driver 20 comprising a transceiver unit and being connected to a communication media 10, namely to a data bus comprising a first communication channel 12 and a redundant second communication channel 14 in order to transmit and/or to receive massages via the transceiver unit, and
- a bus guardian 30 on FlexRay protocol basis, in particular a so-called BGwop (= Bus Guardian without configuration parameter); in this context, the BGwop 30 is embodied as a minimal bus guardian for time-triggered architecture (FlexRay communication systems or communication networks 200, 200'), wherein the bus guardian 30 does not require any configuration parameters or any further a priori knowledge.

The BGwop 30 is in general proposed to protect the communication media 10 from timing failures of the communication controller 40. To this aim, the BGwop 30 is connected to the communication controller 40 as well as to the bus driver 20. Beside this, the BGwop 30 is independent of the protocol communication controller.

In particular, the BGwop 30 monitors the communication media access schedule of the communication controller 40 in order to prevent the communication controller 40 from blocking the communication media 10 by temporarily or continuously sending messages (so-called "babbling idiot" failure); in order to maintain independence of the two redundant channels 12, 14, the node 100 may also comprise two bus drivers 20 and two BGwops 30.

If during start-up of the communication procedure the communication controller 40 succeeds to start up communication, i.e. is able to send appropriate communication elements, the communication controller 40

- succeeds to integrate into a communication schedule, i.e. performs clock synchronisation operation, or
- does not succeed to integrate into a communication schedule, for example due to wrong configuration.

In the latter case of not succeeding to integrate into a communication schedule, the communication controller 40 notices this failure by itself.

Consequently, the BGwop 30 can rely on that the first completely

operated communication cycle either is correctly performed or is aborted by the communication controller 40. Thus, the BGwop 30 can learn about the communication schedule. After learning in the first complete communication cycle and with taking some FlexRay protocol configuration constraints for plausibility checks into account the BGwop 30 is able to perform its full operation and protect the communication media 10 from faulty access.

As can be taken from Fig. 1, the BGwop 30 is provided with the following input signals:

- an arming signal 403, namely a bus guardian arming signal ARM, from the communication controller 40, wherein a falling edge of said signal ARM indicates a start of the communication cycle;
- a transmit signal 423, namely a transmit data enable signal TxEN wherein
  -- the logical low state of said signal TxEN indicates a transmit access and
  -- said signal TxEN is transmitted from the communication controller 40 not only to the BGwop 30 but also to the bus driver 20;
- a receive signal 243, namely a receive data enable output signal RxEN, wherein
  -- the logical low state of said signal RxEN indicates activity on the communication media 10 and
  -- said signal RxEN is transmitted from the bus driver 20 not only to the BGwop 30 but also to the communication controller 40;
- a reset signal 304 from any state 34 (cf. Fig. 2); and
- a clock signal 303 from a clock unit 32 being assigned to the BGwop 30; the clock signal 303 can alternatively be generated internally in the BGwop 30.

The BGwop 30 puts out

- a control signal 302, namely a bus guardian enable input signal BGEN (HIGH active) to the transmitter unit of the bus driver 20 in order to enable and disable one or more output stages of the bus driver 20, in particular for disabling transmission in case of schedule violations SV1, SV2, SV3 (cf. Fig. 2)

and

- a signal 306, namely an error flag indication signal, for example a single bit "error not" ERRN signal, to the host 60.

As can be further taken from Fig. 1, the bus driver 20 is

- provided with a signal 402, namely with a transmit data input signal TxD, being transmitted from the communication controller 40, and
- designed for transmitting a signal 204, namely a receive data output signal RxD, to the communication controller 40.

The host unit 60 is connected to the bus driver 20, to the BGwop 30 as well as to the communication controller 40. Beside this, the host unit 60 is designed for

- transmitting a control signal 602 to the bus driver 20 and receiving a status data signal 206 from the bus driver 20 (wherein neither said control signal 602 nor said status data signal 206 are related to the actual communication within the network 200); and
- transmitting a signal 406 to the communication controller 40 and receiving said signal 406 from the communication controller 40.

The power supply unit 50, namely the battery, is connected with ground GND and with the bus driver 20; the voltage regulator 52 is connected with

- the power supply unit 50,
- the host unit 60,
- the communication controller 40 and
- the bus driver 20.

The protocol of the FlexRay communication system 200 (cf. Fig. 3A), 200' (cf. Fig. 3B) can be divided into various layers of a layer architecture comprising

- a physical layer which defines how signals are actually transmitted; one task of the physical layer is to detect errors of the communication controller 40 in the time domain, which is done by the BGwop 30;
- a transfer layer which represents the kernel of the FlexRay protocol;
- a presentation layer which is concerned with frame filtering, frame masking, and frame status handling; and
- an application layer.

A state diagram of the BGwop 30 is depicted in Fig. 2. The BGwop 30

[i] enters BGwop_wake up mode after being provided with the reset signal 304 from any state 34;

[ii] enters BGwop_start up mode after being provided with the first falling edge of the arming signal 403;

[iii] enters BG_guarding mode after being provided with the second falling edge of the arming signal 403; and

[iv] enters BG_fail silent mode upon detection of one or more of the possible schedule violations SV1, SV2, SV3.

In the following the states or modes [i], [ii], [iii], [iv] of the BGwop 30 are described in more detail:

Step [i] of waking up comprises enabling the bus driver 20, namely the transmitter unit of the bus driver 20. During said step [i] the first type SV1 of the possible schedule violations SV1, SV2, SV3 can be detected

- after a certain amount of negative edges of the transmit signal 423, for example after a maximum of 63 W[ake-]U[p]S[ymbols], and/or
- upon a negative edge of said transmit signal 423, while the receive signal 243 is on logical low state, and/or
- when said transmit signal 423 is on logical low state for longer than a certain timeout dWU_0 of about or less than six microseconds, and/or
- when the clock unit 32 stops.

Step [ii] of starting up comprises the steps of

- enabling the transmitter unit of the bus driver 20,
- counting clock cycles in order to learn about the cycle time, and
- counting clock cycles until the first falling edge of said transmit signal 423, wherein in particular during the first cycle no dynamic frame is sent; in this context, a frame comprises all information transmitted in one slot with one identifier on one communication channel 12, 14 (in case of FlexRay protocol any further, in particular the second, communication channel 14 is redundant and thus optional).

During said step [ii] the second type SV2 of the possible schedule violations SV1, SV2, SV3 can be detected

- after a certain amount of negative edges of said transmit signal 423, for example after a maximum of sixteen static slots per C[ommunication]C[ontroller] 40, and/or
- upon a negative edge of said transmit signal 423, while said receive signal 243 is on logical low state, and/or
- when said transmit signal 423 is on logical low state for longer than a certain timeout of about 2.047 microseconds, and/or
- when the cycle time is longer than a certain timeout of about sixteen milliseconds, and/or
- when the clock unit 32 stops.

Step [iii] of guarding comprises the steps of

- enabling the transmitter unit of the bus driver 20, and
- counting clock cycles in order to supervise the cycle time.

During said step [iii] the third type SV3 of the possible schedule violations SV1, SV2, SV3 can be detected

- upon a certain, namely the X_{cycle}th, negative edge of the transmit signal 423, wherein X_{Cycle} sets a protocol configuration constraint, and/or
- upon a negative edge of said transmit signal 423, while said receive signal 243 is on logical low state, and/or
- when said transmit signal 423 is on logical low state for longer than a certain timeout of about 2.047 microseconds, and/or
- when the cycle time deviates more than a certain margin from at least one cycle time learned during step [ii], and/or
- when a time span between respective falling edges of the arming signal 403 and of the transmit signal 423 deviates more than a certain margin from the time span learned during step [ii], and/or
- when the clock unit 32 stops.

The step [iv] of behaving fail silent comprises the steps of

- disabling the transmitter unit of the bus driver 20, and
- not monitoring the input signals except the reset signal 304.

Two embodiments of an x-by wire FlexRay communication system 200, 200' are depicted in Figs 3A, 3B. The x-by wire FlexRay communication system 200,

200' can be arranged

- in linear bus topology (cf. Fig. 3A) or
- in star bus topology (cf. Fig. 3B).

A possible combination of linear bus topology according to Fig. 3A and of star bus topology according to Fig. 3B makes the x-by wire FlexRay-communication system 200, 200' very flexible.

LIST OF REFERENCE NUMERALS

100	node, in particular E[lectronic]C[ontrol]U[nit]
10	communication media
12	communication channel, in particular first communication channel, of communication media 10
14	optional further, in particular redundant second, communication channel of communication media 10
20	bus driver, in particular transceiver, for example combination of transmitter and of receiver, assigned to communication media 10, in particular assigned to communication channel 12 and/or to optional further communication channel 14
204	signal, in particular receive data output signal RxD, from bus driver 20 to communication controller 40
206	signal, in particular status data signal, from bus driver 20 to host unit 60
243	receive signal, in particular receive data enable output signal RxEN, from bus driver 20 to communication controller 40 as well as to bus guardian 30
30	bus guardian, in particular without configuration parameter(s) and without any other a priori knowledge
32	clock unit, in particular clock
302	control signal, in particular bus guardian enable input signal BGEN: high active, from bus guardian 30 to bus driver 20
303	clock signal, in particular from clock unit 32 to bus guardian 30
304	reset signal from any state 34
306	signal, in particular error flag indication signal ERRN, from bus guardian 30 to host unit 60
34	any state
36	power on
40	communication controller
402	signal, in particular transmit data input signal TxD, from communication controller 40 to bus driver 20

403	arming signal, in particular bus guardian arming signal ARM, from communication controller 40 to bus guardian 30
406	signal between communication controller 40 and host unit 60
423	transmit signal, in particular transmit data enable signal TxEN: low active, from communication controller 40 to bus driver 20 as well as to bus guardian 30
50	power supply unit, in particular battery
52	voltage regulator
60	host unit, in particular application host
602	signal, in particular control signal, from host unit 60 to bus driver 20
200	communication system, in particular with linear topology (first embodiment; cf. Fig. 3A)
200'	communication system, in particular with star topology (second embodiment; cf. Fig. 3B)
ARM	bus guardian arming signal from communication controller 40 to bus guardian 30
BGEN	bus guardian enable input signal (HIGH active) from bus guardian 30 to bus driver 20
ERRN	error flag indication signal between bus guardian 30 and host unit 60
GND	ground
RxD	receive data output signal from bus driver 20 to communication controller 40
RxEN	receive data enable output signal from bus driver 20 to communication controller 40 as well as to bus guardian 30
SV1	schedule violation, in particular first type of deviation from said communication media access schedule
SV2	schedule violation, in particular second type of deviation from said communication media access schedule
SV3	schedule violation, in particular third type of deviation from said communication media access schedule
TxD	transmit data input signal from communication controller 40 to bus driver 20
TxEN	transmit data enable signal (LOW active) from communication controller 40 to bus driver 20 as well as to bus guardian 30

CLAIMS:

1. A bus guardian (30) for monitoring communication between and among a number of nodes (100), in particular between and among a number of electronic control units, the bus guardian (30)

- being designed for monitoring at least one cyclic time-triggered communication media access schedule for transmitting messages between and among the nodes (100) across at least one communication media (10), in particular across at least one channel (12) and across at least one optional further channel (14), and

- being assigned to at least one communication controller (40), the communication controller (40) comprising the communication media access schedule, characterized in

- that the bus guardian (30) is able to learn, in particular within the first cycle, about said communication media access schedule, and

- that the bus guardian (30) makes use of the learned knowledge with respect to at least one possible schedule violation (SV1, SV2, SV3), in particular with respect to at least one deviation from said communication media access schedule, for example during start-up of the communication.

2. The bus guardian according to claim 1, characterized by being provided with

- at least one clock signal (303) from at least one clock unit (32) being assigned to and/or comprised in the bus guardian (30) and/or

- at least one reset signal (304) from any state (34) and/or

- at least one arming signal (403), in particular at least one bus guardian arming signal (ARM), from the communication controller (40).

3. A node (100), in particular an electronic control unit, of a distributed communication system (200, 200') with a number of nodes (100) being interconnected by at least one communication media (10), in particular by at least one channel (12) and by at least one optional further channel (14), characterized by at least one bus guardian (30) according to claim 1 or 2.

4. The node according to claim 3, characterized by at least one bus driver (20), in particular at least one transceiver unit,

- being connected
  -- to the communication controller (40),
  -- to the bus guardian (30), as well as
  -- to the communication media (10),
- being controlled, in particular being enabled and disabled, by the bus guardian (30),
- being provided with
  -- at least one signal (402), in particular at least one transmit data input signal (TxD), being transmitted from the communication controller (40),
  -- at least one transmit signal (423), in particular at least one transmit data enable signal (TxEN: low active), being transmitted from the communication controller (40) also to the bus guardian (30), and
  -- at least one control signal (302), in particular at least one bus guardian enable input signal (BGEN: high active), being transmitted from the bus guardian (30), and
- being designed for
  -- transmitting and receiving the messages via the communication media (10),
  -- transmitting at least one signal (204), in particular at least one receive data output signal RxD, to the communication controller (40), and
  -- transmitting at least one receive signal (243), in particular at least one receive data enable output signal RxEN, to the communication controller (40) as well as to the bus guardian (30).

5. The node according to claim 3 or 4, characterized by

- at least one host unit (60)
-- being connected
--- to the bus driver (20),
--- to the bus guardian (30), as well as
--- to the communication controller (40), and
-- being designed for
--- transmitting at least one signal (602), in particular at least one control signal, to the bus driver (20),
--- receiving at least one signal (206), in particular at least one status data signal, from the bus driver (20),
--- receiving at least one signal (306), in particular at least one error flag indication signal (ERRN), from the bus guardian (30), and
--- transmitting and/or receiving at least one signal (406) to and/or from the communication controller (40), and/or
- at least one power supply unit (50), in particular at least one battery, being connected with ground (GND) and with the bus driver (20), and/or
- at least one voltage regulator (52) being connected with
-- the power supply unit (50),
-- the host unit (60),
-- the communication controller (40), and
-- the bus driver (20).

6. A distributed fault-tolerant and/or time-triggered communication system (200, 200') with at least two nodes (100) according to at least one of claims 3 to 5.

7. A method for monitoring communication between and among a number of nodes (100), in particular between and among a number of electronic control units, the method comprising the steps of

- transmitting messages between and among the nodes (100) based on at least one cyclic time-triggered communication media access schedule being assigned to at least one communication controller (40) and
- monitoring the communication media access schedule by means of at least one bus guardian (30),

characterized in

- that the bus guardian (30) is able to learn, in particular within the first cycle, about said communication media access schedule, and
- that the bus guardian (30) makes use of the learned knowledge with respect to at least one possible schedule violation (SV1, SV2, SV3), in particular with respect to at least one deviation from said communication media access schedule, for example during start-up of the communication.

8. The method according to claim 7, characterized in that the bus guardian (30), in particular after the power (36) being switched on,

[i] wakes up after being provided with at least one reset signal (304) from any state (34),

[ii] starts up after being provided with the first falling edge of at least one arming signal (403), in particular of at least one bus guardian arming signal (ARM), from the communication controller (40),

[iii] enters guarding after being provided with the second falling edge of the arming signal (403), and

[iv] behaves fail silent upon detection of at least one of the possible schedule violations (SV1, SV2, SV3).

9. The method according to claim 8, characterized in

- that step [i] of waking up comprises the step of enabling at least one bus driver (20), in particular at least part of at least one transceiver unit, for example at least one transmitter unit, and
- that during said step [i] the first type of schedule violation (SV1) can be detected

-- after a predetermined amount of negative edges of at least one transmit signal (423), in particular of at least one transmit data enable signal (TxEN: low active), from the communication controller (40) to the bus driver (20) as well as to bus guardian (30), and/or

-- upon a negative edge of said transmit signal (423), while at least one receive signal (243), in particular at least one receive data enable output signal (RxEN), from the bus driver (20) to the communication controller (40) as well as to bus guardian (30) is on logical low state, and/or

-- when said transmit signal (423) is on logical low state for at least one predetermined time period, in particular for longer than a certain timeout of about or less than six microseconds, and/or

-- when at least one clock unit (32) being assigned to the bus guardian (30) stops.

10. The method according to claim 8 or 9, characterized in

- that step [ii] of starting up comprises the steps of

-- enabling the bus driver (20), in particular at least part of the transceiver unit, for example the transmitter unit,

-- counting clock cycles in order to learn about the cycle time, and

-- counting clock cycles until the first falling edge of said transmit signal (423), wherein in particular during the first cycle no dynamic frame is sent, a frame comprising all information transmitted in at least one slot with at least one identifier on at least one channel (12, 14), and

- that during said step [ii] the second type of schedule violation (SV2) can be detected

-- after a predetermined amount of negative edges of said transmit signal (423), and/or

-- upon a negative edge of said transmit signal (423), while said receive signal (243) is on logical low state, and/or

-- when said transmit signal (423) is on logical low state for at least one predetermined time period, in particular for longer than a certain timeout of

about 2.047 microseconds, and/or

-- when the cycle time is longer than a certain timeout of about sixteen milliseconds, and/or

-- when the clock unit (32) stops.

11. The method according to at least one of claims 8 to 10, characterized in

- that step [iii] of guarding comprises the steps of

-- enabling the bus driver (20), in particular at least part of the transceiver unit, for example the transmitter unit,

-- counting clock cycles in order to supervise the cycle time, and

- that during said step [iii] the third type of schedule violation (SV3) can be detected

-- upon a certain, in particular the X_{cycle}th, negative edge of the transmit signal (423), and/or

-- upon a negative edge of said transmit signal (423), while said receive signal (243) is on logical low state, and/or

-- when said transmit signal (423) is on logical low state for at least one predetermined time period, in particular for longer than a certain timeout of about 2.047 microseconds, and/or

-- when the cycle time deviates more than a predetermined margin from at least one cycle time learned during said step [ii], and/or

-- when a time span between respective falling edges of the arming signal (403) and of the transmit signal (423) deviates more than a predetermined margin from at least one time span learned during said step [ii], and/or

-- when the clock unit (32) stops.

12. The method according to at least one of claims 7 to 11, characterized in that step [iv] of behaving fail silent comprises the steps of

- disabling the bus driver (20), in particular at least part of the transceiver unit, for example the transmitter unit, and

- not monitoring the input signals except the reset signal (304).

13. A computer program being able to run on at least one computer, in particular on at least one microprocessor, for example on the communication controller (40), characterized in that the computer program is programmed in order to execute a method according to at least one of claims 7 to 12.

14. The computer program according to claim 13, characterized in that the computer program is stored

- on at least one R[ead]O[nly]M[emory] module,
- on at least one R[andom]A[ccess]M[emory] module, or
- on at least one flash memory unit.

15. Use of at least one bus guardian (30) according to claim 1 or 2 and/or of at least one node (100) according to at least one of claims 3 to 5 and/or of at least one distributed communication system (200, 200') according to claim 6 and/or of the method according to at least one of the claims 7 to 12 and/or of at least one computer program according to claim 13 or 14 for ensuring error containment in the time domain of the node (100), in particular for synchronizing clocks (32) of the communication system (200, 200') transmitting messages between and among the nodes (100) across the communication media (10), for example in an at least dual-channel (12, 14) environment, wherein differences in offset of the clocks as well as differences in rate of the clocks can be corrected.

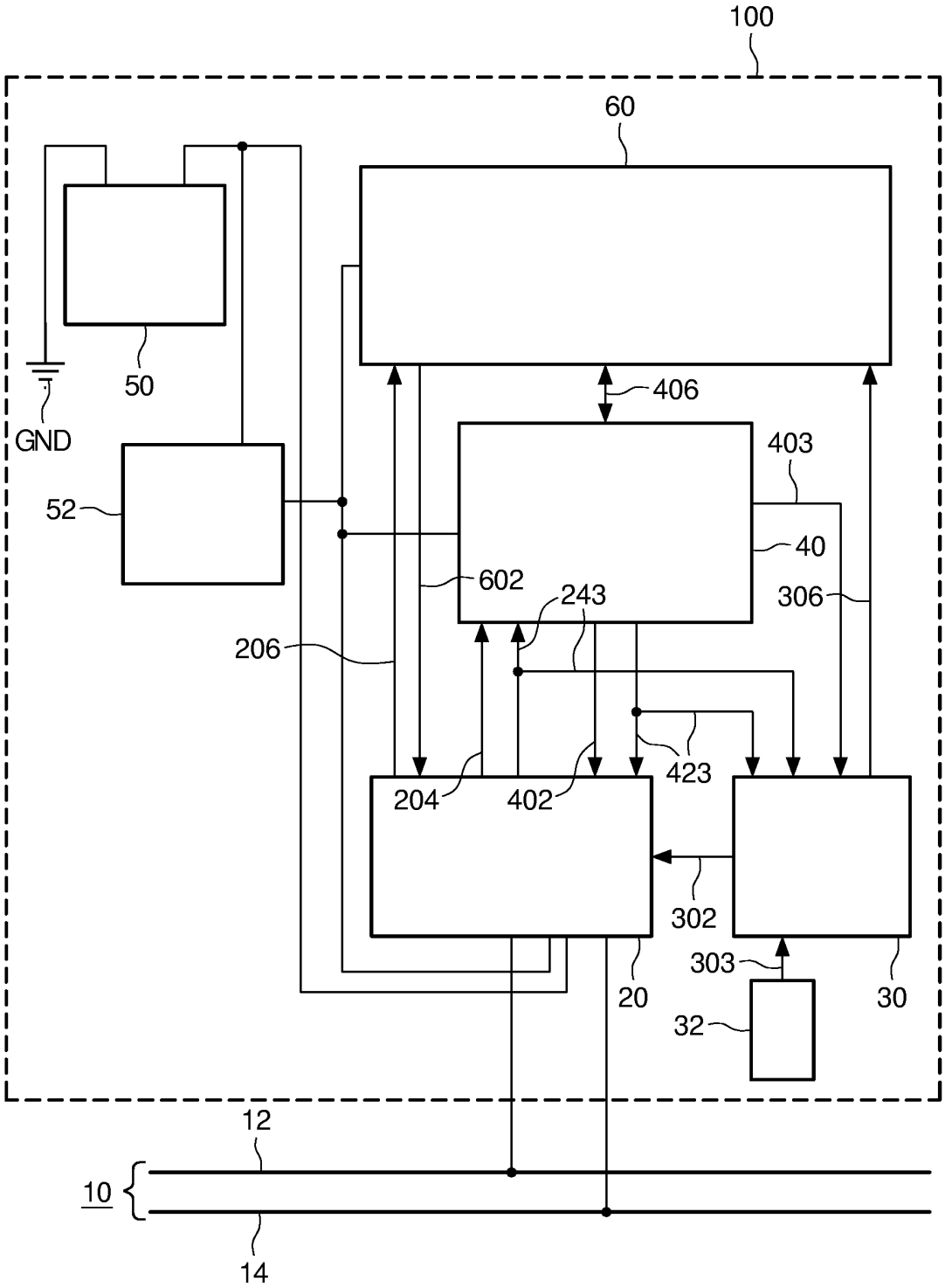

100
60
50
GND
406
403
52
40
602
243
306
206
423
204
402
302
303
20
30
32
12
10
14

FIG. 1

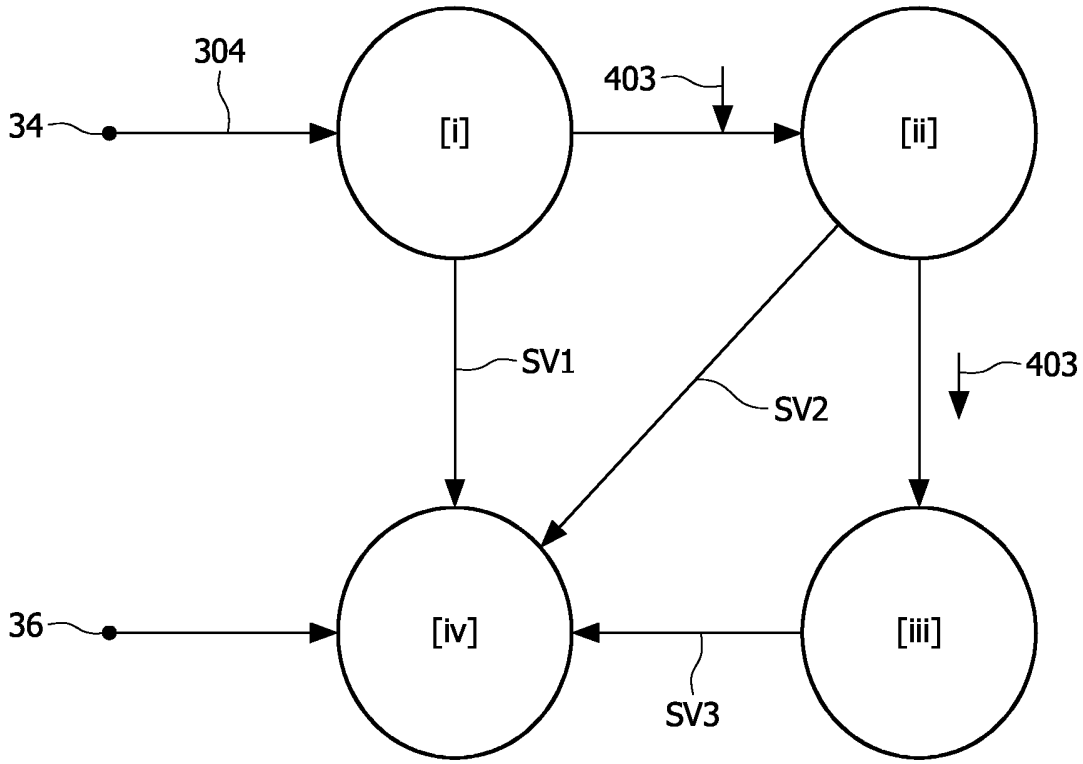


FIG. 2

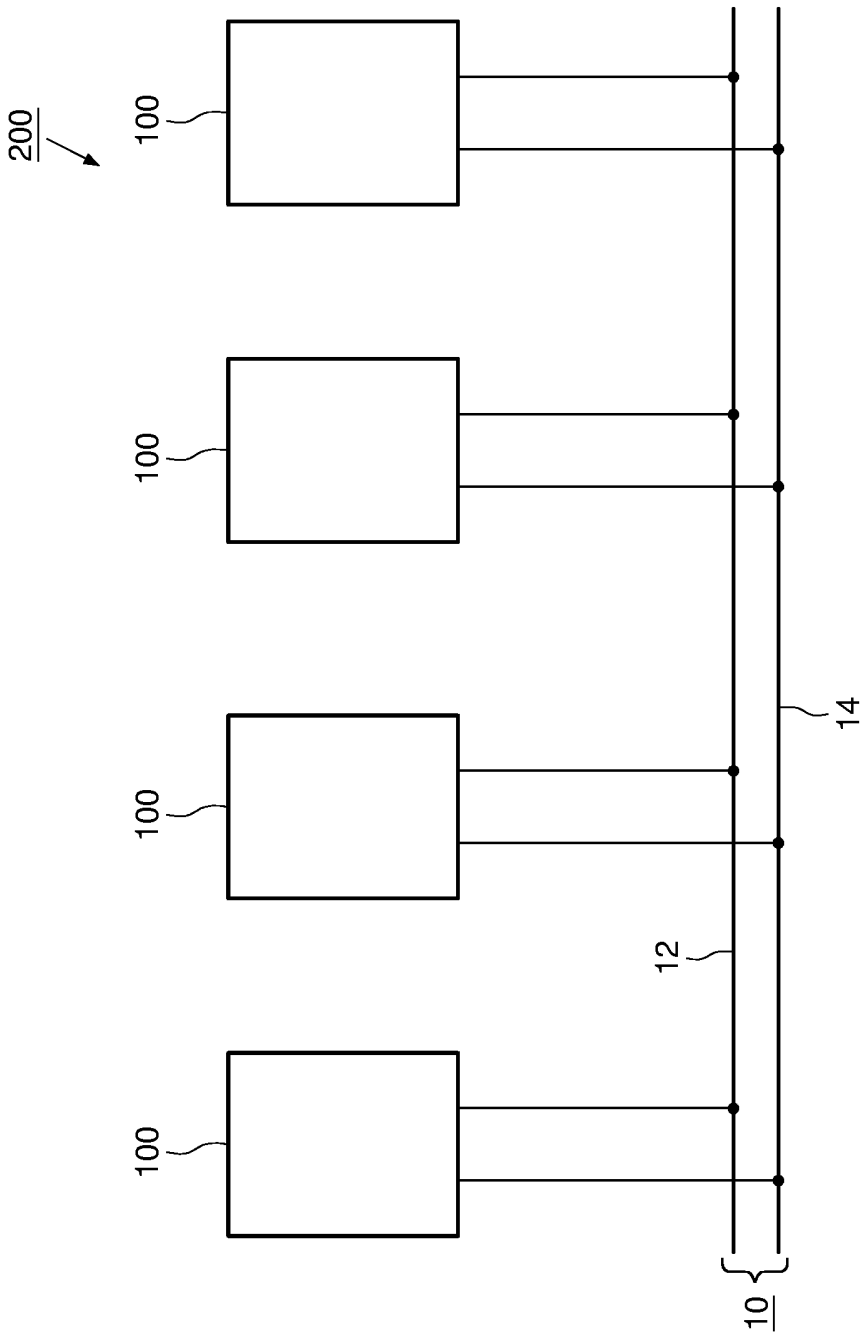


FIG. 3A

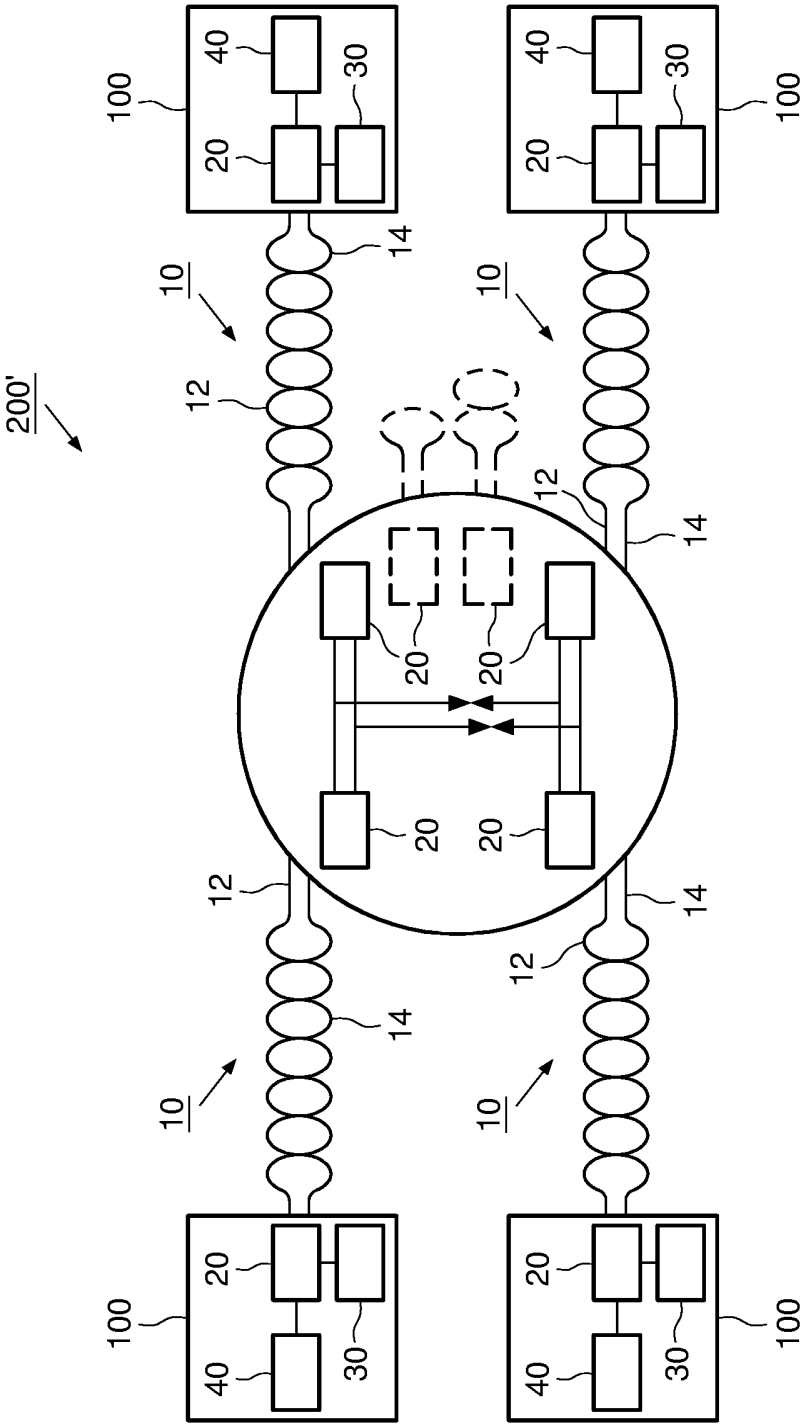


FIG. 3B