



(12) 发明专利

(10) 授权公告号 CN 102189995 B

(45) 授权公告日 2016.03.16

(21) 申请号 201110048980.9

KR 10-2009-0082727 A, 2009.07.31,

(22) 申请日 2011.02.28

CN 1577197 A, 2005.02.09,

(30) 优先权数据

审查员 马娟娟

102010002468.6 2010.03.01 DE

(73) 专利权人 罗伯特·博世有限公司

地址 德国斯图加特

(72) 发明人 傅承焯 W·费伊赫特 R·比肖夫

(74) 专利代理机构 中国专利代理(香港)有限公司

72001

代理人 曹若 梁冰

(51) Int. Cl.

G05B 9/02(2006.01)

(56) 对比文件

US 6628993 B1, 2003.09.30,

US 4853932 A, 1989.08.01,

DE 3841400 A1, 1989.07.06,

WO 2008/119869 A1, 2008.10.09,

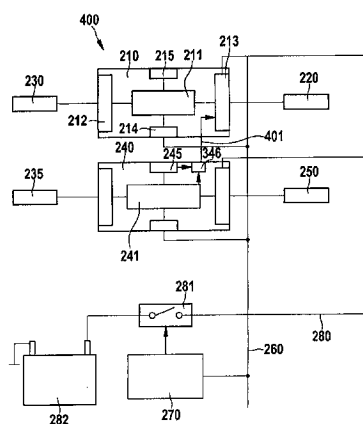
权利要求书1页 说明书3页 附图4页

(54) 发明名称

用于使在汽车中由控制器控制运行的功能单元停止运行的方法

(57) 摘要

本发明涉及一种使汽车中由第一控制器(210)控制运行的功能单元(220)停止运行的方法,其中,第一控制器(210)具有用于功能单元(220)运行的内部末级电路(213),其中,规定第二控制器(240)用于监控第一控制器(210),其中,当通过第二控制器(240)识别到第一控制器(210)的功能故障时由第二控制器(240)断开第一控制器的内部末级电路(213)。此外,本发明还涉及一种相应的监控装置(400)。



1. 用于使汽车中由第一控制器(210)运行的功能单元(220)停止运行的方法,其中,第一控制器(210)具有用于功能单元(220)的运行的内部末级电路(213),其中,规定第二控制器(240)用于监控第一控制器(210),其中,当通过第二控制器(240)识别到第一控制器(210)的功能故障时由第二控制器(240)断开第一控制器(210)的内部末级电路(213),其中第二控制器(240)内部的断开线路从功能计算机(241)和监控模块(245)出发首先聚集在聚集器(246)中,并且紧接着通过所述断开线路(401)通往第一控制器(210)的内部末级电路(213)。

2. 按照权利要求1所述的方法,其中,为断开使用至少一个自己的断开线路(401)。

3. 按照权利要求1或2所述的方法,其中,由第二控制器(240)的功能计算机(241)断开第一控制器(210)的内部末级电路(213)。

4. 按照权利要求1或2所述的方法,其中,由第二控制器(240)的监控模块(245)断开第一控制器(210)的内部末级电路(213)。

5. 按照权利要求1或2所述的方法,其中,断开内部末级电路(213)中的开关元件,或者使其停止工作。

6. 按照权利要求1或2所述的方法,其中,断开内部末级电路(213)中的电压提供电路,或者使其停止工作。

7. 监控装置(400),包括至少一个第一控制器(210)和至少一个用于监控第一控制器(210)的第二控制器(240),其中,第一控制器(210)具有用于运行功能单元的内部末级电路(213),其中,为了通过第二控制器(240)断开第一控制器(210)的内部末级电路(213),在第二控制器(240)和第一控制器(210)之间设置直接的断开线路(401),其中第二控制器(240)内部的断开线路从功能计算机(241)和监控模块(245)出发首先聚集在聚集器(246)中,并且紧接着通过所述断开线路(401)通往第一控制器(210)的内部末级电路(213)。

8. 按照权利要求7所述的监控装置,其中,设置断开线路,从而它可由第二控制器(240)的功能计算机(241)和/或监控模块(245)进行触发。

用于使在汽车中由控制器控制运行的功能单元停止运行的方法

技术领域

[0001] 本发明涉及一种用于使在汽车中由第一控制器控制运行的功能单元,例如电动机或者动作器停止运行的方法,以及一种包括至少两个控制器的监控装置。

背景技术

[0002] 在汽车中的对安全重要的功能单元中,例如在电子的发动机填充控制系统 (EGAS) 中,为了进行安全监控在运行的控制器中使用了一种所谓的三级方案。其中主要是在控制器的内部在功能计算机 (计算单元, CPU) 和单独的监控模块 (看门狗 (Watchdog)) 之间相互进行监控。功能计算机和监控模块通过问 - 答通信进行联系,并且在发生故障时可使控制器中的功率末级 - 它的设置是用于功能单元的运行 - 停止运行,并且因此保证汽车的安全。

[0003] 例如当电动机作为功能单元由控制器控制运行时一级就是原来的功能软件,它是功能单元运行时所需要的。在功能计算机上执行这个软件。在二级中 - 它也在功能计算机上被执行 - 一个借助简化的发动机模型计算出来的允许的力矩和一个发动机的实际力矩进行比较。这一级在一个通过三级得到保护的硬件区域中被执行。指令检测、程序运行控制、A/D 转换器检测以及周期性的和完全的存储器检测是三级的组成部分。如 DE 44 38 714 A1 所公开的,在实际的电子的发动机填充控制系统中在控制器中设置有功能 - 监控软件。

[0004] 此外还公开了一种 2 计算机方案。在对安全特别重要的功能单元,例如 ABS- 或者 ESP 系统运行时使用了这种 2 计算机方案。在这方面 DE 103 31 872 A1 公开了一种用连网的控制器监控系统的方法,其中,这些控制器分别具有至少一个计算元件,并且分别执行对监控重要的控制程序以及监控程序。

[0005] 监控系统的控制器通过总线系统,例如 CAN、FlexRay 或者以太网彼此进行通信。二级功能 / 模块可自由地分布到所有在联合网络上连接的控制器上,这样一个控制器中的一级模块就可由另一个或者另一些控制器的二级模块进行监控。分布在多个控制器中的监控有如下优点,即通过附加的余度设计可减少监控功能特性的故障概率。这样,分散的监控可以达到比三级方案更高的车辆安全集成级别 (ASIL Level)。

[0006] 在分散的监控中的已公开的断开方案是断开能源供给。至少两个控制器可通过通信网络给能源管理系统发送断开请求,然后这个能源管理系统就给整个监控系统断开能源供给。然而这个断开方案有一系列的缺陷。一方面它是以能量管理系统中的高的 ASIL 水平为前提,也就是说断开功能特性必须是“本安型”的 (eigensicher)。这个问题由于下述情况变得更加突出,即能源管理系统的生产厂家也不必是监控系统或者监控装置的生产厂家。

[0007] 此外,使监控系统的功能检测变得困难,因为对能源供给系统提出的断开要求可能会导致整个汽车电气设备停止工作。此外,在电池系统中的主保险装置 (例如断路器 - 继电器) 通常在不承载时是可打开的,因为这会损伤或者破坏主保险装置。因此例如在功能

检测的框架中的断开导致维护费用的提高和附加的成本。总之通过这种做法也增加了例如在研发期间的断开试验的困难。

[0008] 此外, 因为是通过通信网络由控制器将断开请求传输给能源管理系统的, 所以由于例如 EMV 干扰出现图像跳动或者信息短缺时会增加故障情况时的反应时间。

[0009] 根据现有技术的这种情况人们希望在 2 计算机方案中能就功能单元的断开问题提出一种改进的办法。

发明内容

[0010] 根据本发明建议一种具有独立权利要求特征的用于使由第一控制器控制运行的功能单元停止运行的方法以及一种监控装置。一些有利的方案是从属权利要求以及下述说明的主题。

[0011] 本发明的优点

[0012] 本发明通过一个监控的第二控制器实现第一控制器的确定功率的末级电路的直接断开。通过这一措施可避免在现有技术中所描述的那些缺陷。故障反应时间是恒定的, 并且因此是可计算机的, 并且是可重复的。具有多个控制器的整个监控装置是本安型的。因此系统的功能安全性和外购产品, 例如和能源管理系统无关。在断开过程中或者在检测时也不会损伤部件, 因为根据规定末级电路是可接通的。通过这一措施和现有技术相比提高了汽车的可供使用性, 其改进了可维修性。特别应强调的是通过附加的冗余设计附加地提高了安全性或降低了故障概率。

[0013] 从说明书和附图可得到本发明的其它优点和方案。

[0014] 当然, 前面所述的特征和下面还将说明的特征不仅可在各个已说明的组合中使用, 而且在不脱离本发明的框架的情况下也可在其它的组合中使用, 或者单独使用。

[0015] 借助附图中的实施例简图示出本发明, 下面参考附图对本发明进行详细的说明。

附图说明

[0016] 图 1: 监控装置, 它包括两个现有技术的控制器。

[0017] 图 2: 根据本发明的监控装置的一个优选的实施形式。

[0018] 图 3: 根据本发明的监控装置的一个第二优选的实施形式。

[0019] 图 4: 根据本发明的监控装置的另一优选的实施形式。

具体实施方式

[0020] 在图 1 中简图示出了一个现有技术的监控装置 100 的电路平面图。该监控装置包括一个用于第一功能单元 120 的运行的第一控制器 110 以及一个用于功能单元 150 的运行的第二控制器 140。控制器 110 具有一个功能计算机 (计算单元或者 CPU) 111。这个功能计算机和一个用于接收例如传感器 130 的传感器信号的接口 112 相连接。这个功能计算机 111 处理传感器信号, 并且根据处理和它的编程对用于功能单元 120 的运行的末级电路 113 进行触发。此外控制器 110 还具有一个用于和通信总线 160 相耦合的接口 114, 并且具有一个用于监控功能计算机 111 的功能能力的监控模块 (看门狗) 115。

[0021] 控制器 110 的末级电路 113 通过一个引线 180 和一个主保护装置 181 和一个能源

提供装置,在此是一个电池 182 相连接。为了对能源提供装置进行检查设置了一个能源管理系统 170。这个能源管理系统也和通信总线 160 连接,并且针对相应的请求触发主保险装置 181,以便切断电源。

[0022] 第二控制器 140 在它的结构上和第一控制器 110 相应,在此就不详细介绍了。在控制器 140 内部的一些部件用增加 30 的附图标记表示。第二控制器 140 和一个或者多个传感器 135 连接,并且运行功能单元 150。

[0023] 功能单元 120、150 特别是可以为电动机,其中,末级电路 113、143 例如包括用于脉冲逆变器的晶体管或者 IGBT。

[0024] 为了实现 2 计算机方案第一控制器 110 和第二控制器 140 彼此相互监控,并且当确定有故障时通过通信总线 160 给能源管理系统 170 发送一个断开请求。

[0025] 在下述图中介绍根据本发明的优选的实施形式的与之相比改进的监控系统。在图 2 到图 4 中相同的部件用相同的附图标记表示。那些和附图 1 中的部件相同的部件用提高 100 的附图标记表示。

[0026] 根据图 2 的本发明的监控装置的优选的实施形式 200 在第二控制器 240 的功能计算机 241 和第一控制器 210 的末级电路 213 之间有一个直接的连接导线 201。通过导线 201 上的信号,例如数字信号或者 PWM- 信号,第二控制器 240 可直接将第一控制器 210 的末级电路活化或者去活化。例如在数字信号中高电平表示“活化”,并且低电平 (Low-Pegel) 表示“不活化”,或者在 PWM 信号中有信号表示“活化”,无信号则表示“不活化”。

[0027] 在根据图 3 的监控系统的第二优选的实施形式 300 中附加地在第二控制器 240 的监控模块 245 和第一控制器 210 的末级电路 213 之间设置了一个断开线路 301。这个方案具有下述优点,即即使第二控制器 240 的功能计算机 241 的功能出现故障时第二控制器 240 的监控模块 245 也可通过断开线路 301 断开第一控制器 210 中的末级电路 213。

[0028] 在图 3 中示出了一个优选的实施形式。在这个实施形式中除了断开线路 301 外还设置了根据图 2 的断开线路 201。虽然如此还需提到的是,也可以有这样的实施形式,在此实施形式中只设置断开线路 301。

[0029] 在图 4 的优选的实施形式 400 中第二控制器 240 内部的一些断开线路从功能计算机 241 和监控模块 245 出发首先聚集在一个聚集器 246 中,例如一个“与”元件中,并且紧接着通过断开线路 401 通往第一控制器 210 的末级电路 213。按照这种方式保留了既能通过第二控制器的功能计算机 241,也能通过监控模块 245 断开的优点,其中,虽然如此在控制器之间只需设置一个物理的断开线路。

[0030] 断开末级电路例如可以包括停止在末级电路中设置的晶体管,IGBT、开关等的运行。代替地或者附加地断开末级电路也可以包括停止必要时在末级电路中设置的变压器等的运行。也可在末级电路中专门为断开电路设置一些开关元件,这些开关元件由第二控制器的断开线路进行触发。虽然在图 2 到图 4 中只示出了通过第二控制器断开第一控制器的末级电路的情况,但是在本发明的方案中也可相互进行监控和断开。

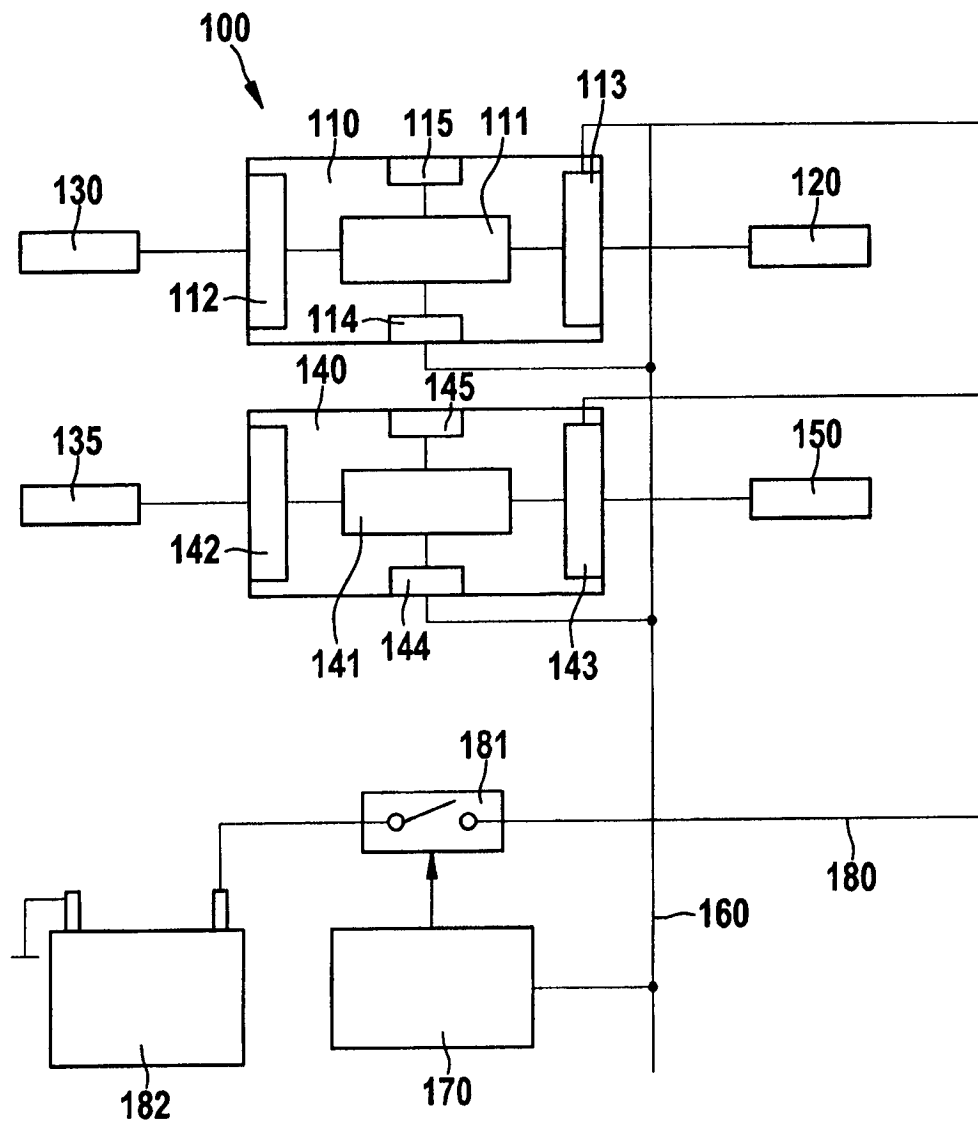


图 1

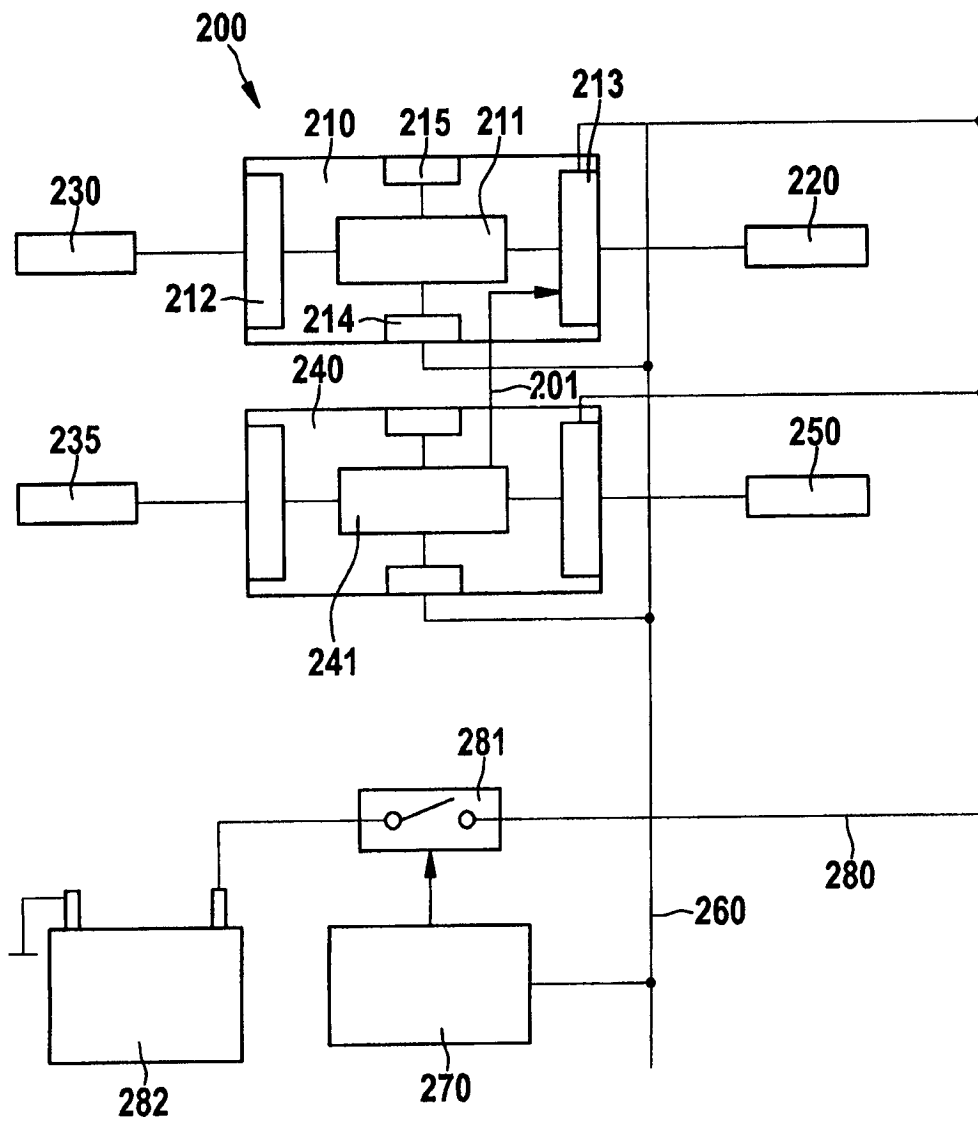


图 2

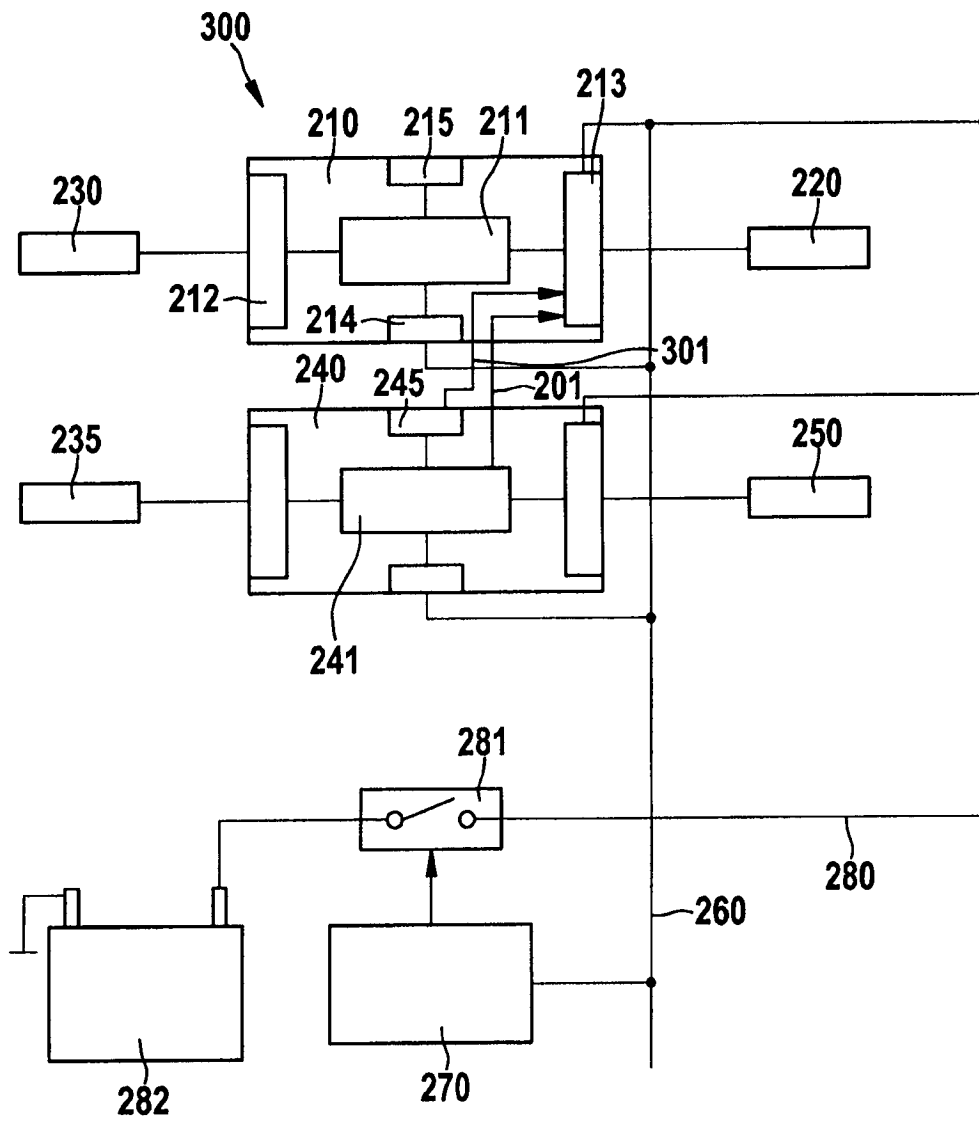


图 3

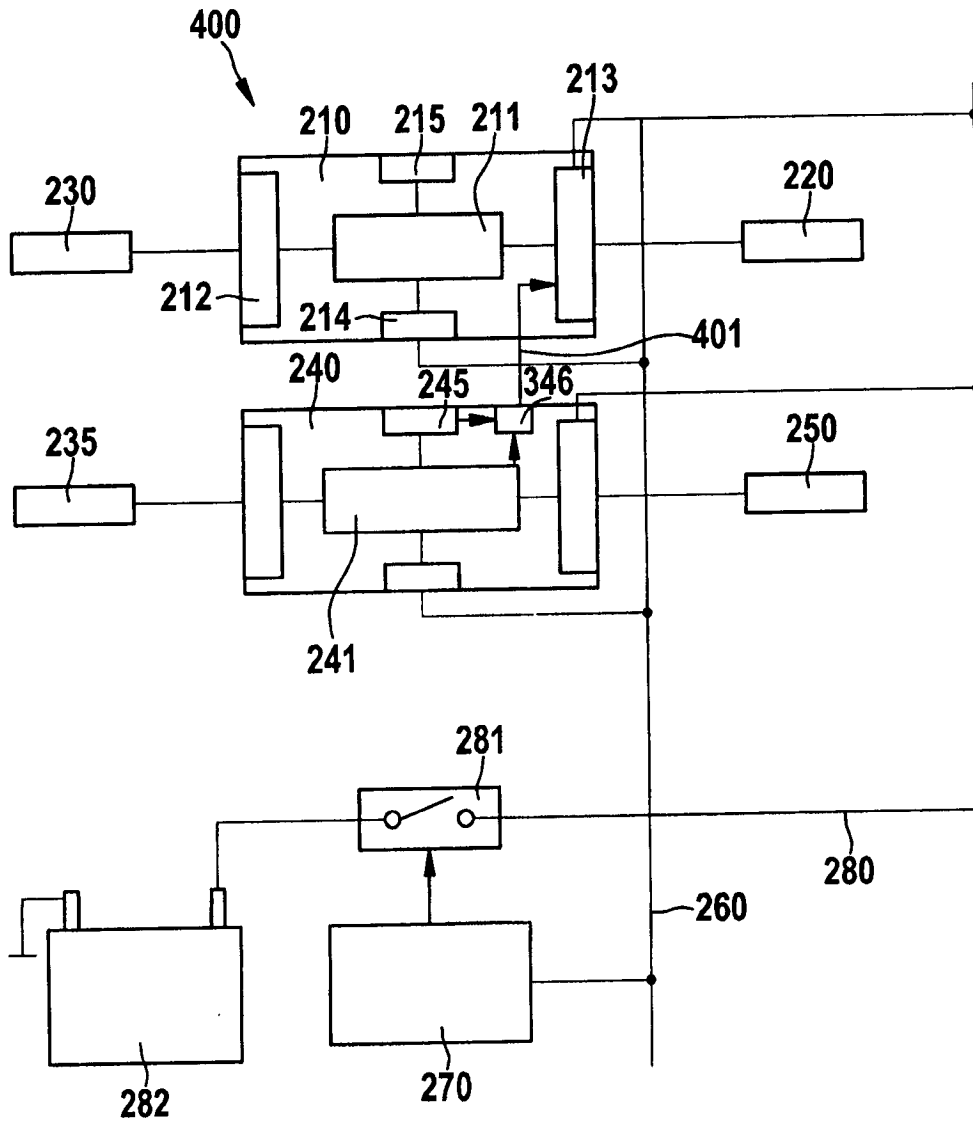


图 4