(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102739639 B
(45)授权公告日 2016.03.16

(21)申请号 201210097036.7
(22)申请日 2012.04.01
(30)优先权数据
102011006668.3 2011.04.01 DE
(73)专利权人 西门子公司
地址 德国慕尼黑
(72)发明人 安德烈亚斯·克普克
(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 张春水 田军锋
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/10(2006.01)
(56)对比文件
US 2010165878 A1,2010.07.01,
CN 1559133 A,2004.12.29,
CN 101375272 A,2009.02.25,
CN 101662428 A,2010.03.03,
审查员 岳晋

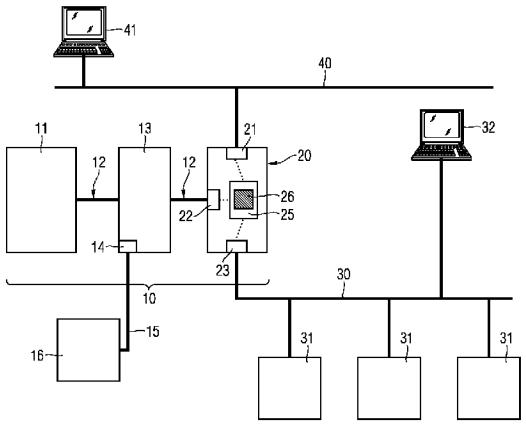
权利要求书2页 说明书6页 附图1页

(54)发明名称

用于模块化控制设备的接口模块

(57)摘要

本发明涉及一种用于模块化控制设备的接口模块，其中接口模块包括：背板总线接口，用于与模块化控制设备的背板总线连接以在模块化控制设备内进行通信，第一通信接口，用于连接到第一通信网络上，安全装置，用于监控在第一通信接口和背板总线接口之间的第一通信，其中接口模块还包括：第二通信接口，用于与设置用于和模块化控制设备进行通信的控制单元进行通信，并且其中安全装置进一步设立和构成用于监控在第二通信接口和背板总线接口之间的第二通信，和/或用于监控在第一通信接口和第二通信接口之间的第三通信。



CN 102739639 B

1. 用于模块化控制设备 (10) 的接口模块 (20)，所述接口模块 (20) 包括：

- 背板总线接口 (22)，用于与所述模块化控制设备 (10) 的背板总线 (12) 连接，以在所述模块化控制设备 (10) 之内进行通信，

- 第一通信接口 (21)，用于连接到第一通信网络 (40) 上，和

- 安全装置 (26)，用于监控在所述第一通信接口 (21) 和所述背板总线接口 (22) 之间的第一通信，

- 第二通信接口 (23)，用于与设置用于和所述模块化控制设备 (10) 通信的控制单元 (31) 进行通信，

其中，所述安全装置 (26) 还设立和构成为

- 用于监控在所述第二通信接口 (23) 和所述背板总线接口 (22) 之间的第二通信，和 / 或

- 用于监控在所述第一通信接口 (21) 和所述第二通信接口 (23) 之间的第三通信，

其特征在于，

所述接口模块 (20) 包括存储装置并且还设立和构成为，

- 使得能够与用于监控所述第二通信的第二规则无关地确定用于监控所述第一通信的第一规则，和

- 使得能够与用于监控所述第三通信的第三规则无关地确定用于监控所述第一通信的所述第一规则，和

- 使得能够与用于监控所述第三通信的所述第三规则无关地确定用于监控所述第二通信的所述第二规则，以及

- 使得所述第二通信接口 (23) 构成并设立用于连接到 HART 网、Profibus 网络上或者连接到 Profinet 网络上，

其中，所述第一规则和所述第二规则存储在所述存储装置中。

2. 根据权利要求 1 所述的接口模块，其特征在于，所述第一规则、第二规则和第三规则中的至少一个规则取决于所述模块化控制设备 (10) 的与所述背板总线 (12) 连接的 CPU(11)、IO 模块 (13) 和通信模块 (20)。

3. 根据权利要求 1 或 2 所述的接口模块，其特征在于，所述第一规则、第二规则和第三规则中的至少一个规则取决于在所述第一通信接口 (21) 和所述背板总线接口 (22) 之间或者在所述第一通信接口 (21) 和所述第二通信接口 (23) 之间是否存在通信。

4. 根据权利要求 1 或 2 所述的接口模块，其特征在于，所述第一规则、第二规则和第三规则中的至少一个规则取决于在所述第一通信接口 (21) 和所述背板总线接口 (22) 之间或者在所述第二通信接口 (23) 和所述背板总线接口 (22) 之间是否存在通信。

5. 根据权利要求 1 或 2 所述的接口模块，其特征在于，所述第一规则、第二规则和第三规则中的至少一个规则取决于在所述第二通信接口 (23) 和所述背板总线接口 (22) 之间或者在所述第一通信接口 (21) 和所述第二通信接口 (23) 之间是否存在通信。

6. 根据权利要求 1 或 2 所述的接口模块，其特征在于，所述接口模块 (20) 设立并且构成用于引入到所述模块化控制设备 (10) 的模块插槽中和 / 或用于安装在所述模块化控制设备 (10) 的装配轨道上，

其中在接口模块 (20) 引入所述模块化控制设备 (10) 中或者安装在所述模块化控制

设备 (10) 上时，所述接口模块 (20) 的所述背板总线接口 (22) 自动与所述模块化控制设备 (10) 的所述背板总线 (12) 连接。

用于模块化控制设备的接口模块

技术领域

[0001] 本发明涉及一种用于模块化控制设备的接口模块，具有

[0002] • 背板总线接口，用于与模块化控制设备的背板总线连接，以在模块化控制设备之内进行通信，

[0003] • 第一通信接口，用于连接第一通信网络，和

[0004] • 安全装置，用于监控在第一通信接口和背板总线接口之间的第一通信。

背景技术

[0005] 例如从美国专利申请US 7,853,677 B2中已知用于模块化控制设备的这种接口模块。在此，公开了用于耦合到化控制单元 (PLC) 的背板总线上的模块化的PLC的安全模块或者相应的网络模块，所述安全模块或者相应的网络模块包括所谓的“防火墙”，借助所述防火墙能够监控外部计算设备与PLC的通信。然而，至今还常通过例如具有自身的通信能力或者结合到较小或较大的通信－自动化网络中的PLC来控制设备。然而，在这种系统和/或具有外部网路部件或者设备的这种系统之内的多种通信可能性例如仅能借助所述接口模块和/或安全模块相对不灵活和/或不充分地来保护。

发明内容

[0006] 因此，本发明的目的是，更灵活地和/或更好地保护在控制系统之内的或者到外部设备的通信。

[0007] 本发明的目的通过一种用于模块化控制设备的接口模块来实现，所述接口模块包括：第二通信接口，用于与设置用于和模块化控制设备通信的控制单元进行通信，并且其中安全装置进一步设立和构成为用于监控在第二通信接口和背板总线接口之间的第二通信，和/或，用于监控在第一通信接口和第二通信接口之间的第三通信。

[0008] 这种接口模块包括

[0009] • 背板总线接口，用于与模块化控制设备的背板总线连接，以在模块化控制设备之内进行通信，

[0010] • 第一通信接口，用于连接到第一通信网络上，和

[0011] • 安全装置，用于监控在第一通信接口和背板总线接口之间的第一通信。

[0012] 接口模块还包括第二通信接口，用于与设置用于和模块化控制设备进行通信的控制单元进行通信，其中安全装置此外设立和构成为用于监控在第二通信接口和背板总线接口之间的第二通信，和/或用于监控在第一和第二通信接口之间的第三通信。

[0013] 这种接口模块例如能够除了监控与具有模块化控制设备的、例如连接到第一通信网络上的计算机通信之外还监控在例如该计算机和用于模块化控制设备的控制单元之间的通信，所述控制单元与在接口模块上的第二通信接口连接。替选地，代替于此，例如还能够监控模块化控制设备与所述的控制单元进行的通信。此外能够监控全部上面所述的三个通信可能性。

[0014] 以这种方式能够灵活地控制并监控在所述网络之内非常不同的通信路径，并且因此更灵活地对所涉及的设备的要求和通信可能性做出反应。

[0015] 模块化控制设备例如能够为用于控制和调节设备、机器、仪器等的控制设备，所述控制设备具有下述可能性：容纳一个或多个附加模块或者功能模块以便建立或者扩展控制设备的功能性。这种功能模块例如能够是用于这种模块化控制的输入输出模块、电源模块、通信模块或者以及中央控制模块(CPU)。在此，待控制的设备或者仪器例如能够与输入输出模块、接口模块或者以及中央控制模块连接。此外，中央控制模块例如还能够是模块化控制设备的固定的组成部分。例如，用于这种模块化控制设备或系统的有例如西门子公司的所谓 S7- 控制器或者如罗克韦尔公司、三菱公司、横河公司、施耐德电气公司或类似公司的相应类似的模块化控制系统。

[0016] 此外，接口模块例如能够具有微处理器，尤其是多核微处理器和 / 或实时操作系统。以这种方式，接口模块例如能够满足提高的要求，所述要求通过在接口模块中的安全装置根据上面的描述而对于接口模块的运算能力或者数据处理特性来提出。

[0017] 背板总线能够是任何适于在模块化控制设备之内进行通信的串行和 / 或并行总线。特别地，背板总线设立并且构成用于在模块化控制设备的各个模块之间进行通信和 / 或一个或多个这种模块与中央模块化控制设备进行通信。在此，模块化控制设备的模块尤其能够可拆卸地固定在控制设备上，其中在固定的模块的情况下所述模块为了通信而通过背板总线进行与所述控制设备连接。特别地，背板总线构成和设立用于模块化控制设备的模块与模块化控制设备的中央控制模块 (CPU) 进行通信。此外，背板总线例如能够实现通过背板总线进行的实时通信。这种背板总线系统的示例为下述背板总线，其在西门子公司的模块化 S7 控制器中使用或者在例如施耐德电气、罗克韦尔、三菱、横河、Vipa 等公司的类似的模块化控制器中使用。

[0018] 接口模块的背板总线接口例如能够构成并设立用于与模块化控制设备的中央控制模块 (CPU) 和 / 或还与模块化控制设备的其他模块进行通信。特别地，背板总线接口例如能够包括用于与背板总线的相应的配对连接元件连接的连接元件。

[0019] 接口模块例如能够可拆卸地与模块化控制设备的背板总线连接。模块化控制设备的其他模块还能够可拆卸地与模块化控制设备连接。特别地，模块化控制设备的模块能够可拆卸地与背板总线连接或者是可连接的。

[0020] 第一通信接口例如能够构成并且设立为用于与线缆连接的或者无线的通信网络连接的接口。特别地，为此通信接口能够包括相应的连接元件或者插接连接元件或者也包括用于无线网络的天线等。通信接口例如能够构成并设立用于与以太网网络或者相应的所谓“办公网络”连接。这种网络例如能够构成并设立为所谓的“局域网 (LAN)”或者“广域网 (WAN)”或者因特网，或者连接到这种网络上。

[0021] 通过第一通信网络例如能够将例如为计算设备、PC、计算机、通信发射设备、移动通信设备等的外部通信装置与接口模块连接并且然后进一步与模块化控制设备连接。

[0022] 在当前的描述中，通信的监控在根据一个或多个预设的或可预设的规则的范围中表示为至少一个通信元件的检测。在此，然后例如能够根据这种规则来决定，根据规则是否必须阻止或者能够转发所检测的通信元件、通信信息和 / 或通信数据。

[0023] 例如，在这种监控的范围中，能够检测对于在这种通信的范围中的待传输的有用

数据的许可性和/或不允许性的检测（例如与所谓的“应用层防火墙”的功能性相比）。此外，例如能够在这种监控的范围中还检测地址和/或发送器（例如在不同的所谓OSI（开放系统互联）层上）。

[0024] 此外，还能够根据最高的所包含的OSI层（根据所谓的“OSI”层模型）来进行检测。在此，例如能够预设规则，即层2通信是允许的，但是包含层3或者更高的通信层的通信是不允许的。此外，能够进行对于确定使用的通信协议的检验。

[0025] 此外，检验还能够包括关于确定的发射和/或接收地址的许可性或者以及作为发送人和/或接收人的确定的用户的许可性的规则。在此，通信的监控或者安全装置例如还能够包括用户的授权。

[0026] 在当前的描述中通常提起在第一和第二接口之间的通信，因此其即理解为第一到第二接口的通信，还理解为第二到第一接口的通信，也还理解为能够在其中出现两个通信方向的通信。

[0027] 第二通信接口例如能够同样构成并且设立用于连接不同的无线网络和有线网络。特别地，第二通信接口能够构成和设立用于与为工业应用而设置并设立的有线连接网络和无线网络连接。因此，第二通信接口例如能够构成并设立用于连接到以太网、工业以太网、WLAN、工业WLAN、HART网（高速可寻址远程传感器）、无线HART网上和/或连接到现场总线系统上，例如Profinet网络、Profibus网络或者类似的网络。

[0028] 设置用于与模块化控制设备进行通信的控制单元例如能够构成并且设立用于接收、处理、转换和/或用于转发模块化控制设备的控制信号。这种控制单元例如还能够设立并且构成用于操纵模块化控制设备和/或用于显示模块化控制设备的数据。

[0029] 设置用于与模块化控制设备通信的控制单元例如还能够为由模块化控制系统所控制的不同的仪器、机器或设备或者相应的机器部分或元件、仪器部分或元件或者设备部分或元件。此外，这种控制单元例如还能够是控制系统的外界供应的或者远距离存在的部分（例如所谓的“分散式外围设备”）。控制单元还能够构成并设立为用于模块化控制系统的操控元件和/或显示元件或者设备（例如特殊的操控和/或显示设备或者以及相应的PC或计算设备）。

[0030] 多个控制单元例如能够通过通信网络，例如上述的工业的有线网络、无线网络和/或现场总线网络连接成所谓的“自动化网络”，所述自动化网络因此例如能够经由第二通信接口与接口模块耦合。

[0031] 与控制单元进行的通信例如能够包括将数据发送到控制单元上，从控制单元接收数据或者以及以两个方向进行通信。在此，一个或多个控制单元能够与第二通信接口连接或者是可连接的，例如通过之前阐明的所构成的“自动化网络”来连接。

[0032] 第二通信的监控例如能够包括通信数据的监控，所述通信数据应该从第二通信网络接口传输到背板总线接口或者反之亦然，或者也以两个方向进行。相应地，第三通信的监控能够包括通信数据，所述通信数据应该从第一通信接口发送到第二通信接口上或者反之亦然，或者也以两个方向进行。

[0033] 在优选的扩展方案中，接口模块能够包括存储装置。特别地，存储装置设置用于存贮用于监控第一、第二和/或第三通信的规则和/或用于检测经过接口模块进行的任意通信的规则。

[0034] 此外能够提出，与用于监控第二通信的第二规则无关地确定或可确定用于监控第一通信的第一规则。此外，还与用于监控第三通信的第三规则无关地确定或可确定用于监控第一通信的第一规则。同样地，还与用于监控第三通信的第三规则无关地确定或可确定用于监控第二通信的第二规则。第一规则、第二规则还和第三规则能够分别彼此无关地来确定。

[0035] 以该方式例如能够实现，例如在第一步骤中检验安全装置，所述第一步骤将当前进行的和待检验的通信与通信的所述三种类型相关联。于是，然后继续使用特别设置用于该类型的通信的规则，以便检验是否应阻止或者转发相应的通信。因此，对于不同的通信路径能够分别确定不同的控制规则和不同的许可性，由此提高在这种联网的自动化系统之内的通信的灵活性。

[0036] 因此，特别的控制法则例如能够用于在模块化控制设备和因此进行通信的控制单元之间的通信，所述控制法则通过模块化控制设备确保相应的控制单元和可能的操控单元的可靠的控制。此外，能够与其无关地调整在外部运算设备和模块化控制设备之间的通信，使得尤其良好地保护模块化控制设备的访问，使其不受未授权的改动或者侵入。第三，通过另一控制法则例如还能够直接地借助控制单元，例如在与网络模块连接的自动化网络中对外部的运算设备的通信再次进行其他的监管，以便例如从控制单元中仅读取一次数据，但是更深地进入到该控制单元（例如接管该单元的控制）是不允许的。

[0037] 此外，为了监控通过接口模块进行的通信能够设置至少一个规则，所述规则取决于与作为发送者或者接收者的模块化控制设备的、与背板总线连接的单元。与背板总线连接的这种单元例如能够是模块化控制设备的其他的模块，例如输入输出组件或者电源模块，或者以及模块化控制设备的中央控制模块。以这种方式，例如能够根据是否应该直接地与控制中央单元，或者例如与输入输出组件进行确定的通信来设置监控规则，对于与所述控制 - 中央单元的通信必须例如设置极其高的安全标准。

[0038] 此外，为了监控通过接口模块进行的通信能够设置至少一个规则，所述规则取决于是否在第一通信接口和背板总线接口之间或者在第一和第二通信接口之间存在通信。因此，与此相关地例如能够检测，例如是否应该进行从外部设备经过第一通信接口到模块化控制单元自身的访问，或者是否应该直接地访问控制单元，例如通过连接在第二通信接口上的自动化网络来访问。在外部运算设备之间经过第一通信接口的通信例如能够根据用户的授权在确定的前提下许可到控制系统中的侵入（例如在设立控制系统时），但是在这种外部的运算设备和在自动化网络中的控制设备之间的通信例如限制于这种控制设备上的网络服务器的只读。

[0039] 此外，在接口模块中还能够设置至少一个规则，所述规则取决于在第一通信接口和背板总线接口之间或在第二通信接口和背板总线接口之间是否存在通信。因此能够为连接在第一通信接口上的运算设备与模块化控制器的以及待控制的系统或操控单元的通信设置不同的规则。因此，例如能够将在模块化控制设备和待控制的单元（或者相应地操控单元）之间的通信限制于现场总线协议、确定的现场总线协议（例如 Profinet 或者 Profibus）或者也限制于“层 2”通信，而例如在模块化控制设备与外部的装置（例如在外部网络中的 PC）通过第一通信接口进行通信时正好不许可这种协议。

[0040] 还能够提出，接口模块包括至少一个规则，所述规则取决于在第二通信接口和背

板总线接口或者在第一和第二通信接口之间是否存在通信。在此，还能够区分上面已经提出的通信可能性。因此，模块化控制设备的通信例如能够借助使相应的控制单元再次限制于现场总线通信或者类似的通信，而与第一通信接口连接的运算设备直接与控制单元的通信例如能够限制于控制单元的网络服务器的只读或者至少限制于 HTTP 协议和 / 或 TCP/IP 协议。

[0041] 如上所述，还能够设置上述控制可能性的组合。因此，例如能够设置至少一个规则，所述规则取决于是否存在第一、第二或第三通信。

[0042] 此外，还能够设置下述规则，所述规则不取决于是否存在第一、第二或第三通信（例如，通用授权或者用户检验、检查病毒和 / 或恶意软件、阻止确定的发送地址和 / 或接收地址）。

[0043] 在另一构成可能性中，接口模块能够设立并且构成用于引入到模块化控制设备的模块插槽中和 / 或用于安装在模块化控制设备的装配轨道上。此外，能够提出，在模块化控制设备中引入的或者安装在其上的接口模块中，接口模块的背板总线接口与模块化控制设备的背板总线连接。特别地能够提出，在引入过程或者安装过程的范围中，自动地建立在接口模块的背板总线接口和模块化控制设备的背板总线之间的接触。以该方式可以特别简单地将接口模块安装在模块化控制设备上，因为由此可以无需与机械安装独立地建立与背板总线的电连接。

[0044] 本发明中给出其他优选的构成可能性。

附图说明

[0045] 下面，示例性地通过参考附图详细阐明本发明。

具体实施方式

[0046] 图 1 示出模块化的存储器可编程控制器 10(SPS)，其中包括中央控制单元 (CPU)11、输入输出模块 13 和通信安全模块 20，所述模块又通过背板总线 12 彼此连接以进行通信。在此，SPS 10 由具有背板总线 12 以及相应的用于接触背板总线 12 的插接联接器的基本单元组成。于是，在该基本单元上装配构成为模块的 CPU 11、I/O 模块 13 以及通信模块 20，其中在装配时，模块的相应的插接联接器与基本单元的用于背板总线 12 的插接联接器连接，并且因此 CPU 11、IO- 模块 13 以及通信模块通过背板总线 12 连接。

[0047] IO 模块 13 具有现场总线端口 14，通过所述现场总线端口经由现场总线线缆 15（例如 Profinnet 线缆）连接传感器 16 或者执行器 16，所述传感器或者执行器还能够通过在 CPU 11 上运行的控制程序来控制或者读取。此外，通过通信模块 20 的现场总线 23 和构成为现场总线网络（例如 Profinet）的自动化网络 30 将不同的控制单元 31 以及监控 PC 32 与 SPS10 连接。控制单元 31 例如能够构成并且设立为待控制的机器或者设备、人机接口（例如为所谓的“human machine interface（人机接口）”(HMI)）、用于 SPS 10 的分散式附加控制单元（例如所谓的“分散式外围设备”）等。通过监控 PC 32 或者构成为 HMI 的控制单元 31 例如能够读取或者改变 SPS 10 当前的状态，或者读取并显示或还改变设备或者机器数据。

[0048] 此外，通信安全模块 20 具有用于以太网网络 40 的外部网络端口 21，通过所述以太

网网络将 PC 41 与 SPS 10 连接。在此，以太网网络 40 被极度地扩展或者以及例如包括因特网。以这种方式，距与 SPS10 非常远地存在的 PC41 通过外部网络 40 访问 SPS 10，以便例如读取或者改变中央控制单元的数据，或者还以便能够例如在设立 SPS 10 时介入到控制程序的程序运行中。此外，通过 PC 41 还能够直接从连接在现场总线网络 23 上的控制单元 31 读取数据。当在控制单元上设置例如自己的网络服务器或者类似的通信元件时，这种数据例如能够是各个控制单元 31 的网页或者其他数据的读取物。

[0049] 为了在通信模块 20 中展开通信，在其中包含通信控制器 25，所述通信控制器此外具有安全装置 26 或者“防火墙”26。

[0050] 通过防火墙 26 将每个经过通信模块 20 的通信进行检测。如果所述通信不满足包含在防火墙中的规则，该通信将被阻止。否则许可该通信并且让相应的信息通过。在此，用于在外部的 PC 41 和 SPS 10 的 CPU11 之间的通信的防火墙规则能够与用于 CPU 11 与控制单元 31 的通信的规则区分。因此，例如能够在 CPU 11 和控制单元 31 之间仅许可一个所谓的“层 2”通信或者以及现场总线通信，所述通信足以确保连接到 SPS 10 上的系统 31 的控制。相反地，能够为在外部 PC 41 和 SPS 10 之间的通信设置用户的授权并且此外，例如排除层 2 通信，以便能够阻止 PC 41 的外部用户侵入到 SPS 10 的控制运行中。此外，外部 PC41 与控制单元 31，例如具有自身网络服务器的机器 31 的通信能够限制于 TCP/IP 通信或者 HTTP 协议。以这种方式，在这种通信的范围中，也不能够介入到在 SPS 10 和所连接的控制单元 16、31 之间的控制机制中，所述控制机制典型地在更深的协议层中来进行。

[0051] 通过通信安全模块 20 的该构型和可能取决于通信路径的防火墙规则，可能的是，将经受可能的外部损害源的外部网络 40 与包含 SPS 10 和自动化网络 30 的自动化系统分离，使得位于外部网络中的用户完全地得到对于其必需的、对 SPS 10 以及连接在该 SPS 上的控制单元 31、16 的访问，并且仍然遵守必要的安全准则。然而，尽管如此，仍由于相应匹配的防火墙规则而尽可能少地阻止在自动化系统之内的通信。

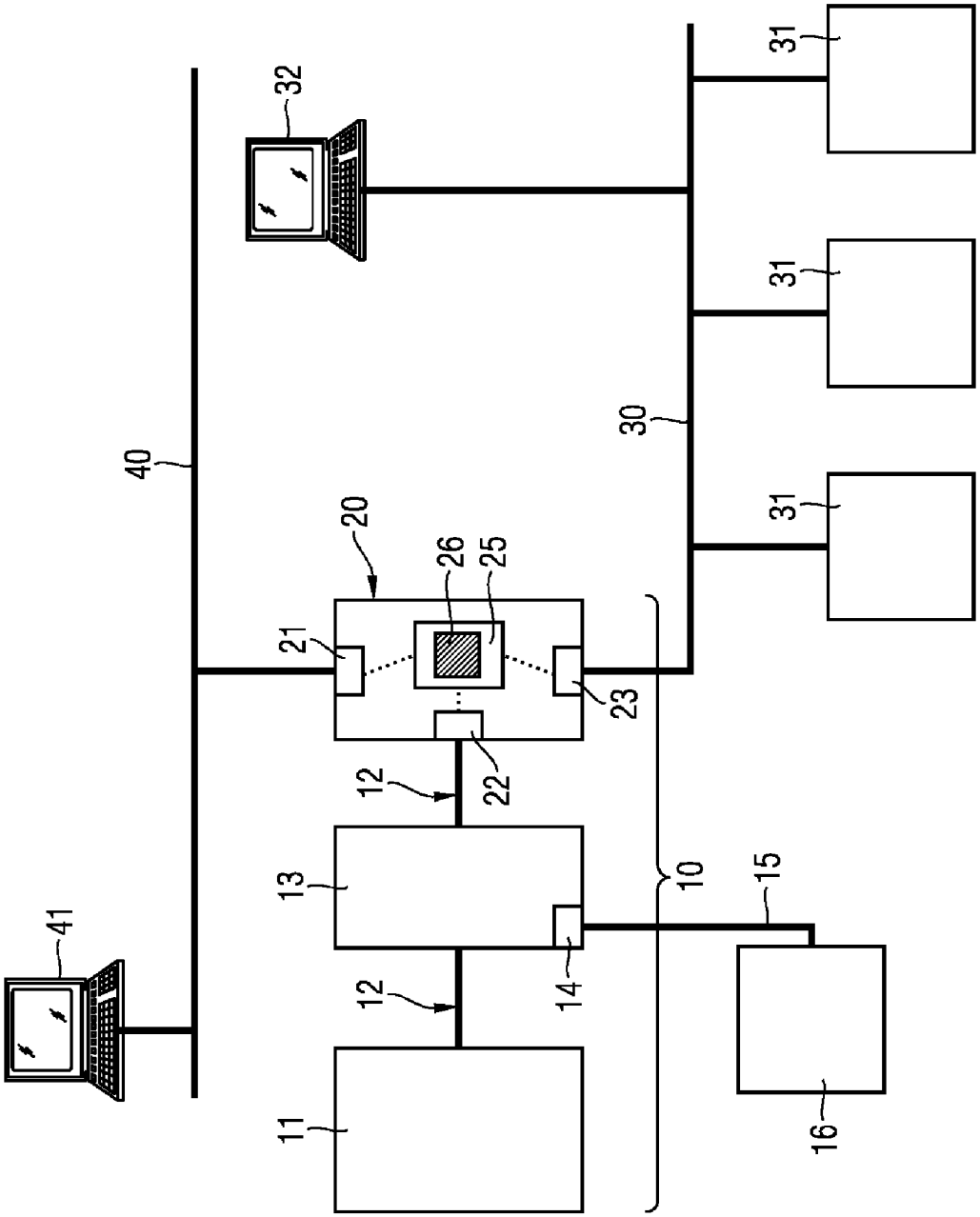


图 1