(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111108451 B
(45)授权公告日 2024.03.26

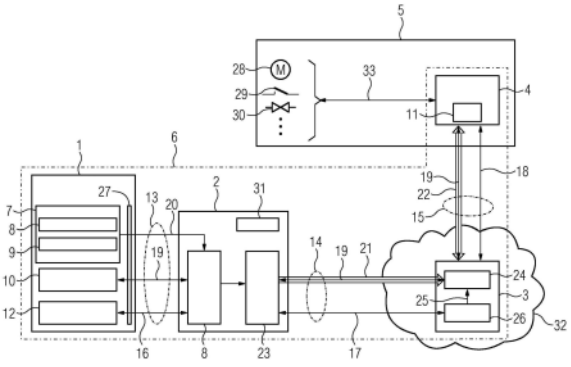
(21)申请号 201880061499.3
(22)申请日 2018.09.21
(65)同一申请的已公布的文献号
申请公布号 CN 111108451 A
(43)申请公布日 2020.05.05
(30)优先权数据
17192679.3 2017.09.22 EP
(85)PCT国际申请进入国家阶段日
2020.03.20
(86)PCT国际申请的申请数据
PCT/EP2018/075569 2018.09.21
(87)PCT国际申请的公布数据
WO2019/057873 DE 2019.03.28
(73)专利权人 西门子股份公司
地址 德国慕尼黑
(72)发明人 勒内·埃姆勒 约尔格·奈迪格
(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
专利代理师 陈方鸣
(51)Int.Cl.
G05B 19/042(2006.01)
(56)对比文件
US 2017025040 A1,2017.01.26
US 2016179993 A1,2016.06.23
US 2016182309 A1,2016.06.23
CN 103957228 A,2014.07.30
CN 105531635 A,2016.04.27
CN 105278398 A,2016.01.27
CN 102749885 A,2012.10.24
DE 102015221652 A1,2017.05.04
DE 102004006509 A1,2005.09.01
DE 102015221650 A1,2017.05.04
审查员 杨幸
权利要求书1页 说明书7页 附图1页

(54)发明名称

工业控制系统

(57)摘要

本发明涉及用于运行工业控制系统(6)的方法和工业控制系统,其中,工业控制系统(6)具有工程化设备(1),其中,所述工程化设备(1)具有存储器(7)和用户接口(10),其中,工程化设备(1)的用户接口(10)代表工业控制系统(6)的操作设备(4)的用户接口(11),其中,工程化设备(1)能够经由编程设备(2)与云设备(3)连接,其中,工程化设备(1)具有安全密钥(12),并且项目数据(9)能够被存储,其中,使用工程化设备(1)和编程设备(2)进行编程。



CN 111108451 B

1.一种工业控制系统,包括:

操作设备,所述操作设备具有用户接口并且设置用于接收由云控制系统生成的控制数据;

工程化设备,所述工程化设备包括

安全令牌、存储器和用户接口,所述工程化设备的用户接口实施为显示器并且代表所述操作设备的用户接口,所述工程化设备存储项目数据,

工程化程序,所述工程化程序存储在所述存储器中并且在云中运行,以及许可,所述许可控制配属于所述云中的流程的属性并且具有基于所述安全令牌的存储区域中的共享秘密的链接或基于云供应商的密钥的加密签名;以及

编程设备,所述编程设备具有用于连接所述云的数据链接的网络和将所述编程设备与所述工程化设备连接的数据接口,利用所述密钥或所述安全令牌的所述存储区域中的共享秘密的链接,所述数据接口提供所述工程化设备与所述编程设备之间的安全数据链接,其中,所述工程化设备激活所述云控制系统上的功能以响应经由所述密钥或所述安全令牌的所述存储区域中的共享秘密的链接的认证,并且

其中,为了实现计算结果经由所述云将命令和输出传输到所述工程化设备和所述操作设备。

2.根据权利要求1所述的工业控制系统,其中,所述工业控制系统具有云设备。

3.根据权利要求1或2所述的工业控制系统,其中,所述工程化程序被加载在所述编程设备上并且能够在所述编程设备上被执行。

4.根据权利要求1或2所述的工业控制系统,其中,存储在所述工程化设备上的所述项目数据被传输到所述编程设备上并且能够在所述编程设备上被所述工程化程序使用。

5.一种用于运行工业控制系统的方法,其中,所述工业控制系统具有工程化设备,其中,所述工程化设备具有存储器和用户接口,其中,所述工程化设备的用户接口是显示器并且代表所述工业控制系统的操作设备的用户接口,其中,所述工程化设备能够经由编程设备与云设备连接,其中,所述工程化设备具有安全密钥,并且项目数据能够被存储,其中,使用所述工程化设备和所述编程设备进行编程,其中,工程化程序被设计用于在云中运行,其中,为了实现计算结果将相应的命令和输出经由所述云传输到所述工程化设备和/或所述操作设备,所述方法使用根据权利要求1至4中任一项所述的工业控制系统。

6.根据权利要求5所述的方法,其中,使用云设备。

7.根据权利要求5或6所述的方法,其中,在所述工程化设备与所述编程设备之间建立第一数据连接,并且在所述编程设备与所述云设备之间建立第二数据连接,其中,在所述云设备与操作设备之间建立第三数据连接。

8.根据权利要求5或6所述的方法,其中,将安全密钥从所述工程化设备传输到所述编程设备。

9.根据权利要求5或6所述的方法,其中,借助于所述工程化设备激活所述云设备。

10.根据权利要求5或6所述的方法,其中,工程化程序被存储在所述工程化设备上并且在所述编程设备上被执行。

工业控制系统

技术领域

[0001] 本发明涉及一种工业控制系统。

背景技术

[0002] 工业控制系统例如用于控制和/或调节过程(例如在化学工业、制药工业等中)、设备(例如生产设备、监控设备等)、机器(例如机床、生产机器等)、建筑(建筑自动化)、机器人等。生产机器例如是注塑成型机、拉丝机、压力机、造纸机等。如果工业控制系统用于机床或生产机器或机器人,则工业控制系统也能被称为或实施为数控系统。如果工业控制系统用于生产设备,则工业控制系统也能被称为或实施为可编程逻辑控制器(SPS)。可编程逻辑控制器(通常缩写为SPS)例如还用于控制简单的和复杂的设备,例如用于生产货物。SPS或工业控制系统例如控制和/或调节设备的马达,和/或尤其从描述系统状态的传感器接收数据。工程系统能够用于工业控制系统的编程和参数设置。除了工程系统外,工业控制系统还能具有模拟程序。模拟程序例如用于计算虚拟的传感器系统。

[0003] 工业控制系统尤其位于要执行的任务的位置处。通常还在工业控制系统的使用位置处进行编程和/或参数设置。这种方式不灵活。

发明内容

[0004] 本发明的目的是改善工业控制系统的灵活性。

[0005] 工业控制系统的工程化设备具有存储器和用户接口,其中,工程化设备的用户接口代表工业控制系统的操作设备的用户接口。工程化设备也能被称为工程系统的至少一部分。工程化设备尤其用于工业控制系统的编程和/或参数设置。工程化设备的用户接口尤其是显示器和/或LED(发光二极管)和/或开关或者分别是其中多个。除了工程化设备外,工业控制系统还具有操作设备。在工业控制系统运行时,工程化设备尤其与工业控制系统的操作设备在空间上间隔开。这种间距可能是几米或者几百公里或几千公里。工业控制系统的操作设备位于用于控制和/或调节过程、设备、机器、建筑(建筑自动化)等的应用位置处。工程化设备尤其被设计成由调试员、程序员、机器操作员等使用。操作设备还具有用户接口,操作设备的用户接口例如是显示器和/或LED和/或开关或者分别是其中多个。操作设备的和工程化设备的至少一部分用户接口是相同的。因此,例如工程化设备的用户能够让工程化设备的用户接口处的输出与操作设备的用户接口处的输出相同。因此,工程化设备用作为操作设备的一种代表。操作设备尤其具有用于控制和/或调节的输入接口和/或输出接口。例如能够经由输出接口驱控或调节马达、开关和/或阀门。例如能够经由输入接口接收关于设备的执行器的位置的信息和/或电机、设备和/或传感器的运行数据。

[0006] 工程化设备不用于或不是主要用于控制和/或调节过程、设备、机器、建筑(建筑自动化)等,并且不具有特别为此设置的输入接口和/或输出接口。自动化任务能够全部或部分地转移到云中。通过云,能够由互联网提供信息技术基础设施,例如提供存储空间、计算能力或应用软件。为此,例如能够使用一个计算中心或多个计算中心和/或多个单独的计算

机。通过云计算,尤其由计算机网络提供信息技术基础设施,而不必在本地设有信息技术基础设施。因此,能够以自动化技术使用所谓的云服务或软件即服务。尤其在时间不紧迫的过程(例如建筑自动化)或任务中,调节任务能够转移到云中的计算中心中。其由此转移到云中的装置中,也就是转移到云装置、例如计算中心中。时间不紧迫的任务在这里取决于通信连接(安全的传输速度、安全的带宽等)以及要求(建筑、造纸机、机床、船舶等的自动化)。如果能够在时间和/或数据量方面确保安全的连接,则时间紧迫的任务也能转移至云中。除了偶尔的例外(例如计算中心中的计算过程的迁移和/或网络问题)之外,控制和/或调控的延迟时间可以在两位数的毫秒范围之内。传感器和执行器还在本地存在并且利用合适的网络机制与自动化装置、操作设备连接。

[0007] 为了对这种系统进行编程,考虑使用多种不同方法。一方面,工程软件能够在计算中心中的服务器上执行。对该软件的使用以网络浏览器和/或借助于屏幕共享技术实现,例如基于远程桌面或类似协议。另一方面,工程软件能够在本地安装在开发计算机上,其中全部控制程序和/或各个模块都借助于网络机制转移到云控制系统中。因此,云控制系统尤其是云中的工业控制系统。在此能提出,云控制系统仅作为计算中心中的一个进程存在。在该设计方案中,物理上不存在提供有关云进程的当前状态的反馈的、具有显示器、开关、存储插槽的物理设备,或者该设备仅作为PC(个人电脑)应用程序存在。为此需要互联网连接。如果自动化程序仅被存储在云中并且无法访问该云,则不能进行自动化程序的离线研究或离线开发。如果工业控制系统的程序数据仅位于云中,则在本地安装软件(工程系统、远程桌面软件、VPN(虚拟私人网络)通道等)还能是必要的,尽管云控制系统、即工业控制系统、其功能和计算能力是在云中实现的,原则上在互联网上通常是能获得的。工程系统例如能在本地安装在计算机(例如个人电脑、智能手机、平板电脑等)上和/或云中。在此,例如能在云控制系统(即在云控制装置)上强制性地设置授权系统,该授权系统具有例如登录数据和/或加密信息或由这些内容组成。不需要本地安装应用程序或移动应用程序的解决方案尤其基于Web(网络)并且以浏览器执行。在该解决方案中,自动化程序的源代码(或其逻辑或规则)能被存储在计算中心、即云中,或被传输到其中以进行编译。在这种纯云端解决方案中,在与自动化现场分隔开的本地工程中,在云(例如计算中心)中的虚拟计算过程与具有显示器、开关等的工程现场的本地物理设备之间没有连接。

[0008] 通过使工业控制系统的工程化设备具有至少一个存储器和至少一个用户接口,能够实现远离操作设备所在的自动化现场的、在工程现场的位于壳体内的物理设备,该物理设备尤其包括显示器、开关等等。

[0009] 在工程化设备的一种设计方案中,工程化设备具有用于存储数据的存储器(数据存储器)。通过工程化设备的这种装置,因此为数据和/或文件提供一种存储可能性,其例如能够与安全令牌的功能以及例如是显示器和开关的物理部件结合使用。存储在工程化设备中的安全令牌例如能被传输至在云中实现的工业控制系统(云控制系统),以便在那里例如实现功能。

[0010] 在工程化设备的一种设计方案中,工程化设备具有安全密钥。安全令牌是一种安全密钥。安全令牌功能尤其执行加密算法并且安全地存储密钥资料。如果工程化设备自身具有“安全性”,则不再丢失工程化设备。在纯基于软件的通路中,例如在基于网络的工程系统和/或纯云控制系统中,授权信息(密码、登录名、密钥等)可能被忘记、丢失和/或以欺诈

方式被未察觉地复制或提供给未授权者。如果将授权连接到工程化设备的物理设备上,则能将该问题最小化。带有硬件加密狗的解决方案最适合安全存储密钥资料和许可功能的要求。这些例如实现为芯片卡或USB(通用串行总线)设备并且例如与服务器进行加密通信,以批准访问流程或实现功能。

[0011] 在工程化设备的一种设计方案中,工程化设备具有工程化程序。工程化程序尤其被存储在数据存储器中。在数据存储器中不仅能存储工程软件(即应用程序),还能存储其全部配置。该配置还能包括许可证、项目数据、版本状态、对云基础设施的访问数据和其他信息。

[0012] 在工程化设备的一种设计方案中,工程化设备具有项目数据、例如程序代码。程序代码还能被存储在云中和/或至少传输到云中以进行编译。可以对程序代码进行加密以进行保护。

[0013] 在工程化设备的一种设计方案中,工程化设备具有用于连接编程设备的数据接口。编程设备例如是编程装置、工程PC、具有编程应用程序的智能手机、具有编程应用程序的平板电脑等。编程设备尤其具有用于与互联网并因此与云进行数据连接的网络接口或通信接口。在互联网中或者通过互联网能够访问云。

[0014] 在工程化设备的一种设计方案中,工程化设备具有显示器和/或操作部件并且因此实现自动化设备的显示,但是在工程化设备中创建的程序不在该设备上执行。反而使用云中的计算能力。因此设有云控制系统。云尤其具有计算中心。必要时,在云控制系统中启动执行自动化程序的流程。

[0015] 工业控制系统具有工程化设备。该工程化设备例如是在此描述的类型,或者是实现技术系统的工程的其他类型的工程化设备。该工程涉及具有技术系统的工程技术设施。工业控制系统的工程化设备具有存储器和用户接口,其中,工程化设备的用户接口代表工业控制系统的操作设备的用户接口。“代表”能被理解为例如替换和/或补充和/或复制。替换和/或补充和/或复制在此尤其仅涉及整体的一部分。因此,能够尤其通过“代表”实现工业控制系统的MMI(人机接口)的至少一部分和/或表现图像,人机接口例如是操作设备的用户接口。因此,该表现图像作为用户接口尤其能够具有操作功能和/或输出功能和/或输入功能和/或显示功能。工程化设备和操作设备能被集成在一个装置中,也能是两个独立的单元或装置。

[0016] 在工业控制系统的一个设计方案中,工程化设备能够经由编程设备与云设备连接,其中,工程化设备具有安全密钥,并且项目数据能够被存储。通过安全密钥可以实现安全的数据连接。如果工程化设备具有项目数据,则项目数据由此例如能被存储在本地待控制的设备上。

[0017] 在工业控制系统的一个设计方案中,工程化设备具有工程化程序。该工程化程序可以在云中运行。尤其在云中执行控制和/或调节功能、也就是其计算。为了实现计算结果,尤其将相应的命令和输出经由云传输到工程化设备和/或操作设备。工业控制系统能被设计使得工程化程序和/或例如用于可编程逻辑控制器的程序在云中运行。云在此尤其是通过内联网和/或互联网进行基于在线的存储、服务器和/或计算服务的常用术语。

[0018] 在工业控制系统的一种设计方案中,工程化设备具有用于连接编程设备的数据接口。该数据接口例如与线缆连接或者是基于无线电的。

[0019] 在工业控制系统的一个设计方案中,工业控制系统具有云设备。例如,在云中设有存储器和/或服务器作为云设备。

[0020] 在具有操作设备的工业控制系统的一种设计方案中,操作设备被设计用于接收云设备的控制数据,其中,控制数据借助于云控制系统产生。控制数据在此例如还能包括用于调节的数据。

[0021] 在工业控制系统的一种设计方案中,工程化程序被加载在编程设备上并且还能在该处被执行。这例如实现具有不同版本的工程化程序的实际设施。

[0022] 在工业控制系统的一种设计方案中,存储在工程化设备上的项目数据被传输到编程设备上并且能在该处被工程化程序使用。这使得操作人员可以在现场轻松地操作工业控制系统。

[0023] 工业控制系统还能被设置成使其具有工程化设备(例如如上所述的工程化设备)和编程设备(例如如上所述的编程设备)。工程化设备和编程设备是两个尤其各自具有专用外壳的不同的设备。编程设备尤其具有显示器和键盘、或用于移动光标或鼠标指针的装置。编程设备的显示器也能用作为工程化设备的显示装置。

[0024] 在工业控制系统的一个设计方案中,工业控制系统具有云设备。该云设备例如是尤其能在云中的计算中心中实现的云控制系统。

[0025] 在工业控制系统的一个设计方案中,工业控制系统具有操作设备。工业控制系统的操作设备位于控制和/或调节过程、设备、机器、建筑(建筑自动化)等的应用位置处。操作设备尤其具有I/O(输入/输出)接口。

[0026] 通过工业控制系统的这种设计方案,能够解决安装、安全和/或可视化的问题。这尤其通过使用单独的工程化设备实现。在一个设计方案中,工程作为便携式应用被存储在大容量存储设备中。通过使用USB式大容量存储设备,实现应用程序和/或项目数据的存储。

[0027] 根据用于运行工业控制系统的方法,其中,该工业控制系统具有工程化设备,其中,该工程化设备具有存储器和用户接口,其中,工程化设备的用户接口代表工业控制系统的操作设备的用户接口,其中,工程化设备能够经由编程设备与云设备连接,其中,工程化设备具有安全密钥,并且项目数据能够被存储,将工程化设备和编程设备用于编程。还能以还要说明的方式实施工业控制系统。

[0028] 在用于运行工业控制系统的一种方法或这种方法中,例如使用工程化设备和编程设备进行编程。这使系统既安全又灵活,并且能给用户带来使用工程化设备在本地对工业控制系统进行编程或参数设置的感觉。

[0029] 在该方法的一种设计方案中,使用云设备。该云设备尤其是云控制系统,在其上执行要由工业控制系统执行的计算过程。

[0030] 在该方法的一种设计方案中,在工程化设备与编程设备之间建立第一数据连接,在编程设备与云设备之间建立第二数据连接,其中,尤其在云设备与操作设备之间建立第三数据连接。因此,工程化设备也能与云设备进行通信并且交换数据。这些数据尤其涉及身份验证或在云控制系统上实现功能。因此,通过购买工程化设备能够同时购买软件功能,软件功能被存储在工程化设备中并且由工程化设备在云控制系统上实现。

[0031] 工程化设备能被理解为计算中心中的云过程的物理代表。例如,如果将设备(即工程化设备)与PC(即编程设备)连接,则无需事先安装过程就启动工程系统,该设备的用户因

此能立即工作。所有必要的项目文件由工程化设备加载并且还存储在该处。工作位置变化或将设备交给其他人很容易实现。该设备、即工程化设备代表自动化系统的状态并实现其操作。但是,用于执行系统的计算能力被存储在云中的中央计算机系统、即云设备上。

[0032] 在该方法的一个设计方案中,将安全密钥从工程化设备传输到编程设备。这能通过安全令牌功能实现。工程化设备中的安全令牌功能允许进行安全的授权,并且通过为云设备(例如计算中心)中的授权过程证明设备的身份或存在的方式来表现复制保护和操作安全性。云设备中的云控制过程(必要时)被启动,并且只有在成功完成授权过程后才授予该工程系统访问该过程的权限。利用授权、安全存储和/或身份认证能够将工程化设备个性化,从而使非中心地存储在设备上的许可能够设置云过程的功能和行为。本地工程化设备的许可控制了配属于云中的流程(也就是计算功能)的属性(即资源、功能或保证的服务质量)。

[0033] 在该方法的一种设计方案中,借助于工程化设备激活云设备、尤其是云控制系统。这实现了简单的许可证管理。

[0034] 在该方法的一种设计方案中,工程化程序被存储在工程化设备上并且在编程设备上被执行。工程化设备因此需要很少的计算能力并且能够使用编程设备的计算能力。

[0035] 在该方法的一种设计方案中,使用由能由工程化程序实现的工程系统管理的双向的网络连接,并且该连接因此用于将工程化设备上的操作元件的动作转发至云控制系统、也就是云设备,并且将其状态输出至工程化设备的装置的显示器上。云控制系统和工程系统支持该过程。工程化设备的控制元件能够代表单独的USB设备,或者也能通过装置中的支持进程进行寻址。工程系统为此透明地连接云设备中的授权过程和安全令牌功能。可以使用TOTP(基于时间的一次性密码算法)或非对称加密法(例如RSA(非对称加密算法))作为协议。在这两种情况下,加密资料都存储在令牌的存储区中。该资料从不离开安全令牌,并且因此不能以通常方式复制。能够以相同方式实现服务器的授权。能够使用SSL(加密套接字协议层)方法来实现传输加密。能够在操作系统级(例如通过防火墙技术)或在应用程序级通过授权令牌(例如公开ID(标识))来限制访问。成功的授权表明工程化设备的存在。云控制系统的需要的属性例如被存储在许可证文件中,该文件被存储在工程化设备的存储区内。例如通过使用云供应商的密钥材料进行加密签名,或者通过绑定在安全令牌的存储区域中(HMAC(基于哈希的消息授权代码))的秘密(共享秘密),实现许可证文件的完整性。

[0036] 基于Web的或便携式的工程系统、和/或基于加密狗的授权、和/或用于输出状态和/或用于连接至少一个控制元件的硬件也可以用于工业控制。

附图说明

[0037] 下面根据附图示例性地详尽阐述本发明。

[0038] 图1是工业控制系统的示意图。

具体实施方式

[0039] 图1示出了工程化设备1。也能被称为用于工程的虚拟工业控制系统6的工程化设备1具有存储器7、用户接口10和安全密钥12。存储器7具有工程化程序8和另外的数据9。工程化程序8尤其能在编程设备2上运行,该编程设备也能被称为工程PC。另外的数据9例如包

括项目数据、源数据、许可证数据、密钥数据等。用户接口10具有例如显示器、开关、LED等。工程化设备具有安全密钥12,该安全密钥能被安全地传输到编程设备2。工程化设备1具有数据接口27。经由该数据接口27实现到编程设备2的第一数据连接13。经由第一数据连接13能够传输安全数据16,例如传输安全密钥12、用户接口数据19和/或存储器数据20。存储器数据20例如是由存储器7加载、读取、写入和/或执行的数据。

[0040] 编程设备2具有可执行的工程化程序8。工程化程序8在编程设备2上执行,该编程设备还具有屏幕31。工程化程序8的数据通过第二数据连接14经由网络接口23被传输至云设备3。云设备3位于云端、即互联网32中。通过第二数据连接14传输用户接口数据19、工程数据21和安全数据17。云设备3具有云控制系统24。通过认证过程26,能够通过认可25启动云控制系统24。第三数据连接15将云设备3与操作设备4连接。第三数据连接15具有工业控制系统的控制数据22、用户接口数据19和安全性数据18。操作设备具有自身的用户接口11。操作设备4集成在设施5中。该设施5具有马达28、开关29、阀门30等。这些元件能够由操作设备4控制和/或调节。为此提供控制数据33。

[0041] 工程化设备1的独立的装置能够将多个原本不相关的方法组合为一个整体。由此得到能为用户例如带来以下优点的对象:

[0042] • 容易使用;

[0043] • 工程化设备1中已包含的、用于工业控制系统的许可证没有问题;

[0044] • 无需安装和配置工程系统,因为工程化程序是能直接由工程系统启动的便携式软件,其中能够已经包含许可证;

[0045] • 自动化设备的类型能被预设或与许可证连接;

[0046] • 云服务无需配置或另外的密码;

[0047] • 通过使用强授权在首次使用时就已经很安全;

[0048] • 能够在很大程度上排除错误配置和错误操作;

[0049] • 为用户提供专用技术保护,因为项目数据在本地存储在工程化设备中;

[0050] • 为用户提供专用技术保护,因为源代码原则上不必存储在云中;

[0051] • 为用户提供专用技术保护,因为只有编译后的控制代码(例如SPS代码)才被传输到云控制系统;

[0052] • 工程化设备1能由便宜的硬件制造,因为其不表现为复杂的工业控制系统,而是仅具有存储器和/或LED式显示器和/或LED的简单设备;

[0053] • 用于控制系统制造商的专用技术保护,因为用户不需要自动化设备的固件、也就是工业控制系统来执行代码;

[0054] • 改善的可扩展性、资源利用和/或控制代码(例如SPS代码)出错时排除故障的可能性,由于计算中心的所有过程都在云中运行;

[0055] • 更安全的许可,因为工程化设备1还作为不可复制的加密狗起作用;

[0056] • 用于怀疑云技术的用户的简单的迁移方案,因为用户不必交出数据和源代码,因为工程化设备1具有“真实”设备(硬件)而不仅仅是云(计算中心)中的软件流程。

[0057] 工程化设备1通过其作为硬件设备的设计方案能够表示数据中心(云)中的虚拟工业控制系统的本地代表。工程化设备能够将控制单元、存储功能和加密狗技术结合在一起,以便能够因此对云控制系统进行编程。能够设计工程化设备,从而不需要安装工程系统或

工程化程序。能够将工程化程序设计为便携式软件,从而能够直接由装置(工程化设备)启动该程序,以便实现在装置上将云控制系统的状态和操作可视化。到云控制系统的更安全且无配置的连接(访问数据、密码、加密密钥等)可以在装置(工程化设备1)上实现。也可以转移或转售工程化设备1,其中不能像软件解决方案那样进行复制。能够将工程化设备1作为硬件设备与云过程连接,其中能够确保工程系统或工程化程序与虚拟工业控制系统(云控制系统)的、更安全且经过双方认证的连接。

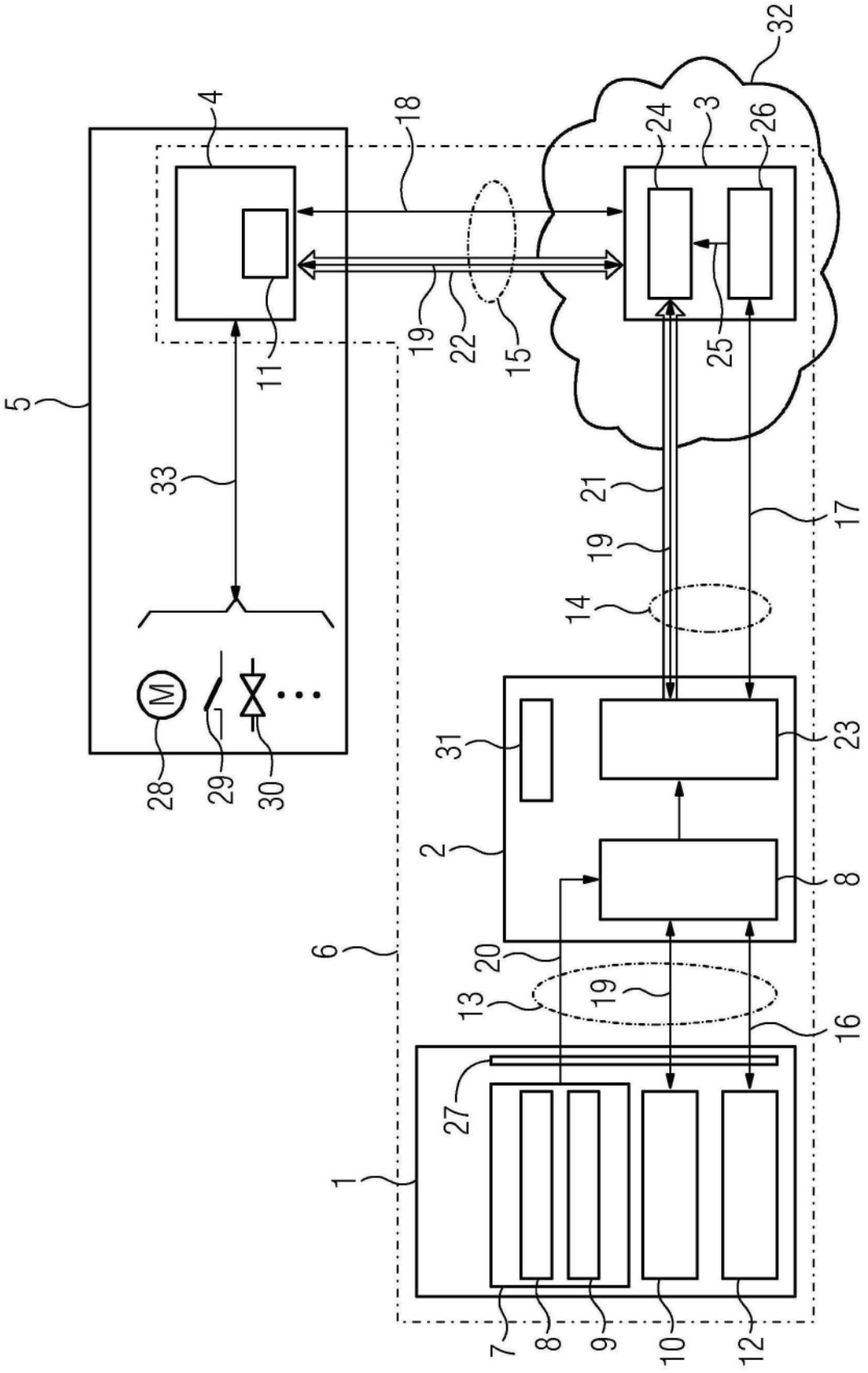

32
4
18
24
3
26
5
11
19
22
15
25
33
21
17
19
14
M
28
29
30
31
23
2
8
6
20
13
19
16
27
1
7
8
9
10
12

图1