



(12)发明专利申请

(10)申请公布号 CN 111669361 A

(43)申请公布日 2020.09.15

(21)申请号 202010157336.4

(22)申请日 2020.03.09

(30)优先权数据

102019106049.4 2019.03.08 DE

(71)申请人 克洛纳测量技术有限公司

地址 德国杜伊斯堡

(72)发明人 W.霍特根罗特

(74)专利代理机构 中国专利代理(香港)有限公司

司 72001

代理人 姬亚东 刘春元

(51)Int.Cl.

H04L 29/06(2006.01)

H04L 29/08(2006.01)

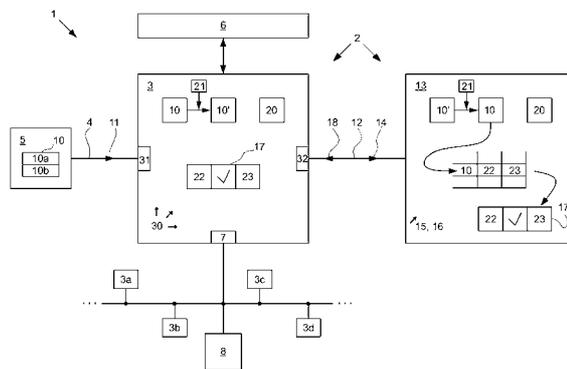
权利要求书3页 说明书8页 附图3页

(54)发明名称

用于在自动化技术的现场设备与终端设备之间的安全通信的方法及系统

(57)摘要

描述了一种用于在自动化技术的现场设备和通过终端设备通信连接与现场设备连接的终端设备之间的安全通信的方法。通过如下方式安全性高地防止借助于终端设备通信接口对现场设备的滥用访问:在终端设备中寄存有单独的访问标志符且终端设备将其访问标志符传输给现场设备;现场设备通过服务器通信连接与认证服务器连接并且现场设备将访问标志符或从访问标志符推导出的访问标志符传输给认证服务器;在认证服务器上寄存有认证数据,在认证服务器上依据认证数据来检查访问标志符的可信度,且所得到的认证结果由认证服务器经由服务器通信连接传输给现场设备;且根据被传输到现场设备的认证结果来使终端设备可支配现场设备的资源。



1. 一种用于在自动化技术的现场设备(2)和通过终端设备通信连接(4)来与现场设备(2)连接的终端设备(5)之间的安全通信的方法(1),其中所述现场设备(3)与物理过程(6)保持有效关联而且所述现场设备(3)能通过现场总线接口(7)来与其它现场设备(3a、3b、3c、3d)和/或过程控制系统(8)连接,用于交换过程信息,

其特征在于,

在所述终端设备(5)中寄存有单独的访问标志符(10)而且所述终端设备(5)将其访问标志符(10)传输(11)给所述现场设备(3);

所述现场设备(3)通过服务器通信连接(12)来与认证服务器(13)连接并且所述现场设备(3)将所述访问标志符(10)或者从所述访问标志符(10)推导出的访问标志符(10')传输(14)给所述认证服务器(13);

在所述认证服务器(13)上寄存有认证数据(15),在所述认证服务器(13)上依据所述认证数据来检查(16)所述访问标志符(10)的可信度,而且所得到的认证结果(17)由所述认证服务器(13)经由所述服务器通信连接(12)传输(18)给所述现场设备(3);而且

根据被传输到所述现场设备(3)上的认证结果(17)来使所述终端设备(5)可支配(19)所述现场设备(3)的资源。

2. 根据权利要求1所述的方法(1),其特征在于,寄存有单独的终端设备名称(10a)和单独的终端设备密码(10b),作为单独的访问标志符(10);和/或所述单独的访问标志符(10)具有与现场设备(2)保持连接的终端设备(5)的用户的单独的用户名(10a)和单独的用户密码(10b)。

3. 根据权利要求1或2所述的方法(1),其特征在于,在所述现场设备(3)中寄存有所述认证服务器(13)的地址(20),而且在使用所述认证服务器(13)的地址(20)的情况下建立所述服务器通信连接(12)。

4. 根据权利要求1至3之一所述的方法(1),其特征在于,在所述现场设备(3)中以及在所述认证服务器(13)中都寄存有加密装置(21),所述加密装置允许所述现场设备(3)和所述认证服务器(13)经加密地彼此交换数据;所述现场设备(3)用它的加密装置(21)从所述访问标志符(10)推导出经加密的所推导出的访问标志符(10')并且将其传输(14)给所述认证服务器(13);而且所述认证服务器(13)用它的加密装置(21)将经加密的所推导出的访问标志符(10')解密成所述访问标志符(10)。

5. 根据权利要求1至4之一所述的方法(1),其特征在于,所述认证服务器(13)的认证数据(15)也包括与访问标志符(10)相关联的权限范围(22),而且由所述认证服务器(13)传送给所述现场设备(3)的认证结果(17)也包括分配给访问标志符(10)的权限范围(22)。

6. 根据权利要求5所述的方法(1),其特征在于,权限范围(22)是如下权限范围(22)之一:只读访问、受限制的读访问、写访问、受限制的写访问、功能性调用,尤其是其中所述权限范围配备有参数列表和/或功能列表。

7. 根据权利要求5或6所述的方法(1),其特征在于,所述权限范围(22)表示子权限组,其中对所述子权限组的定义或者存放在所述现场设备(3)上或者存放在所述认证服务器(13)上而且在调用时被传输到所述现场设备(3)上,尤其是其中可能的子权限组是:用户、操作员、专家、服务、工厂。

8. 根据权利要求1至7之一所述的方法(1),其特征在于,所述认证服务器(13)的认证数

据(15)也包括与访问标志符(10)相关联的会话属性(23),并且由所述认证服务器(13)传送给所述现场设备(3)的认证结果(17)也包括分配给访问标志符(10)的会话属性(23),尤其是其中会话属性(23)可以是:会话语言、会话时长、绝对会话时间、会话访问的数目、会话接口。

9.根据权利要求5至8之一所述的方法(1),其特征在于,所述现场设备(3)向所述终端设备(5)提供个性化操作界面,而且依据所述权限范围(22)和/或所述会话属性(23)来实现对操作界面的个性化,尤其是其中所述现场设备(3)通过个性化网络服务器向所述终端设备(5)提供个性化操作界面,或者所述现场设备(3)使所述现场设备(3)本身的物理显示装置的操作界面个性化。

10.根据权利要求1至9之一所述的方法(1),其特征在于,所述现场设备(3)将与所述终端设备(5)的通信至少部分地记录(26)在报告(27)中,尤其是其中在通信结束时所述报告(27)被传送(28)给所述认证服务器(13)并且所述报告(27)被存储在所述认证服务器(13)上,或者其中备选地,所述报告(27)在所述通信期间不断地被传送(28)给所述认证服务器(13)并且所述报告(27)被存储在所述认证服务器(13)上。

11.根据权利要求1至10之一所述的方法(1),其特征在于,所述终端设备通信连接(11)和/或所述服务器通信连接(12)按照如下技术之一来构造:蓝牙、无线局域网(WLAN)、红外(IR)、以太网。

12.一种用于在自动化技术的现场设备(3)与终端设备(5)之间的安全通信的系统(2),所述系统包括所述现场设备(3)和认证服务器(13),其中所述现场设备(3)与物理过程(6)保持有效关联而且所述现场设备(3)能通过现场总线接口(7)来与其它现场设备(3a、3b、3c、3d)和/或过程控制系统(8)连接,其中所述现场设备(3)包括数据处理电子电路(30),其中所述现场设备(3)能通过与所述现场总线接口(7)不同的终端设备通信接口(31)来与所述终端设备(5)连接,而且其中所述现场设备(3)通过服务器通信接口(32)来与所述认证服务器(13)连接,

其中所述数据处理电子电路(30)被设计为使得所述数据处理电子电路能够通过所述终端设备通信接口(31)来接收所连接的终端设备(5)的单独的访问标志符(10),

其中所述数据处理电子电路(30)被设计为使得所述数据处理电子电路通过所述服务器通信接口(32)来将所述访问标志符(10)或者从所述访问标志符(10)推导出的访问标志符(10')传输给所述认证服务器(13),

其中在所述认证服务器(13)上寄存有所认证数据(15),在所述认证服务器(13)上依据所述认证数据来检查(16)所述访问标志符(10)的可信度,

其中所述数据处理电子电路(30)被设计为使得所述数据处理电子电路通过所述服务器通信接口(32)来接收由所述认证服务器(13)确定的认证结果(17),而且

其中所述数据处理电子电路(30)被设计为使得所述数据处理电子电路根据所接收到的认证结果(17)来使所述终端设备(5)可支配(19)所述现场设备(3)的资源。

13.根据权利要求12所述的系统(2),其特征在于,所述现场设备(3)和所述认证服务器(13)被设计为使得它们能够执行根据权利要求1至11中的至少一项权利要求的前序部分的特征的方法(1)。

14.根据权利要求12或13所述的系统(2),其特征在于,所述服务器通信接口(32)、所述

终端设备通信接口(31)以及可能的与所述通信接口(31、32)保持关联的软件服务在所述现场设备(3)上与所述现场总线接口(7)和与所述现场总线接口(7)保持关联的软件服务隔离地来实现,使得尤其是不可能通过所述服务器通信接口(32)、通过所述终端设备通信接口(31)以及通过可能的与所述通信接口(31、32)保持关联的软件服务来影响所述现场总线接口(7)和与所述现场总线接口(7)保持关联的软件服务。

用于在自动化技术的现场设备与终端设备之间的安全通信的方法及系统

技术领域

[0001] 本发明涉及一种用于在自动化技术的现场设备和通过终端设备通信连接来与该现场设备连接的终端设备之间的安全通信的方法,其中该现场设备与物理过程保持有效关联而且该现场设备能通过现场总线接口来与其它现场设备和/或过程控制系统连接,用于交换过程信息。此外,本发明也涉及一种用于在自动化技术的现场设备与终端设备之间的安全通信的系统。

背景技术

[0002] 自几十年以来,自动化技术的现场设备被用于测量值检测(传感装置)并且被用于操控在物理技术过程中的调节环节(执行装置);如果这些现场设备与物理过程保持有效关联,这就是其所意指的。在传感器式现场设备的情况下,这些现场设备通过它们的传感器在测量技术上检测过程参量,借助于数据处理电子电路来将原始测量数据编辑成所要传送的测量参量并且大多将该测量参量传输给上级过程控制系统。现场设备“在现场”工作,这些现场设备通常设计得非常鲁棒并且更抗干扰,因为这些现场设备受到工业过程的不利影响,这些现场设备部分地在户外使用。因此,通常并不存在“实验室条件”。

[0003] 现场设备使用所提及的现场总线接口来传送测量数据或调定量,该现场总线接口实现了所建立的协议。例如,自几十年来就使用的模拟式4-20mA接口或者数字式HART接口属于所设立的现场总线接口。在这种情况下,双导体装置常常用作物理传输介质,其中可以给电流接口的模拟电流信号调制HART协议的数字信号。这种类型的现场总线接口只实现了比较低的传输率,尽管这些现场总线接口在过程工业中具有及其高的稳定性,因为这些现场总线接口的可靠性被证实并且它们被视为不易受影响。通过现场总线接口常常只能非常有限地影响现场测量设备,因为完全没有规定通过现场总线接口对现场设备的在对测量结果的真正传输或者对调定量的接收之外的功能性的访问(有意维护运行安全性)。

[0004] 现场设备的在测量数据传输或调节信号传输的范围之外的敏感的并且因此要保护的功能性例如涉及参数化、对运行模式的设定、现场设备的校准参数以及诊断。

[0005] 所力求的是:给之前描述的现场设备配备(其它)通信接口、即开头已经提及的终端设备通信接口,大多利用该终端设备通信接口来实现现代通信技术,使得能实现更高的传输率和现代操作接口。通过该终端设备通信接口,应该交换基本上并不过程相关的数据。

[0006] 本研究的主题是拥有终端设备通信接口的现场设备,通过该终端设备通信接口,外部终端设备可以访问现场设备的信息技术内容,其中这些信息技术内容首先并不是真正的测量数据。因此,不涉及现场设备通过其来输出测量数据和接收调定量的过程接口。

[0007] 终端设备可能是用于相应的现场设备的特殊的操作设备,但是也可能是商用计算机、手机或平板计算机。终端设备不必具有自己的操作单元(键盘、鼠标、触摸屏)或者显示装置,也可能只是涉及具有相对应的硬件式接口的存储器(例如USB记忆棒、加密狗)。

发明内容

[0008] 本发明的任务是：说明一种用于在现场设备和通过终端设备通信接口来与该现场设备连接的终端设备之间的安全通信的方法以及一种相对应的具有现场设备和其它组件的系统，其中安全性高地防止借助于终端设备通信接口对该现场设备的滥用访问。

[0009] 在引文中所描绘的方法的情况下，该任务通过如下方式来解决：在终端设备中寄存单独的访问标志符并且终端设备将其访问标志符传输给现场设备。可以在与现场设备发生联系的情况下自动地传输访问标志符或者在现场设备提出要求之后才传输访问标志符，而这一点在这里并不重要。

[0010] 还规定：现场设备通过服务器通信连接来与认证服务器连接并且该现场设备将访问标志符或者从该访问标志符推导出的访问标志符传输给认证服务器。因此，该访问标志符可以以明文或者也可以以经修改的、例如经加密的形式被传输给认证服务器。

[0011] 现在规定：在认证服务器上寄存认证数据，在认证服务器上依据这些认证数据来检查访问标志符或所推导出的访问标志符的可信度并且借此检查终端设备的可信度。因此，即在与现场设备不同的认证服务器上检查终端设备的授权。这样保证了：具有未知的访问标志符的终端设备被判定为未经授权的通信成员。因此，在认证服务器上的检查可以得出：具有相对应的访问标志符的终端设备未知并且因而未经授权或者已知并且因此带有某种程度的通信授权。

[0012] 接着，所得到的并且在认证服务器上确定的认证结果经由服务器通信连接被传输给现场设备。借此，现场设备拥有：与该现场设备保持连接的终端设备已知还是未知以及因此是否具有关于通信的授权的信息。接着，根据被传输到现场设备上的认证结果来使终端设备可支配现场设备的资源。如果检查已经得出终端设备未知，则无论如何都不使该终端设备可支配现场设备的资源。该结果可以被通知给终端设备，现场设备也可以通过不做出任何反应来做出对终端设备未知的反应。

[0013] 使用认证服务器的优点在于：不必将相对应的认证数据寄存在现场设备本身中。这尤其是在大型自动化技术设施的情况下非常有用，其中使用很多现场设备、即例如上百或者几百个现场设备。当然，在这种设施的情况下，出于不同原因应该能够访问投入使用的现场设备的终端设备的数目或终端设备的用户的数目也增加。

[0014] 单独的访问标志符应该明确地标识与现场设备保持连接的终端设备或与现场设备保持连接的终端设备的用户。因此，在一个优选的设计方案中规定：该单独的访问标志符具有单独的终端设备名称和单独的终端设备密码；和/或该单独的访问标志符具有单独的用户名和单独的用户密码。由此，例如可能的是：被多个用户使用的确定终端设备、例如笔记本电脑具有与终端设备无关的、但却明确地标识相对应的用户的标志符。如果同一终端设备的不同的用户配备有不同的用户名和用户密码，则这一个终端设备的不同的用户能彼此区别开。

[0015] 在该方法的一个优选的设计方案中规定：在现场设备中寄存有认证服务器的地址并且在使用认证服务器的地址的情况下建立服务器通信连接。由此，例如可能的是：认证服务器和现场设备可以通过信息技术网络来连接，在该信息技术网络上连接有多个成员，这些成员可以在知道相对应的成员地址的情况下建立联系。借此可能的是：例如使用基于因特网协议(TCP/IP)的通信连接。

[0016] 在该方法的一个优选的设计方案中规定：在现场设备中以及在认证服务器中都寄存有加密装置，这些加密装置允许现场设备和认证服务器经加密地彼此交换数据。该加密装置例如可以是所谓的“shared secret(共享密钥)”，即可以是两个通信伙伴都知道的密钥。接着，现场设备用它的加密装置从该访问标志符推导出经加密的所推导出的访问标志符并且将其传输给认证服务器。接着，认证服务器可以用它的对应的加密装置将经加密的所推导出的访问标志符解密成以明文的访问标志符。立即清楚的是：借此提供了程度更高的安全性，因为使对传输访问标志符的影响变得困难得多。

[0017] 该方法的一个扩展方案的特点在于：认证服务器的认证数据也包括与访问标志符相关联的权限范围；而且由认证服务器传送给现场设备的认证结果也包括分配给访问标志符的权限范围。接着，在现场设备上将关于权限范围的信息用于使终端设备只能与所关联的权限范围相对应地支配现场设备的资源。权限范围例如可以是“只读访问”、“受限制的读访问”、“写访问”、“受限制的写访问”、“对功能性的调用”或者也可以只是“对功能性的受限制的调用”。接着，这些权限范围也可以配备参数列表和/或功能列表。接着，在参数列表中，例如可以列出可由终端设备读取的参数或者也可以由终端设备以写方式改变的参数。相对应地，功能列表可以列出可由终端设备在现场设备上激活的功能。

[0018] 在该方法的一个扩展方案中规定：这些权限范围表示子权限组，其中对子权限组的定义或者存放在现场设备上或者存放在认证服务器上而且在后者的情况下在调用时被传输到现场设备上。这使得对用户组及其授权的管理变得容易。可能的子权限组例如可以是其用户(User)、操作员(Operator)、专家(Expert)、服务(Service)、工厂(Factory)。接着，现场设备的纯用户(User)例如可以对现场设备的少量参数进行只读访问，而对重要的系统参数、诸如校准数据要么可以进行只读访问要么完全不能访问。与现场设备在制造过程的范围内(工厂(Factory))连接的终端设备可以相对应地对现场设备的所有参数进行写访问。

[0019] 该方法的一个优选的设计方案的特点在于：认证服务器的认证数据也包括与访问标志符相关联的会话属性，其中由认证服务器传送给现场设备的认证结果也包括分配给访问标志符的会话属性。这种会话属性例如可以是会话语言、会话时长、绝对会话时间、会话访问的数目或者还有会话接口。再则，会话时长是如下时间，在该时间之后，现场设备独立地使终端设备通信连接中断。绝对会话时间是对在一天中的时间窗口的指定，只能在该时间窗口之内建立终端设备通信连接，在该绝对时间窗口之外不能建立终端设备通信连接。会话接口是如下技术接口，通过该技术接口来建立终端设备通信连接。例如可涉及以如下技术对接口的指定：蓝牙、无线局域网(WLAN、Wifi)、红外(IR)、以太网。

[0020] 采用权限范围以及会话属性能够实现：现场设备向终端设备提供个性化操作界面，而且依据权限范围和/或会话属性来实现对操作界面的个性化。个性化操作界面例如可以通过现场设备经由个性化网络服务器提供给终端设备。如果终端设备本身没有显示装置，则也可以合理的是：现场设备在该现场设备本身的物理显示装置上提供该个性化操作界面。再则，例如可以以确定语言来呈现菜单结构，而且可以只显示与相应的权限范围相对应的参数和/或功能性。

[0021] 在该方法的一个特别优选的设计方案中规定：现场设备将与终端设备的通信至少部分地记录在报告中并且在通信、即相对应的会话结束时将该报告传送给认证服务器，其

中该报告被存储在认证服务器上。替选地,该报告在通信期间不断地被传送给认证服务器并且该报告不断地被存储在认证服务器上。由此可以保证:能追溯对现场设备的任何影响。通过分析这样的报告,也可以确定哪些措施已经通过终端设备通信连接来执行,由此可以反推出例如操作、可操作性、维护强度以及可能的错误源。

[0022] 结合终端设备通信连接,已经阐述的是:该终端设备通信连接可以在不同的技术下实现。相同的情况也适用于服务器通信连接,该服务器通信连接同样可以按照不同的技术来设计(例如蓝牙、无线局域网、红外、以太网),其中也可以同时实现不同的技术。

[0023] 开头引出的任务也通过一种用于在自动化技术的现场设备与终端设备之间的安全通信的系统来解决。该系统包括现场设备和认证服务器,其中该现场设备与物理过程保持有效关联并且该现场设备能通过现场总线接口与其它现场设备和/或过程控制系统连接。该现场设备具有数据处理电子电路,该数据处理电子电路可以设计得完全不一样复杂。对此,在如今的现场设备的情况下,使用数字信号处理器、微控制器、模拟/数字转换器、数字/模拟转换器、相对应的接口电子电路以及还有模拟信号处理组件。现场设备拥有与现场总线接口不同的终端设备通信接口并且能利用该终端设备通信接口来与终端设备连接。此外,该现场设备通过服务器通信接口来与认证服务器连接。

[0024] 比照来说,之前已经针对关于详细呈现的方法方面的相对应的术语解释的内容也适用于这里所呈现的由现场设备和认证服务器构成的系统。该数据处理电子电路被设计为使得该数据处理电子电路可以通过终端设备通信接口来接收所连接的终端设备的单独的访问标志符。如果这里谈及该数据处理电子电路被设计为使得能用它来执行不同的过程,则是指:该数据处理电子电路完全特殊地被准备为使得它可以毫无困难地实施所描述的功能。并不是指以下数据处理电子电路:该数据处理电子电路还要必须首先为此(例如通过相对应的并且仍要进行的编程)进行准备或者可能会在理论上被处理,使得该数据处理电子电路接着必要时也可能会在理论上实施所描述的功能性。

[0025] 认证服务器十分具体地设计为使得在该认证服务器上寄存有认证数据,在认证服务器上依据这些认证数据来检查并且可以检查访问标志符的可信度,其中所得到的认证结果由认证服务器传输给现场设备。相对应地,现场设备的数据处理电子电路被设计为使得该数据处理电子电路通过服务器通信接口来接收由认证服务器确定的认证结果。

[0026] 最后,该数据处理电子电路也具体地被设计为使得该数据处理电子电路根据所接收到的认证结果来使终端设备可支配现场设备的资源。

[0027] 总体而言,现场设备和认证服务器具体地设计为使得它们可以执行之前详细描述的方法。

[0028] 在该现场设备的一个特别优选的设计方案中规定:服务器通信接口、终端设备通信接口以及可能的与这些通信接口保持关联的软件服务在现场设备上与现场总线接口和与该现场总线接口保持关联的软件服务隔离地来实现。由此可以保证:不可能通过服务器通信接口、通过终端设备通信接口以及通过可能的与这些通信接口保持关联的软件服务来影响现场总线接口和与该现场总线接口保持关联的软件服务。

附图说明

[0029] 现在,详细地给出设计和扩展按照本发明的用于在自动化技术的现场设备和通过

终端设备通信连接来与该现场设备连接的终端设备之间的安全通信的方法以及相对应的由现场设备和认证服务器构成的系统的多种途径。为此,一方面参阅专利独立权利要求的专利从属权利要求,另一方面参阅结合附图对实施例的如下描述。在附图中:

图1示意性地示出了按照本发明的用于在自动化技术的现场设备与所连接的终端设备之间的安全通信的方法以及按照本发明的由现场设备和认证服务器构成的系统;

图2示出了按照本发明的方法在以时序图方式的认证检查的结果为肯定的情况下的实施例;

图3示出了按照本发明的方法在以时序图方式的认证检查的结果为否定的情况下的另一实施例;

图4示出了按照本发明的方法在以时序图方式对在现场设备与终端设备之间的通信进行记录的情况下的实施例。

具体实施方式

[0030] 在图1至4中,分别示出了用于在自动化技术的现场设备3和通过终端设备通信连接4来与现场设备3连接的终端设备5之间的安全通信的方法1。在图1中,同时示出了用于执行方法1的设备技术构造,图1尤其是用来呈现用于在现场设备3与终端设备5之间的安全通信的系统2。

[0031] 如开头已经描述的那样,现场设备3与物理过程6保持有效关联,要么现场设备3从物理过程6记录测量数据要么主动影响物理过程6,其方式是例如改变阀位置、电机转速等等,一般来说即所连接的执行器的调定量。物理过程6常常是在工业应用中的自动化技术设施。

[0032] 现场设备3通过现场总线接口7与其它现场设备3a、3b、3c、3d并且与过程控制系统8连接,即通过现场总线9连接。因此,通过现场总线9来交换过程信息。在当前情况下,现场总线9按照HART标准来实现。

[0033] 为了理解在下文呈现的方法1和在下文呈现的系统2的益处,需要意识到:在真实的自动化技术应用中,多个现场设备3与物理过程6保持有效关联。在广泛的应用中,可能使用几百个现场设备3,这些现场设备能按需要与一个或多个终端设备5发生连接,例如用于检查功能性(维护)、用于读取诊断信息或者用于对设备的重新参数化。因此,多个终端设备5可以建立与相应的现场设备3的联系。首先显而易见的是:在每个现场设备3中都寄存有究竟哪个终端设备5已知并且因此可能有访问现场设备3的授权的信息。如果取消终端设备5或添加新的终端设备5,则实际上必须向所有涉及到的现场设备3通知新的情况并且必须在这些现场设备中寄存相对应的信息。这里采用在下文呈现的方法1和所示出的系统2。

[0034] 首先规定:在终端设备5中寄存有单独的访问标志符10,而且只要在终端设备5与现场设备3之间通过终端设备通信连接4而存在联系,终端设备5就将其访问标志符10传输11给现场设备3。此外,现场设备3通过服务器通信连接12来与认证服务器13连接。现场设备3将访问标志符10或从访问标志符10推导出的访问标志符10'传输14给认证服务器13。

[0035] 在认证服务器13上寄存有认证数据15,在认证服务器13上依据这些认证数据来检查16访问标志符10的可信度。在图1中,以示意性示出的认证服务器13阐明了认证数据15寄存在表格中。在当前情况下,访问标志符10列举在表格中,使得可以确认访问标志符10的可

信度,即所得到的认证结果17为肯定。接着,所得到的认证结果17由认证服务器13经由服务器通信连接12被传输18给现场设备3。现场设备现在知道并且现在才知道认证结果17。

[0036] 现在,现场设备3根据被传输到现场设备3上的认证结果17来使终端设备5可支配现场设备3的资源。现场设备3的资源可以是数据,但是也可以是功能性。

[0037] 因为方法1的随时间的进展在图1的具体图示之内并不能简单地看出,所以在图2和3中又以时序图形式示出了流程。左侧的垂线是终端设备5,中间的垂线是现场设备3而右侧的垂线是认证服务器13。在图2中以及在图3中示出了:终端设备5请求访问现场设备3。在图2中,对可信度的检查的结果17为肯定,在图3中,该结果为否定。

[0038] 方法1开始于终端设备5将其访问标志符10传输给现场设备3。现场设备3与认证服务器13连接并且将访问标志符10或所推导出的访问标志符10'传输14给认证服务器13。因此,认证服务器13或者直接获得访问标志符10或者该认证服务器从所推导出的访问标志符10'推断出原来的访问标志符10。

[0039] 现在,认证服务器13依据寄存在认证服务器13上的认证数据15来检查16访问标志符10是否已知。在图2中示出的情况下,认证结果17为肯定。现在,认证服务器13将认证结果17传输18给现场设备3。接着,现场设备3使终端设备5可支配19确定的资源。

[0040] 不同于此,在按照图3的实施例中,认证结果17为否定。这里,认证服务器13也向现场设备3通知18(否定的)认证结果17,但是现场设备3无论如何都不使终端设备5可支配资源。在当前情况下,该现场设备仅仅向终端设备5通知20未建立通信。由现场设备3向终端设备5的这种(否定)的反馈也可以简单地不发生。

[0041] 在图1中,在终端设备5中附加地示出了:寄存有单独的终端设备名称10a和单独的终端设备密码10b,作为单独的访问标志符10。替选地,访问标志符10也可以是单独的用户名10a和单独的用户密码10b。这例如具有如下优点:终端设备5的不同用户当他们拥有不同的用户名10a和不同的用户密码10b时能彼此区别开。

[0042] 在图1中,关于现场设备3以及关于认证服务器13还示出了:在现场设备3中寄存有认证服务器的地址20,其中在使用认证服务器13的地址20的情况下建立服务器通信连接12。

[0043] 从图1中还能看到:在现场设备3中以及在认证服务器13中都寄存有加密装置21,这些加密装置允许现场设备3和认证服务器13经加密地彼此交换数据。现场设备3用它的加密装置21从访问标志符10推导出经加密的所推导出的访问标志符10'并且将其传输14给认证服务器13。认证服务器13用它的加密装置21来将经加密的所推导出的访问标志符10'解密成访问标志符10。

[0044] 在图1中,在认证服务器13方面还示出了:认证服务器13的认证数据15也包括与访问标志符10相关联的权限范围22;而且由认证服务器13传送给现场设备3的认证结果17也包括分配给访问标志符10的权限范围22。在图1中,认证数据15在认证服务器13处通过表格来呈现。这里,布置在一行内的值相关联。

[0045] 从图1中同样能看到:认证服务器13的认证数据15也包括与访问标志符10相关联的会话属性23;而且由认证服务器13传送给现场设备3的认证结果17也包括分配给访问标志符10的会话属性23。接着,这些会话属性23也由认证服务器13传送18回给现场设备3。

[0046] 现场设备3知道权限范围22或会话属性23的含义,其方式是:要么相对应的定义直

接存放在现场设备3中,要么这些定义存放在认证服务器13上并且同样一并被传输18给现场设备3。

[0047] 图4阐明了该方法的另一特殊功能,该功能通过使用认证服务器13而变得可能。时序图的上方部分对应于按照图2的图示。终端设备5向现场设备3发送了通信请求,终端设备5然后可以由认证服务器13在检查16可信度之后被识别,使得原则上使终端设备5可支配19现场设备3的资源。在图4中,终端设备5请求24现场设备3的资源并且随后在现场设备3上处理25资源请求24。现在这里重要的是:现场设备3与终端设备5之间的通信被记录26在报告27中。在终端设备5与现场设备3之间的通信结束之后,报告27被传送28给认证服务器13并且被存储在那里。在所示出的实施例中,认证服务器13还将对报告27的成功存储通知29给现场设备3。这不是强制必需的。

[0048] 因此,对于在现场设备3与终端设备5之间的安全通信来说必要的是包括现场设备3和认证服务器13的系统2,其中现场设备3能通过现场总线接口7来与其它现场设备3a、3b、3c、3d以及过程控制系统8发生连接。现场设备3包括数据处理电子电路30,该数据处理电子电路实际上包括在现场设备3之内的整个电子电路。现场设备3具有与现场总线接口7不同的终端设备通信接口31,该现场设备能通过终端设备通信接口来与终端设备5连接。现场设备3通过服务器通信接口32来与认证服务器13连接。数据处理电子电路30被设计为使得该数据处理电子电路可以通过终端设备通信接口31来接收所连接的终端设备5的单独的访问标志符10。数据处理电子电路30还被设计为使得该数据处理电子电路通过服务器通信接口32来将访问标志符10或者从访问标志符10推导出的访问标志符10'能够传输并且传输给认证服务器13。

[0049] 在认证服务器13上寄存有认证数据15,在认证服务器13上依据这些认证数据来检查16访问标志符10的可信度。

[0050] 数据处理电子电路30还被设计为使得该数据处理电子电路可以通过服务器通信接口32来接收由认证服务器13确定的认证结果17。最后,数据处理电子电路30被设计为使得该数据处理电子电路根据所接收到的认证结果17来使终端设备5可支配19现场设备3的资源。

[0051] 主要目标是:将现场设备3设计为使得现场总线接口7和与现场总线接口7保持关联的软件服务可以不受现场设备3的其它组件的影响。只有这样才能够保证:无论如何都不威胁设施安全性,尤其是没有由于经由终端设备通信接口31或服务器通信接口32的干预而威胁设施安全性。在所示出的对现场设备3的实现方案中,服务器通信接口32、终端设备通信接口31以及可能的与这些通信接口31、32保持关联的软件服务在现场设备3上隔离地实现,即尤其是与现场总线接口7和与现场总线接口7保持关联的软件服务隔离地实现。由此,不可能通过服务器通信接口32、通过终端设备通信接口31以及通过可能的与这些通信接口31、32保持关联的软件服务来影响现场总线接口7和与现场总线接口7保持关联的软件服务。

[0052] 附图标记

- 1 方法
- 2 系统
- 3 现场设备

- 4 终端设备通信连接
- 5 终端设备
- 6 过程
- 7 现场总线接口
- 8 过程控制系统
- 9 现场总线
- 10 单独的访问标志符
- 10' 所推导出的单独的访问标志符
- 10a 终端设备名称/用户名
- 10b 终端设备密码/用户密码
- 11 传输访问标志符
- 12 服务器通信连接
- 13 认证服务器
- 14 传输访问标志符
- 15 认证数据
- 16 检查可信度
- 17 认证结果
- 18 传输认证结果
- 19 使资源可支配
- 20 认证服务器的地址
- 21 加密装置
- 22 权限范围
- 23 会话属性
- 24 请求现场设备资源
- 25 处理资源请求
- 26 对通信进行记录
- 27 报告
- 28 传送报告
- 29 通知成功的报告存储
- 30 数据处理电子电路
- 31 终端设备通信接口
- 32 服务器通信接口。

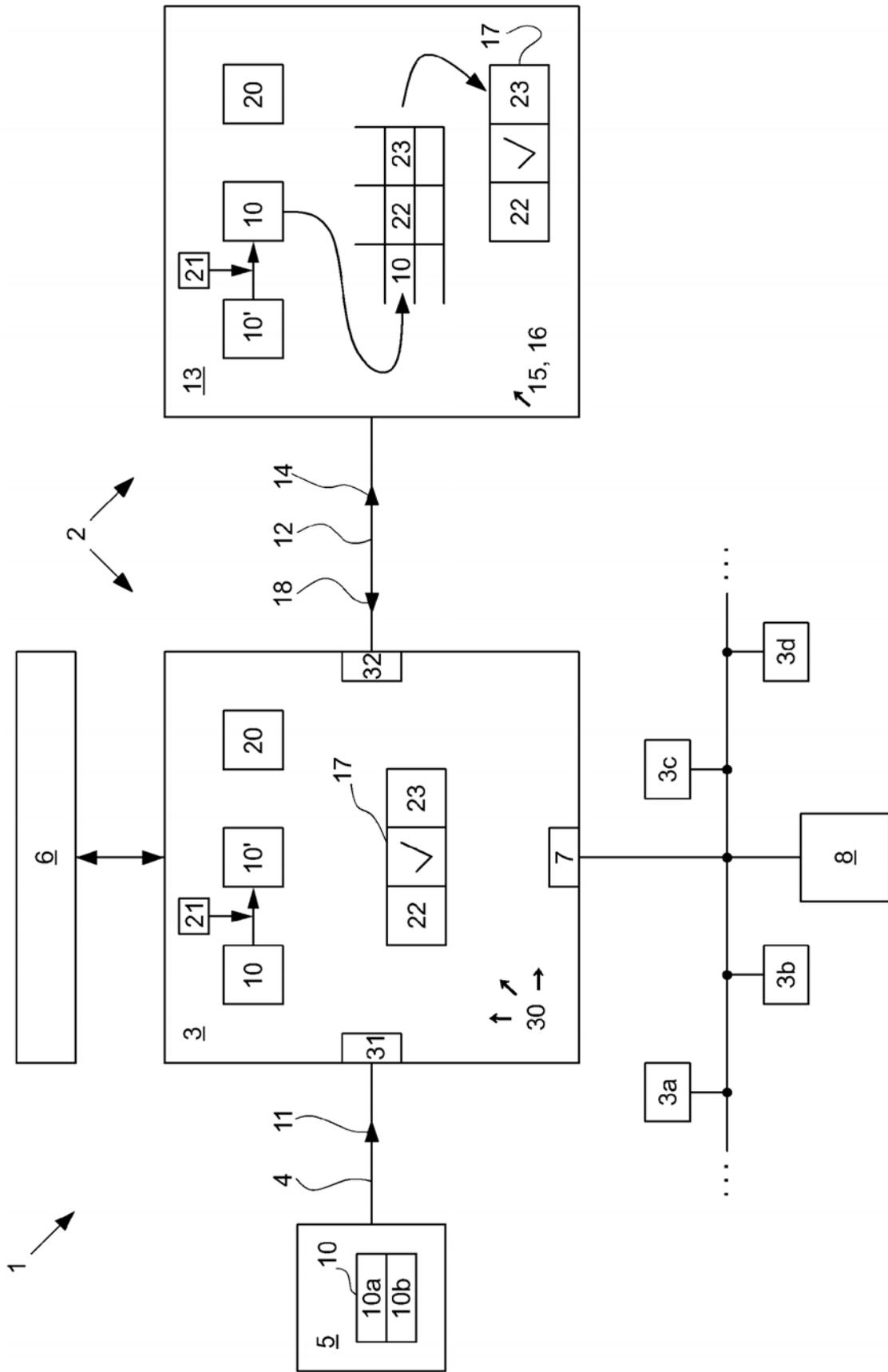


图 1

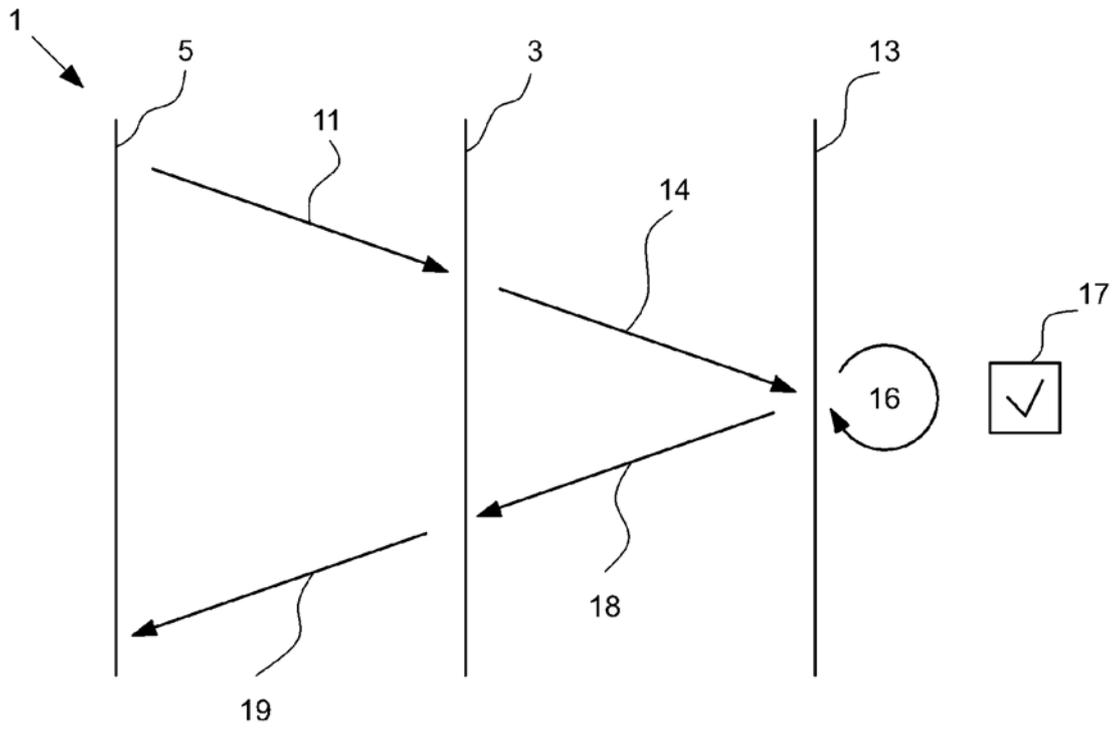


图 2

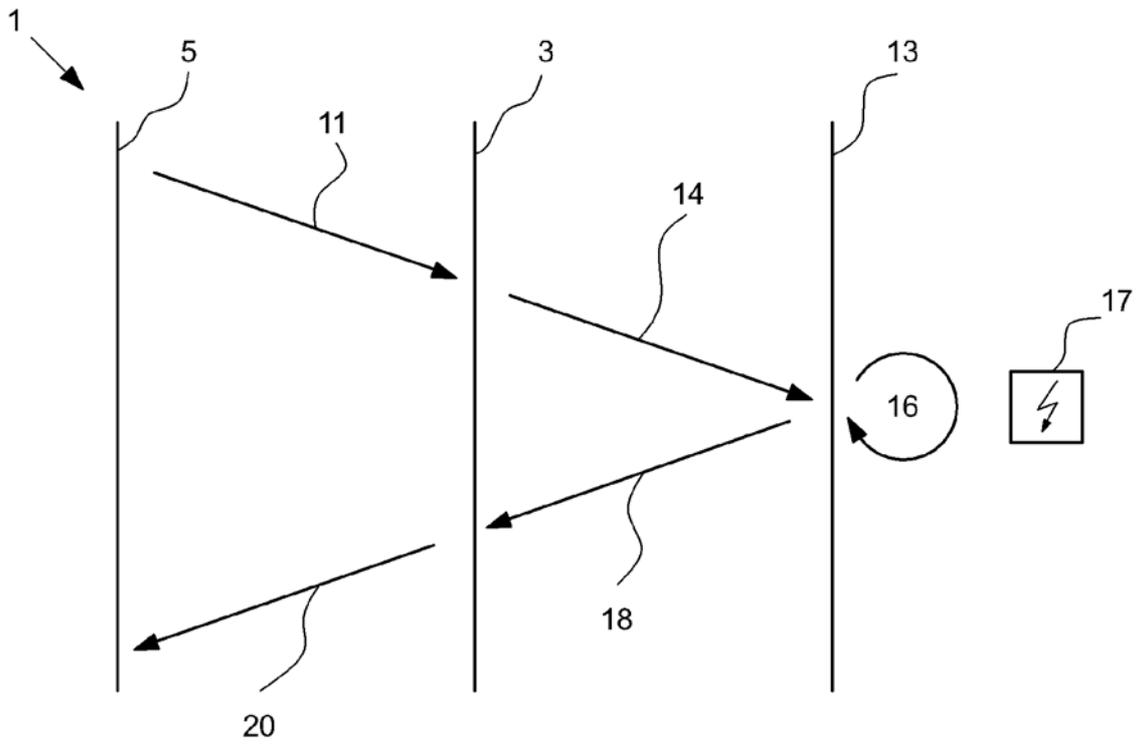


图 3

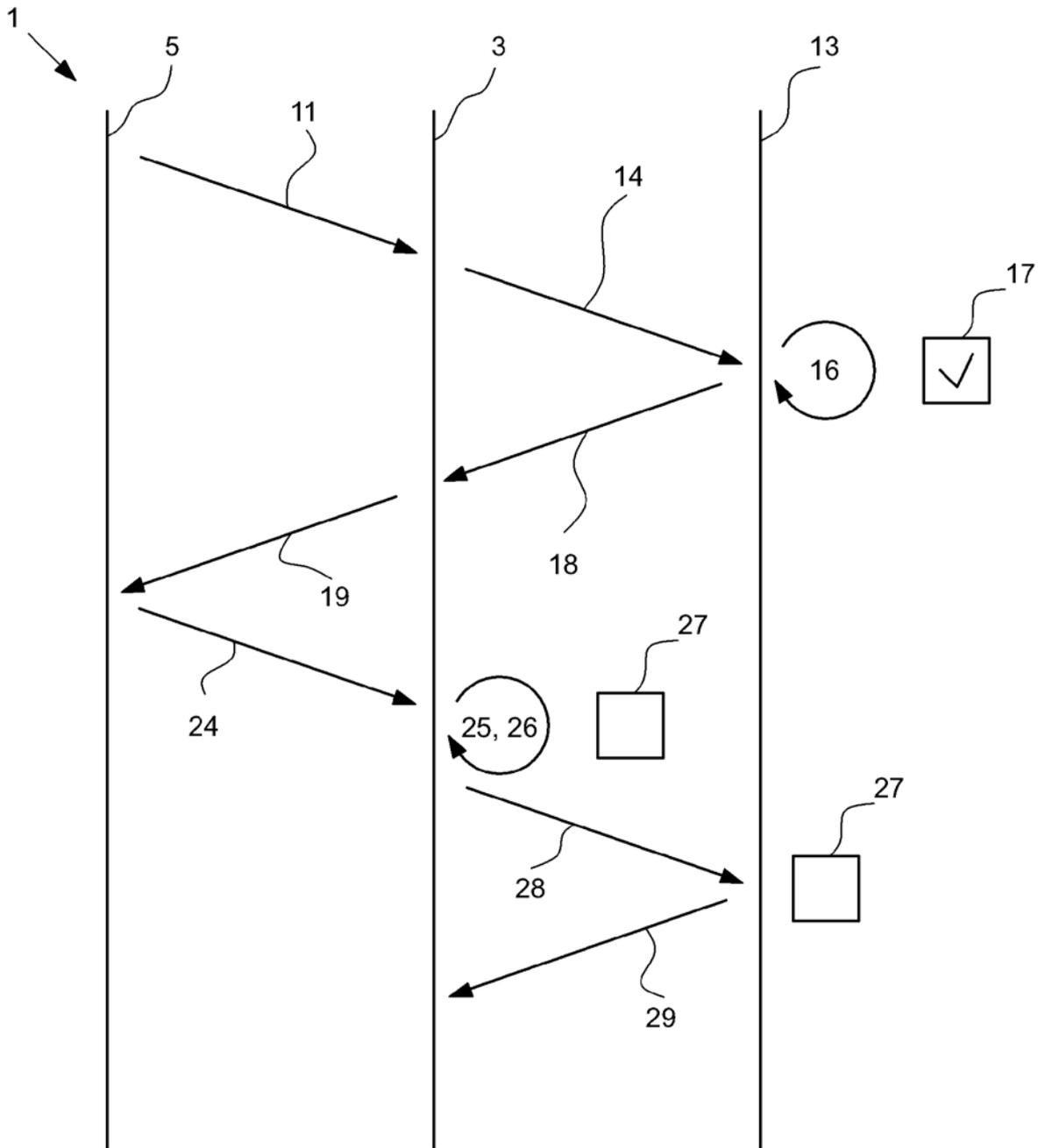


图 4