(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 103376766 B
(45)授权公告日 2017.11.17

(21)申请号 201310153717.5

(22)申请日 2013.04.28

(65)同一申请的已公布的文献号
申请公布号 CN 103376766 A

(43)申请公布日 2013.10.30

(30)优先权数据
13/460794 2012.04.30 US

(73)专利权人 通用电气公司
地址 美国纽约州

(72)发明人 J.B.聪 D.R.索基 P.K.S.萨库尔 W.R.佩蒂格鲁 R.J.博林

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 叶晓勇 朱海煜

(51)Int.Cl.
G05B 19/048(2006.01)

(56)对比文件
CN 102347872 A,2012.02.08,
CN 1338140 A,2002.02.27,
CN 1618060 A,2005.05.18,
CN 1302406 A,2001.07.04,
CN 1202662 A,1998.12.23,
CN 102347872 A,2012.02.08,
CN 1344000 A,2002.04.10,

审查员 张姗姗

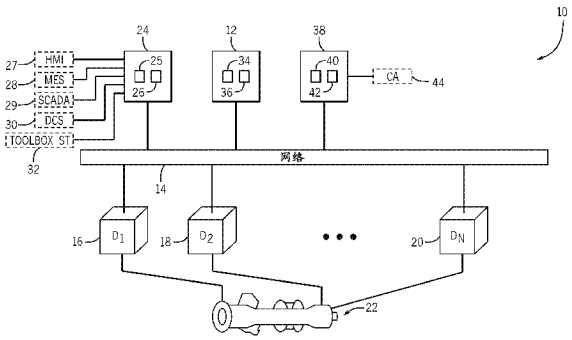
权利要求书2页 说明书7页 附图3页

(54)发明名称

用于工业控制器的安全工作的系统和方法

(57)摘要

一种系统包括具有存储器和处理器的工业控制器，处理器配置成使工业控制器工作在开放模式，其中开放模式配置成使工业控制器能够通过未认证的网络连接或本地连接接收指令。工业控制器的处理器还配置成使工业控制器工作在安全模式，其中安全模式配置成使工业控制器能够仅通过认证的网络连接接收指令。



CN 103376766 B

1.一种系统,包括:

包括存储器和处理器的工业控制器,所述处理器配置成:

使所述工业控制器工作在开放模式,其中,所述开放模式配置成使所述工业控制器能够通过未认证的网络连接或本地连接接收指令;以及

使所述工业控制器工作在替代开放模式的安全模式,其中,所述安全模式配置成使所述工业控制器能够仅通过认证的网络连接接收指令。

2.如权利要求1所述的系统,包括存储在所述工业控制器的所述存储器中的白名单,其中所述白名单包括多个值,其中每个值与在所述工业控制器的所述存储器中存储的可执行文件关联。

3.如权利要求2所述的系统,其中,所述开放模式配置成使所述工业控制器能够执行存储在所述存储器中的多个可执行文件中的任意可执行文件。

4.如权利要求2所述的系统,其中,所述安全模式配置成阻止所述工业控制器执行所述存储器中存储的在所述白名单中没有关联值的多个可执行文件中的任意可执行文件。

5.如权利要求1所述的系统,其中,所述处理器配置成使所述工业控制器工作在协商模式,其中所述协商模式配置成从证书权限(CA)获取证书,并且禁用到所述工业控制器的未认证的网络连接和本地连接。

6.如权利要求5所述的系统,其中,所述处理器配置成使所述工业控制器工作在认证模式,其中所述认证模式配置成使用从所述CA获取的所述证书在所述工业控制器和配置工具之间建立所述认证的网络连接。

7.如权利要求6所述的系统,其中,所述认证的网络连接是加密的认证的网络连接。

8.如权利要求1所述的系统,其中,所述处理器配置成在整个功率循环、软件升级、应用程序下载或它们的任何组合期间继续使所述工业控制器工作在所述开放模式或所述安全模式。

9.如权利要求1所述的系统,其中,所述未认证的网络连接包括远程登录或文件传送协议(FTP)连接,并且其中所述认证的网络连接包括安全套接字层(SSL)连接。

10.如权利要求1所述的系统,包括具有所述工业控制器的工业系统,其中所述工业系统包括气化器、气体处理单元、涡轮、发电机或它们的组合。

11.一种方法,使工业控制器工作在开放模式或安全模式或协商模式中的一种模式,包括:使工业控制器工作在开放模式,其中,所述开放模式包括允许所述工业控制器使用未认证的网络协议与配置工具通信;

接收来自所述配置工具的指令以使所述工业控制器工作在安全模式,其中,所述安全模式包括限制所述工业控制器仅使用认证的网络协议与所述配置工具通信;

使所述工业控制器工作在协商模式,其中,所述协商模式包括从证书权限获取安全证书,并且禁用未认证的网络协议;以及

使所述工业控制器工作在认证模式,其中,所述认证模式包括在所述工业控制器和所述配置工具之间建立证书认证的连接。

12.如权利要求11的所述方法,其中,所述安全模式包括阻止所述工业控制器执行在白名单中没有对应条目的二进制文件。

13.如权利要求12所述的方法,建立证书认证的连接包括在所述工业控制器和所述配

置工具之间建立证书认证的、加密的连接。

14.如权利要求11所述的方法，其中，所述安全模式包括禁用通过本地端口对所述工业控制器的访问。

用于工业控制器的安全工作的系统和方法

技术领域

[0001] 本文公开的主题涉及工业控制系统，并且更具体而言涉及保护工业控制系统的工作的安全。

背景技术

[0002] 工业控制系统，比如自动化的发电系统(例如，风、水以及燃气涡轮系统)和自动化的制造系统(例如，炼油厂、化工厂等)，是现代工业的共同特征。对于此类工业控制系统，工业控制器通常可控制系统的工作。例如，工业控制系统中的某些设备(例如传感器、泵、阀、制动器等)可受工业控制器控制并且可向工业控制器报告数据。此外，工业控制器可执行指令(例如固件和/或应用程序)，该指令通常可使得工业控制器能够控制工业控制系统(例如燃气涡轮系统)的工作。这些指令可由工业控制器的制造商提供。例如，可在工业控制系统中安装工业控制器之前把这些指令载入到工业控制器中。另外，工业控制器可提供访问工业控制器和/或向工业控制器提供指令(比如通过网络连接或本地端口)的若干不同方法。

发明内容

[0003] 以下概括了在范围上与最初要求保护的发明相匹配的某些实施例。这些实施例不意图限制要求保护的发明的范围，而是这些实施例仅意图提供本发明的可能形式的简要概括。实际上，本发明可包含可与以下陈述的实施例相似或不同的各种形式。

[0004] 在一个实施例中，一种系统包括具有存储器和处理器的工业控制器，处理器配置成使工业控制器工作在开放模式，其中开放模式配置成使工业控制器能够通过未认证的网络连接或本地连接接收指令。工业控制器的处理器还配置成使工业控制器工作在安全模式，其中安全模式配置成使工业控制器能够仅通过认证的网络连接接收指令。

[0005] 在另一个实施例中，一种方法包括使工业控制器工作在开放模式，其中开放模式包括允许工业控制器使用未认证的网络协议与配置工具通信。该方法还包括接收来自配置工具的指令以使工业控制器工作在安全模式，其中安全模式包括限制工业控制器仅使用认证的网络协议与配置工具通信。该方法还包括使工业控制器工作在协商(negotiation)模式，其中协商模式包括从证书权限(authority)获得安全证书并且禁用未认证的网络协议。该方法还包括使工业控制器工作在认证模式，其中认证模式包括在工业控制器和配置工具之间建立证书认证的连接。该方法还包括使工业控制器工作在安全模式。

[0006] 在另一个实施例中，一种有形的、非暂时的(non-transitory)计算机可读的介质配置成存储可由工业控制器的处理器执行的指令。该指令包括禁用通过未认证的网络连接或通过本地端口向工业控制器通信的指令。该指令还包括实现通过认证的网络连接向工业控制器通信的指令。该指令还包括验证在允许存储在计算机可读介质上的可执行文件执行以前该可执行文件没有被修改的指令。

[0007] 根据本发明的第一方面，提供一种方法，包括：使工业控制器工作在开放模式，其中，所述开放模式包括允许所述工业控制器使用未认证的网络协议与配置工具通信；接收

来自所述配置工具的指令以使所述工业控制器工作在安全模式，其中，所述安全模式包括限制所述工业控制器仅使用认证的网络协议与所述配置工具通信；使所述工业控制器工作在协商模式，其中，所述协商模式包括从证书权限获取安全证书，并且禁用未认证的网络协议；以及使所述工业控制器工作在认证模式，其中，所述认证模式包括在所述工业控制器和所述配置工具之间建立证书认证的连接；以及使所述工业控制器工作在安全模式。

[0008] 根据本发明第一方面的方法，其中，所述安全模式包括阻止所述工业控制器执行在白名单中没有对应条目的二进制文件。

[0009] 根据本发明第一方面的方法，建立证书认证的连接包括在所述工业控制器和所述配置工具之间建立证书认证的、加密的连接。

[0010] 根据本发明第一方面的方法，其中，所述安全模式包括禁用通过本地端口对所述工业控制器的访问。

[0011] 根据本发明的第二方面，提供一种有形的、非暂时的计算机可读介质，配置成存储可由工业控制器的处理器执行的指令，所述指令包括：禁用通过未认证的网络连接或通过本地端口到所述工业控制器的通信的指令；实现通过认证的网络连接到所述工业控制器的通信的指令；以及验证在允许存储在所述计算机可读介质上的可执行文件执行前所述可执行文件没有被修改的指令。

[0012] 根据本发明第二方面的介质，包括接收来自配置工具的指令以把所述工业控制器从工作的开放模式改变到工作的安全模式的指令。

[0013] 根据本发明第二方面的介质，包括使所述工业控制器能够在功率循环、软件升级、应用程序下载或它们的任何组合之后恢复工作的所述安全模式的指令。

[0014] 根据本发明第二方面的介质，包括：联系证书权限并得到证书的指令；以及使用所述证书通过认证的网络连接、加密的网络连接或认证的加密的网络连接与配置工具通信的指令。

[0015] 根据本发明第二方面的介质，其中，验证所述可执行文件没有被修改的所述指令包括：确定所述可执行文件的哈希密钥值的指令；以及确定当所述哈希密钥值存在于白名单文件中时所述可执行文件没有被修改的指令。

[0016] 根据本发明第二方面的介质，其中，所述工业控制器包括气化器控制器、气体处理控制器、涡轮控制器、发电机控制器或它们的任何组合。

附图说明

[0017] 当下列的详细描述参考附图一起阅读时，将更好地理解本发明的这些和其它的特征、方面以及优点，其中在整个附图中同样的字符表示同样的部件，其中：

[0018] 图1是根据本公开内容的各方面的正由工业控制器操作的工业控制系统的实施例的示意图；

[0019] 图2是根据本公开内容的各方面的过程的实施例的流程图，工业控制器可通过该过程从工作的开放模式移到工作的安全模式；

[0020] 图3是根据本公开内容的各方面的过程的实施例的流程图，工业控制器可以协商模式执行该过程；以及

[0021] 图4是根据本公开内容的各方面的过程的实施例的流程图，工业控制器可以认证

模式执行该过程。

具体实施方式

[0022] 以下将描述当前发明的一个或多个具体实施例。为了努力提供这些实施例的简洁描述，在说明书中可不描述实际实施的所有特征。应该领会，在任何此类实际实施的开发中，如同在任何工程或设计项目中一样，必须作出许多实施特定的决定以实现开发者的具体目标，比如符合涉及系统的和涉及商业的限制，其在一个实施与另一个实施间可有所不同。此外，应该领会，此开发努力可能是复杂并且耗时的，但是对于受益于本公开内容的普通技术人员而言将仍然是设计、加工和制造的常规任务。

[0023] 在引入当前发明的各种实施例的要素(element)时，冠词“一个(a)”、“一个(an)”、“该(the)”以及“所述”意图表示存在一个或多个该要素。术语“包含”、“包括”和“具有”意图是包括在内的并且表示可以有不同于所列出要素的额外要素。另外，如本文所使用的，术语“可执行文件”和“二进制文件”通常都可指包括可由处理器(例如，工业控制器的处理器)执行的指令(例如，二进制指令)的计算机可读文件。此外，如文本所使用的，术语“软件开发者”通常可指开发、维护和/或提供以源代码和/或可执行文件的形式的指令以控制工业控制器工作的机构。此外，如本文所使用的，术语“白名单(whitelist)”可指文件，该文件包括标识被授权在工业控制器上运行的可执行文件的列表。另外，术语“授权的”在本文可用来指可执行文件，该可执行文件被验证来自可靠的源头(即，软件开发者)并且其内容被验证是与当它由可靠的源头提供时相同。

[0024] 通常可需要使工业控制系统的工业控制器工作在安全模式。即，通常可需要对工业控制器的典型行为或工作施加若干限制，以便提高工业控制系统的总体安全。例如，如以下所详细陈述的，使工业控制器工作在安全模式通常可阻止未授权的可执行文件的执行和/或阻止由未授权的人员或系统对工业控制器的访问。因此，当前公开的系统和方法使得工业控制器能够工作在安全模式，其中安全模式通常阻止对工业控制器的未授权访问。此外，当前公开的实施例通过逐渐地向工业控制器应用若干安全限制，使得工业控制器能够从开放模式(例如，没有限制)移到安全模式(例如，有额外安全限制)。通过使得工业控制器能够工作于在工业控制器的各种活动(例如功率循环和软件升级)持续的安全模式，当前公开的实施例通常提供具有未授权访问和/或未授权指令执行的降低风险的工业控制系统。

[0025] 牢记前述，图1是说明工业控制系统10的示意图。根据本公开内容的各方面，所说明的工业控制系统10包括可配置成工作在至少开放模式和安全模式的工业控制器12(例如，Mark™Vie或可从纽约Schenectady的通用电气获得的任何其它Mark™工业控制器)。此外，工业控制器12可耦合到网络14以控制若干现场(field)设备16、18和20的工作。例如，所说明的工业控制器12通过网络14接收来自若干现场设备16、18和20(例如，温度传感器、压力传感器、电压传感器、控制阀、制动器或工业控制系统的类似现场设备)的感知数据，以监测和控制燃气涡轮系统22的工作。在其它实施例中，不是燃气涡轮系统22，正由工业控制系统10监测和控制的系统可包括例如任何自动化的制造系统(例如，炼油厂系统、化工生产系统、气化系统或类似的自动化的制造系统)或自动化的发电系统(例如，发电厂、汽轮机系统、风力涡轮机系统和类似的自动化的发电系统)。例如，在一个实施例中，气化系统可包括：配置成气化碳质原料以生成合成气的气化器，配置成处理合成气以移除不需要的成分

(例如,酸性气体)的气体处理单元,配置成燃烧合成气以驱动涡轮的燃烧室以及配置成产生电力的耦合到涡轮的发电机。在此类实施例中,工业控制器12可使用至少现场设备16、18和20监测和控制气化系统的各个部件(例如,气化器、气体处理单元、燃烧室和涡轮)。

[0026] 对于所说明的工业控制系统10,现场设备16、18和20通信地(communicatiely)耦合到工业控制器12(例如,通过网络14),同时监测和控制燃气涡轮系统22的工作的各个方面和参数(例如,监测燃气涡轮系统的燃烧室中的温度,控制耦合到燃气涡轮系统的轴(shaft)的发电机的电压输出,调节进入燃烧室的燃料的流量,控制热量回收蒸汽发生器(HRSG)的蒸汽输入等)。应该领会,所说明的工业控制系统10表示简化的工业控制系统,并且其它工业控制系统可包括任意合适数目的工业控制器12、网络14、连网设备、现场设备等以监测和控制任何自动化系统22的部分。

[0027] 在所叙述的实施例中,工业控制器12可使用网络14与现场设备16、18或20中的任何一个通信并且控制现场设备16、18或20中的任何一个。例如,工业控制器12可居于工厂中并且可配置成调整涉及设备16、18、20的一个或多个生产过程(process)条件。网络14可以是适合实现通信的任何电子和/或无线网络,并且可包括光纤介质、双绞线线缆介质、无线通信硬件、以太网线缆介质(例如,Cat-5、Cat-7)等。此外,网络14可包括若干子总线,比如适合以100 MB/sec和更高的通信速率连接工业控制系统10的部件的高速以太网子总线。另外,网络14可包括输入/输出(I/O)网络,比如符合电气和电子工程师协会(IEEE) 802.3标准的I/O网络。网络14还可包括适合以大约31.25 Kb/sec的通信速率连接工业控制系统10的部件的H1网络子总线。例如,子总线可通过使用链接设备或网关(比如,在由德国Haar的softing AG提供的命名FG-100下可获得的那些网关和/或从纽约Schenectady的通用电气公司可获得的I/O包装(pack))彼此之间互相通信。实际上,网络14的若干互连子总线可用来在工业控制系统10的部件间通信。

[0028] 工业控制器12,包括存储器34和处理器36,可执行指令(例如,可执行文件中的二进制指令)以通常控制工业控制系统10的工作。例如,工业控制器12的存储器34可包括包含二进制指令的一个或多个文件,该文件可由处理器36执行以便控制和监测布置在燃气涡轮系统22的部分内的现场设备16、18和20。例如,这些可执行文件可在工业控制器12安装到工业控制系统10之前,最初由工业控制器12的制造商安装到工业控制器12的存储器34中。此外,例如,存储在工业控制器12的存储器34中的可执行文件可不定期地更新以增加早先软件版本的特征以及提高性能。

[0029] 还通信地耦合到工业控制器12(例如,通过网络14或其它合适网络)的是设备24,其包括存储器25和处理器26,设备24可托管(host)人机界面(HMI)系统27、制造执行系统(MES) 28、监控站(supervisor)控制和数据获取(SCADA)系统29、分布式控制系统(DCS) 30或类似接口系统。特别地,在某些实施例中,设备24可托管配置应用程序或工具,比如ToolboxST™(由要素32表示),可从纽约Schenectady的通用电气公司获得。通常,前述的系统可提供一个或多个接口,通过该接口用户可监测和控制工业控制器12的工作。例如,HMI 27和/或ToolboxST 32可提供用户接口,通过该用户接口工业控制系统10的各个参数(例如,存储在工业控制器12的存储器34中)可被强加(force)或设定。通过另一个示例,HMI 27和/或ToolboxST 32可包括接口,通过该接口存储在控制器12的存储器34中的各个可执行文件可被更新到更新的版本。在某些实施例中,前述的系统可被托管在单个设备24上,而在

其它实施例中，它们可各自被安装到工业控制系统10中的一个或多个设备上。

[0030] 此外，具有存储器40和处理器42的安全服务器38可通信地耦合到工业控制器12和设备24(例如，通过网络14或其它合适网络)并且可托管证书权限(CA) 44。由安全服务器38托管的证书权限44通常可在工业控制系统10中发出和撤回证书，以例如实现在工业控制器12和设备24之间的安全通信。应该领会，尽管在图1中仅说明了单个安全服务器38和证书权限44，但是在某些实施例中，工业控制系统10可具有1、2、3、4或更多个安全服务器38和/或证书权限44。

[0031] 通常而言，证书是可使用数字签名来验证证书持有者身份的电子文档。例如，可需要控制系统10的各个部件使用相互认证或其它安全技术(例如，双因素(two-factor)认证)来验证彼此的身份。通常，相互认证可指第一个证书持有者(例如，设备24)验证第二个证书持有者(例如，工业控制器12)的身份，并且反过来该第二个证书持有者接着验证该第一个证书持有者的身份(例如，通过网络14)。因此，相互认证可减少工业控制系统10的未授权使用的几率。

[0032] 如此，公开的实施例包括适用于通过使用证书的相互认证(例如，双向认证)的使用使向工业控制器12的通信安全的系统和方法。例如，如以下详细讨论的，设备24(例如，在设备24上运行的ToolboxST 32或HMI 27)和工业控制器12可从证书权限44获得各自的证书。接着，例如当ToolboxST 32想要建立到工业控制器12的经认证通信通道时，作为验证它们各自身份的一部分，该两个设备可交换它们各自的证书。该认证通常可减小或消除工业控制器12和/或设备24的未授权使用的可能性。另外，设备24可反过来验证工业控制器12的身份以进一步提高工业控制系统10的安全。此外，除了该认证之外，某些实施例还可实现加密的使用以进一步保护经认证通信通道的安全。即，在某些实施例中，工业控制器12和设备24可分别使用包含于其它设备的证书中的数据(例如，公用密钥(key))的一部分以加密通信内容，使得这些内容对于工业控制系统10中的其它设备通常不可读。

[0033] 除了使通信安全以外，当前公开的实施例可利用列白名单(whitelisting)方法来对存储在工业控制器12的存储器34中的每个可执行文件在执行之前进行验证。例如，该白名单(whitelist)文件可包括对在特定软件发布中的授权可执行文件所确定的哈希(hash)密钥值的集合。即，在每个可执行文件建立(例如，编译)之后，该可执行文件可作为输入提供给哈希函数(例如，循环冗余校验(CRC)哈希函数、消息摘要算法(MD:Message-Digest Algorithm)哈希函数、安全哈希算法(SHA)哈希函数或其它合适的哈希函数)，并且与该可执行文件关联的哈希密钥值输出可存储在白名单文件(例如，可扩展标记语言(XML)文件)中。此外，白名单文件可安全地提供给工业控制器(例如，在打包和/或传送之前加密，以及由工业控制器解密)。工业控制器在执行特定可执行文件之前，还可提供该特定可执行文件给相同的哈希函数(例如，CRC、MD5、SHA-1或其它合适的哈希函数)，并且可接着确定从哈希函数输出的哈希密钥值是否包括在白名单文件中。如果哈希密钥值位于白名单文件中，那么工业控制器可断定该特定可执行文件经过授权(例如，来自可靠的源头并且自从它被建立以来没有被修改过)并且继续执行该可执行文件。然而，如果该哈希密钥值没有位于白名单文件中，那么工业控制器可阻止该特定可执行文件的执行，并且可把未授权执行的尝试记入日志。通过以这种方式使用列白名单方法，工业控制器12可在执行前有效且同时地验证每个可执行文件的身份和内容。

[0034] 因此，当前公开的实施例可施加若干安全限制(例如，以步进方式)以把工业控制器12从工作的开放模式移到工作的安全模式。图2是根据本公开内容的各方面的过程50的实施例的流程图，工业控制器12可通过过程50从工作的开放模式移到工作的安全模式。过程50始于工业控制器12工作(框52)在开放模式。通常而言，工业控制器12的工作的开放模式既不限制与工业控制器的通信，它也不限制可执行文件由工业控制器的执行。当工作在该开放模式时，工业控制器12可接收(框54)来自配置工具(例如，在设备24上的ToolboxST 32)的指令，以把工业控制器的工作的模式从开放模式改变到安全模式。

[0035] 响应于接收来自配置工具(例如，在设备24上的ToolboxST 32)的使工业控制器12工作在安全模式的指令，工业控制器可切换到工作(框56)在协商模式。通常而言，在协商模式期间，工业控制器12通常可为安全模式工作做准备。例如，转到图3，说明了根据本公开内容的各方面的过程70的实施例的流程图，工业控制器12可在协商模式中执行过程70。协商模式过程70可始于工业控制器12经网络14从证书权限(例如，在安全服务器38上的证书权限44)获得(框72)安全证书。如以下关于图4讨论的，该证书可由工业控制器12稍后用来建立到例如ToolboxST 32的安全(例如，认证的和/或加密的)连接。接着，工业控制器12可禁用(框74)工业控制器12的未认证和/或未加密的网络连接。即，工业控制器12的处理器36可执行禁用与向工业控制器的未认证和/或未加密的通信关联的连接、端口和/或协议的一个或多个指令。例如，在某些实施例中，工业控制器12可禁用到工业控制器12的文件传送协议(FTP)、远程登录和/或任何其它未认证的或明文(plain-text)连接(例如，通过网络14)。此外，工业控制器12可禁用(框76)工业控制器12的本地端口访问(例如，通过本地串行端口登录和/或控制工业控制器12的能力)。

[0036] 另外，作为协商模式过程70的一部分，工业控制器12还可阻止在白名单文件中没有对应条目(entry)的文件的执行(框78)。即，如以上所陈述的，当前工业控制器12的实施例可连同特定软件发布的可执行文件一起接收加密的白名单文件。此外，可执行文件中的一个(例如，启动可执行文件)可包括可用来解密白名单文件的专用密钥值。接着，当特定可执行文件尝试执行时，工业控制器12可比较尝试执行的可执行文件的哈希密钥值与在解密的白名单文件中列出的哈希密钥值。如果可执行文件的哈希密钥值没有位于白名单文件中，那么它可被阻止执行。还应该领会，在协商过程期间，工业控制器12还可验证在工业控制器12进入协商模式之前开始执行的任何可执行文件也经过授权。即，在工业控制器12进入协商模式时，工业控制器12可对当前正在工业控制器12上执行的所有可执行文件执行可执行文件的验证。

[0037] 回到图2，一旦工业控制器12已完成协商模式(框56)，工业控制器12可开始工作(框58)在认证模式。通常而言，认证模式在工业控制器12和配置工具(例如，在设备24上的ToolboxST 32)之间建立安全(例如，认证的和/或加密的)通信。例如，转到图4，说明了根据本公开内容的各方面的过程90的实施例的流程图，工业控制器12可在认证模式中执行过程90。说明的过程90始于工业控制器12接收(框92)来自配置工具(例如，ToolboxST 32)的请求以建立到工业控制器12的认证和/或加密连接(例如，安全套接字层(SSL)连接)。过程90继续，其中工业控制器12在配置工具(例如，ToolboxST 32)和工业控制器12之间建立(框94)认证和/或加密连接。

[0038] 再一次转到图2，在工业控制器12已完成认证模式(框58)后，工业控制器12可开始

工作(框60)在安全模式。应该领会,在协商模式和认证模式期间(例如,如图3和4所叙述的)施加在工业控制器上的安全限制可继续在安全模式中应用。即,在工业控制器12正工作在安全模式时,向工业控制器的认证的和/或未加密的通信(例如,FTP、远程登录、本地端口通信)可被禁止,并且可与白名单文件对照验证所有可执行文件以确保它们在执行之前经过授权。还应该领会,在整个功率循环和/或软件升级中,安全模式可在工业控制器12中持续。例如,在某些实施例中,在工业控制器12正在重新引导时,可遇到存储器中的变量指示在功率循环之前正使工业控制器12工作在安全模式。如此,在重新引导过程期间,工业控制器12通常可执行协商模式的动作(例如,图3的过程70)以应用需要的安全限制(例如,在工业控制器12开始控制工业控制系统10之前)。因此,工业控制器12可开始安全模式中的操作(例如,仅接受来自ToolboxST 32的加密连接并且仅执行授权的可执行文件)。

[0039] 该公开内容的技术效果包括对工业控制系统10的整体安全的提高。即,当前公开的实施例实现使工业控制器12工作在安全模式,该安全模式通常可阻止未授权可执行文件的执行和/或阻止由未授权人员或系统对工业控制器的访问。另外,当前公开的实施例通过对工业控制器12逐渐地应用若干安全限制,使得工业控制器12能够从开放模式(例如,没有限制)移到安全模式(例如,有额外安全限制)。通过使工业控制器12能够工作在持续于工业控制器12的各种活动(例如,功率循环、软件下载和/或软件升级)的安全模式,当前公开的实施例一般提供了具有未授权访问和/或未授权指令执行的降低风险的工业控制系统10。

[0040] 该书面描述使用示例公开包括最好模式的本发明,并且还使本领域的任何技术人员能够实践本发明,包括制造和使用任何设备或系统以及执行任何结合的方法。本发明可授予专利的范围由权利要求书限定,并且可包括本领域技术人员所想到的其它示例。此类其它示例意图在权利要求书的范围之内,如果它们具有与权利要求书的字面语言没有不同的结构要素的话,或者如果它们包括与权利要求书的字面语言没有实质性差别的等价结构要素的话。

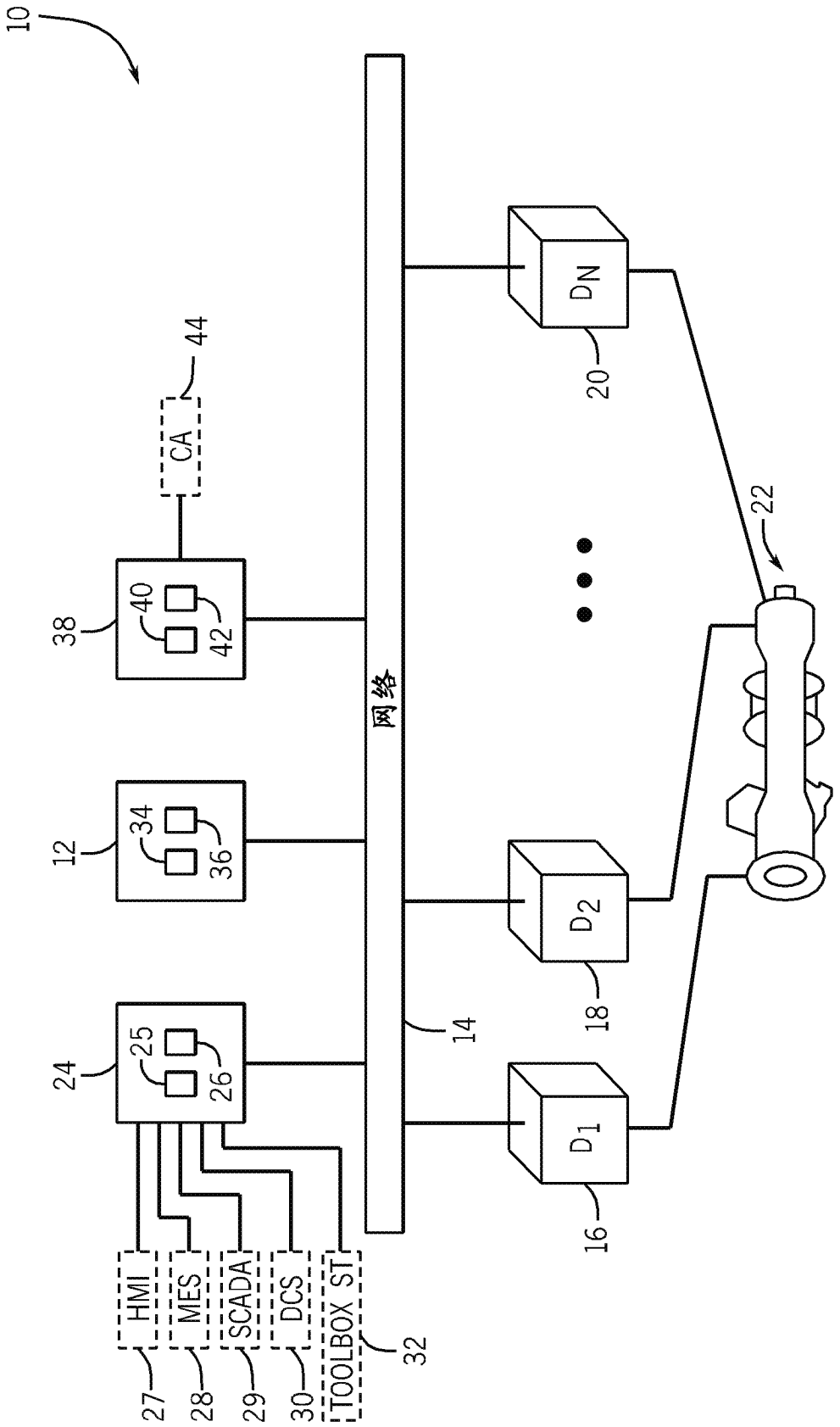

10
网络
DN
20
22
CA
44
38
40
42
12
34
36
24
25
26
D2
18
14
D1
16
HMI
MES
SCADA
DCS
TOOLBOX ST
27
28
29
30
32

图 1

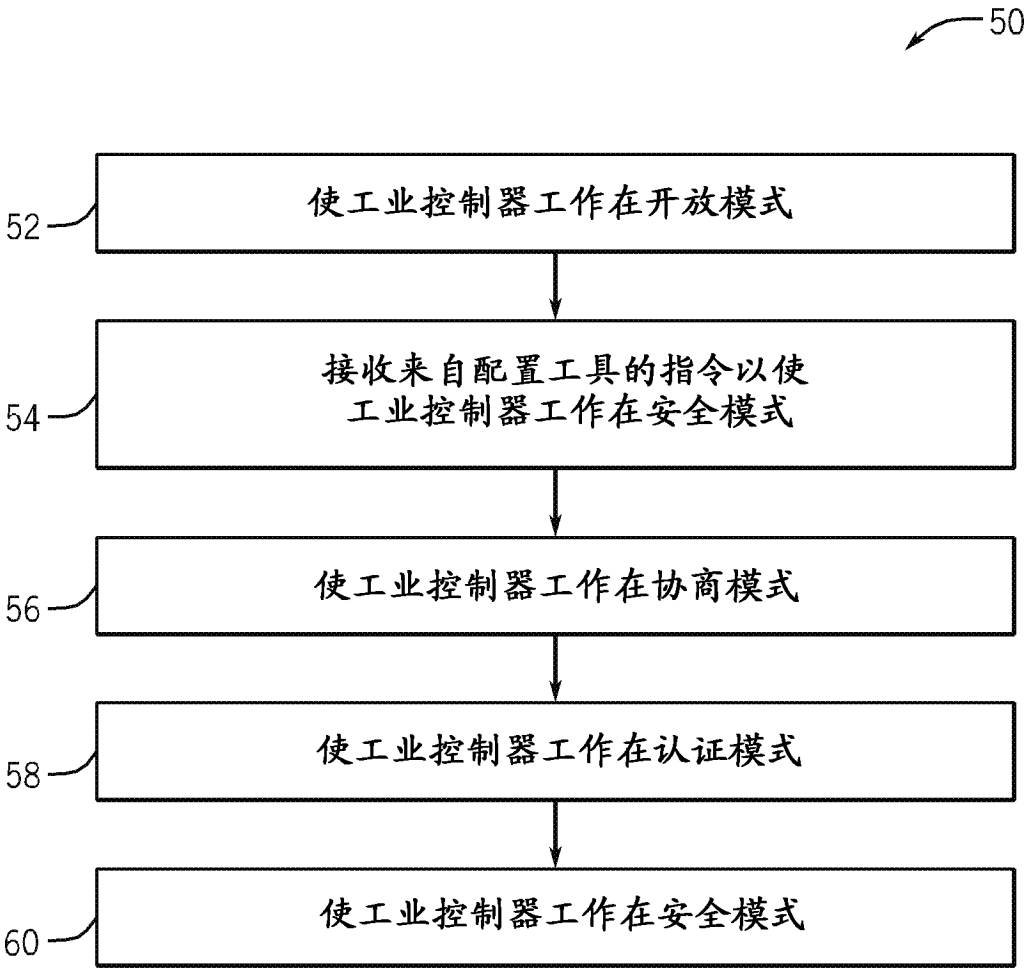

50
52
使工业控制器工作在开放模式
54
接收来自配置工具的指令以使
工业控制器工作在安全模式
56
使工业控制器工作在协商模式
58
使工业控制器工作在认证模式
60
使工业控制器工作在安全模式

图 2

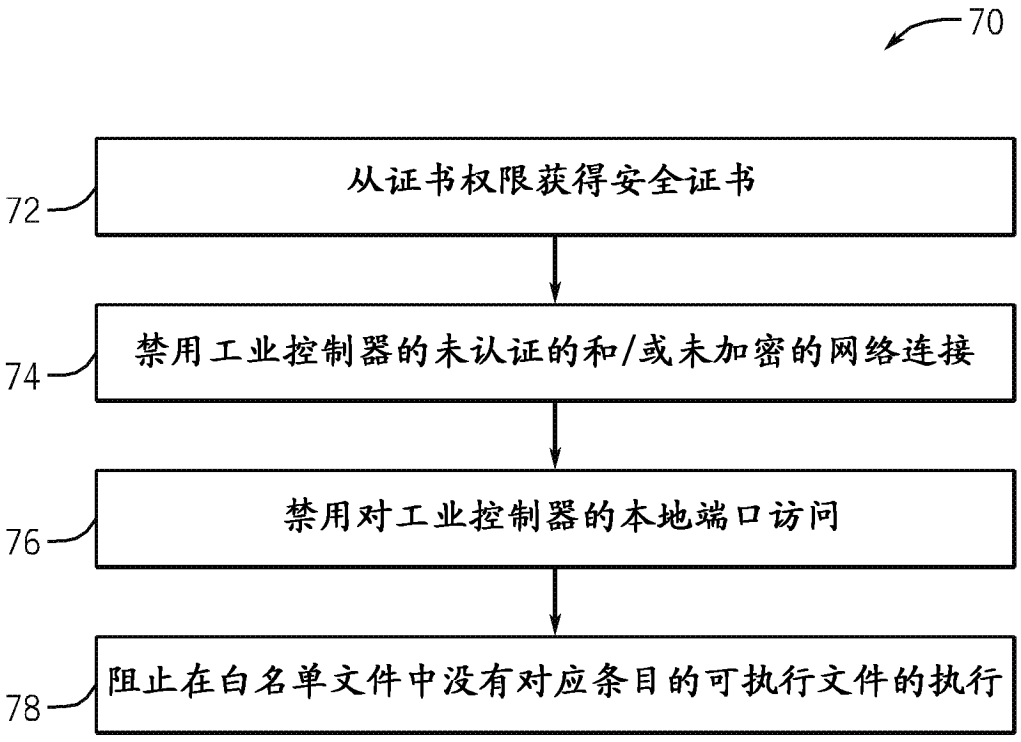

70
72
从证书权限获得安全证书
74
禁用工业控制器的未认证的和/或未加密的网络连接
76
禁用对工业控制器的本地端口访问
78
阻止在白名单文件中没有对应条目的可执行文件的执行

图 3

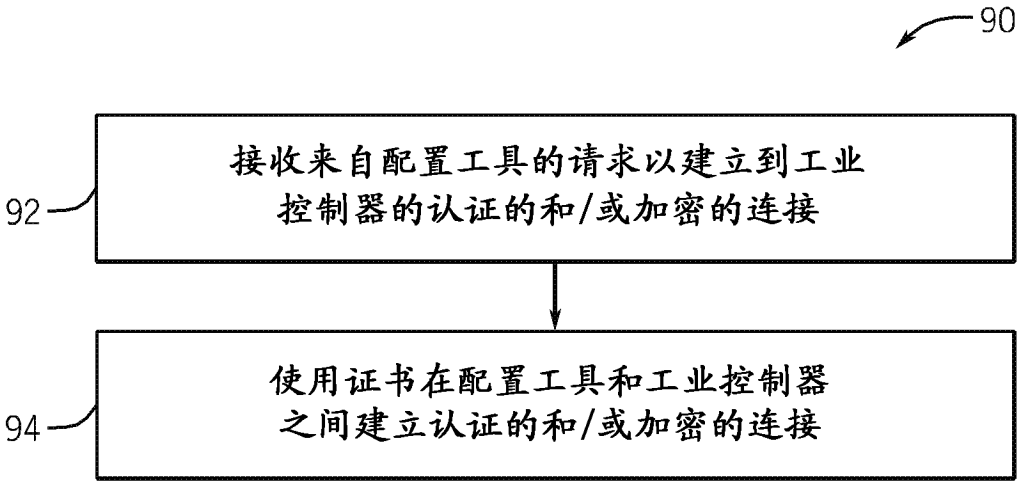

90
92
接收来自配置工具的请求以建立到工业控制器的认证的和/或加密的连接
94
使用证书在配置工具和工业控制器之间建立认证的和/或加密的连接

图 4