(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 103376794 B
(45)授权公告日 2017.06.20

(21)申请号 201310154427.2

(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 103376794 A

(43)申请公布日 2013.10.30

(30)优先权数据
13/460779 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 M.R.萨胡

(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 19/418(2006.01)
G05B 19/048(2006.01)

(56)对比文件
US 2009254655 A1,2009.10.08,
US 2003131096 A1,2003.07.10,
US 2002021791 A1,2002.02.21,
US 7047276 B2,2006.05.16,
US 2002193888 A1,2002.12.19,

审查员 张姗姗

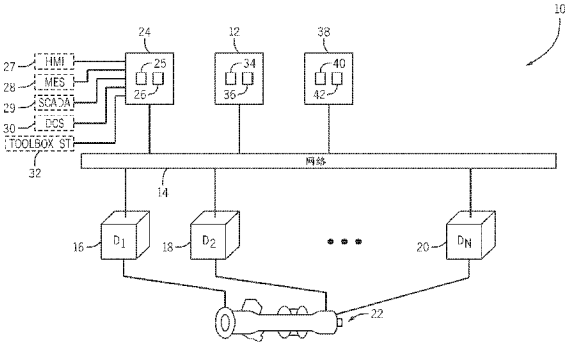
权利要求书2页 说明书9页 附图3页

(54)发明名称

用于把工业控制系统的安全事件记入日志的系统和方法

(57)摘要

一种系统包括包含存储器和处理器的安全服务器，安全服务器配置成接收来自人机界面(HMI)设备的第一组通信，其中第一组通信涉及HMI设备安全事件。安全服务器还配置成接收来自工业控制器的第二组通信，其中第二组通信涉及工业控制器安全事件。安全服务器还配置成打包并且发送接收的第一组和第二组通信给远程管理安全服务提供商(MSSP)用于分析。



CN 103376794 B

1.一种工业控制系统,包括:

包括存储器和处理器的安全服务器,配置成:

接收来自人机界面(HMI)设备的第一组通信,其中,所述第一组通信涉及HMI设备安全事件;

接收来自工业控制器的第二组通信,其中,所述第二组通信涉及工业控制器安全事件;

在所述安全服务器和位于工业控制系统之外的远程管理安全服务提供商(MSSP)建立网络连接;

打包并且发送所接收的第一组和第二组通信给远程管理安全服务提供商(MSSP)用于分析;通过所述网络连接接收来自远程管理安全服务提供商的安全警报,所述安全警报描述由远程管理安全服务提供商在分析第一和第二组通信时识别出的安全问题;以及

指示人机界面将所述安全警报提供给用户。

2.如权利要求1所述的系统,包括:具有另外存储器和另外处理器的所述HMI设备,配置成:

允许授权用户登录到所述HMI设备;

在所述HMI设备上执行配置工具;以及

提供涉及所述HMI设备安全事件的所述第一组通信给所述安全服务器。

3.如权利要求2所述的系统,其中,所述配置工具配置成提供指令给所述工业控制器以设置或强加在所述工业控制器上的变量,以上载可执行文件到所述工业控制器,或两者。

4.如权利要求3所述的系统,其中,所述HMI设备安全事件涉及:尝试登录到所述HMI设备,在所述HMI设备上启动所述配置工具,在所述HMI设备上执行一组指令,尝试从所述HMI设备设置所述工业控制器的变量,从所述HMI设备上载可执行文件到所述工业控制器,或它们的组合。

5.如权利要求1所述的系统,包括:具有另外存储器和另外处理器的所述工业控制器,配置成:

执行多个可执行文件以控制工业自动化系统;

接收和执行由所述HMI设备的配置工具提供的指令;以及

提供涉及所述工业控制器安全事件的所述第二组通信给所述安全服务器。

6.如权利要求5所述的系统,其中,所述工业控制器安全事件涉及设置所述工业控制器的变量或下载可执行文件到所述工业控制器或两者。

7.如权利要求5所述的系统,其中,所述工业控制器安全事件涉及重新引导、启动失败、通信错误或检测到未授权的可执行文件,或它们的组合。

8.如权利要求1所述的系统,包括:具有另外存储器和另外处理器的所述远程MSSP,配置成:

接收和比较所述第一组和第二组通信;

在所述第一组和第二组通信中识别趋势;以及

当某些趋势在所述第一组和第二组通信中被识别时,提供安全警报给所述安全服务器。

9.如权利要求8所述的系统,其中,所述安全服务器配置成:在所述远程MSSP确定在所述系统中存在安全问题时,接收来自所述远程MSSP的所述安全警报。

10.如权利要求1所述的系统，包括具有所述安全服务器的工业系统，其中，所述工业系统包括：气化系统，气体处理系统，涡轮系统，发电系统，热量回收蒸汽发生(HRSG)系统，或它们的组合。

11.一种方法，包括：

采用工业控制系统中的安全服务器聚集安全日志，所述安全日志包括工业控制系统中多个设备的安全事件；

在所述安全服务器和位于工业控制系统之外的远程管理安全服务提供商(MSSP)建立网络连接；

打包并且通过网络连接发送所聚集的安全日志给管理安全服务提供商(MSSP)，其中所述MSSP配置成在所述安全日志中确定趋势，以及

通过所述网络连接接收来自远程管理安全服务提供商的安全警报，所述安全警报描述由远程管理安全服务提供商在分析第一和第二组通信时识别出的安全问题；以及

指示工业控制系统的多个设备中的一个将所述安全警报提供给用户。

12.如权利要求11所述的方法，其中，所述多个设备包括配置成控制所述工业系统的工业控制器。

13.如权利要求12所述的方法，其中，所述安全事件涉及：设置所述工业控制器的变量，下载可执行文件到所述工业控制器，所述工业控制器的重新引导，所述工业控制器的启动失败，所述工业控制器的通信错误，或由所述工业控制器对未授权可执行文件的检测，或它们的组合。

14.如权利要求12所述的方法，其中，所述多个设备包括配置成设置在所述工业控制器上的变量并且配置成上载可执行代码到所述工业控制器的人机界面(HMI)设备。

15.如权利要求14所述的方法，其中，所述安全事件涉及：尝试登录到所述HMI设备，在所述HMI设备上执行一组指令，尝试从所述HMI设备设置所述工业控制器的变量，或从所述HMI设备上载可执行文件到所述工业控制器，或它们的组合。

16.如权利要求11所述的方法，其中，打包所聚集的安全日志包括：把所接收的安全日志打包成档案文件，压缩所述安全日志，加密所述安全日志，或它们的任意组合。

17.如权利要求11所述的方法，包括：当所述多个设备中的两个的安全日志被所述MSSP确定为不互相一致时，接收来自所述MSSP的安全警报。

用于把工业控制系统的安全事件记入日志的系统和方法

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。另外，其它设备，比如人机界面(HMI)设备，可耦合到工业控制系统以提供接口，通过该接口用户可控制工业控制器和工业控制系统的工作。

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，一种系统包括包含处理器和存储器的安全服务器，安全服务器配置成接收来自人机界面(HMI)设备的第一组通信，其中第一组通信涉及HMI设备安全事件。安全服务器还配置成接收来自工业控制器的第二组通信，其中第二组通信涉及工业控制器安全事件。安全服务器还配置成打包并发送接收的第一组和第二组通信给远程管理安全服务提供商(MSSP:managed security service provider)用于分析。

[0005] 在第二个实施例中，一种方法包括聚集(aggregate)包括与工业系统关联的多个设备的安全事件的安全日志。该方法还包括打包并发送聚集的安全日志给管理安全服务提供商(MSSP)，其中MSSP配置成在安全日志中确定趋势。

[0006] 在第三个实施例中，一种有形的、非暂时的(non-transitory)机器可读介质配置成存储可由电子设备的处理器执行的指令。指令包括接收来自人机界面(HMI)设备和工业控制器的安全通知的指令，其中HMI设备配置成执行提供指令给工业控制器的配置工具。指令还包括发送接收的安全通知给远程处理器的指令，其中远程处理器配置成分析和比较来自HMI设备和工业控制器的安全通知。指令还包括当远程处理器基于安全通知指示HMI设备、工业控制器或两者存在安全问题时提供警报的指令。

[0007] 根据本发明的第一方面，提供一种方法，包括：聚集包括与工业系统关联的多个设备的安全事件的安全日志；以及 打包并且发送所聚集的安全日志给管理安全服务提供商(MSSP)，其中所述MSSP配置成在所述安全日志中确定趋势。

[0008] 根据本发明第一方面的方法，其中，所述多个设备包括配置成控制所述工业系统的工业控制器。

[0009] 根据本发明第一方面的方法，其中，所述安全事件涉及：设置所述工业控制器的变量，下载可执行文件到所述工业控制器，所述工业控制器的重新引导，所述工业控制器的启动失败，所述工业控制器的通信错误，或由所述工业控制器对未授权可执行文件的检测，或它们的组合。

[0010] 根据本发明第一方面的方法，其中，所述多个设备包括配置成设置在所述工业控制器上的变量并且配置成上载可执行代码到所述工业控制器的人机界面(HMI)设备。

[0011] 根据本发明第一方面的方法，其中，所述安全事件涉及：尝试登录到所述HMI设备，在所述HMI设备上执行一组指令，尝试从所述HMI设备设置所述工业控制器的变量，或从所述HMI设备上载可执行文件到所述工业控制器，或它们的组合。

[0012] 根据本发明第一方面的方法，其中，打包所聚集的安全日志包括：把所接收的安全日志打包成档案文件，压缩所述安全日志，加密所述安全日志，或它们的任意组合。

[0013] 根据本发明第一方面的方法，包括：当所述多个设备中的两个的安全日志被所述MSSP确定为不互相一致时，接收来自所述MSSP的安全警报。

[0014] 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，配置成存储可由电子设备的处理器执行的指令，所述指令包括：接收来自人机界面(HMI)设备和工业控制器的安全通知的指令，其中，所述HMI设备配置成执行提供指令给所述工业控制器的配置工具；发送所接收的安全通知给远程处理器的指令，其中，所述远程处理器配置成分析和比较来自所述HMI设备和所述工业控制器的所述安全通知；以及当所述远程处理器基于所述安全通知指示所述HMI设备、所述工业控制器或两者存在安全问题时提供警报的指令。

[0015] 根据本发明第二方面的介质，其中，所述远程处理器配置成使用至少一个试探法分析来自所述HMI设备和所述工业控制器的所述安全通知以在所述安全通知中确定趋势。

[0016] 根据本发明第二方面的介质，其中，所述远程处理器配置成：当在所述安全通知中的所述趋势指示安全问题时，通报所述HMI设备。

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是根据当前公开内容的各方面的具有工业控制器、人机界面(HMI)设备和安全服务器的工业控制系统的实施例的示意图；

[0019] 图2是根据当前公开内容的各方面说明安全服务器管理HMI设备安全事件和工业控制器安全事件的实施例的混合流程图；

[0020] 图3是根据当前公开内容的各方面的过程的实施例的流程图，通过该过程安全服务器把来自工业控制系统的安全事件聚集、打包并发送给管理安全服务提供商(MSSP)用于分析；以及

[0021] 图4是根据当前公开内容的各方面的过程的实施例的流程图，通过该过程MSSP分析工业控制系统的安全事件以在安全事件中识别某些趋势。

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之间可不同。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。此外，如本文所使用的，术语“白名单(whitelist)”可指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的文件。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] 通常可需要跟踪工业控制系统的各个部件的某些活动以确保部件按预期运转。因而，当前实施例包括安全服务器，其耦合到工业控制系统以便聚集与工业控制系统的部件的各个涉及安全的活动有关的安全通知。另外，某些公开的安全服务器实施例还可把聚集的安全通知打包并传送到远程设备，比如由工业控制系统的管理安全服务提供商(MSSP)托管(host)并且维护的设备，以供比较和分析。此外，远程设备的处理器可比较和分析接收自安全服务器的工业控制系统的各个安全通知，以便在安全通知内识别可指向工业控制系统内的安全问题的趋势。因而，远程设备可通知(例如，提供安全警报给)安全服务器，并且可能通知HMI设备，关于工业控制系统内的安全问题，使得它们可被处理。

[0025] 牢记前述，图1是说明工业控制系统10的示意图。所说明的工业控制系统10包括工业控制器12。另外，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)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(sub-bus)，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安装到工业控制网络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(例如，使用以下讨论的设备24)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)或设置。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不同版本。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网络中的一个或多个设备上。

[0030] 此外，所说明的工业控制系统10的部分，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)。通常而言，安全服务器38可执行若干关于工业控制系统10的安全的功能。例如，在某些实施例中，安全服务器38可负责托管可发出和撤回证书的证书权限(CA)，证书用于当某些部件(例如，工业控制器12、设备24上的ToolboxST 32、或工业控制系统10的其它部件)在网络14上通信时通过实现身份验证以及加密通信通道以安全方式在网络14上通信。

[0031] 此外，安全服务器38可接收来自工业控制系统10的各个部件的安全通知。在特定部件(比如，工业控制系统10的工业控制器12)的工作期间，工业控制器12可生成与例如以

下有关的安全通知：由工业控制器12执行的各个任务、访问和/或登录工业控制器12的尝试、由工业控制器12接收的指令和/或在工业控制器12工作期间遇到的错误。安全通知最初可存储在工业控制器12的存储器34中，并且可随后传递到安全服务器38（例如，通过网络14）。在某些实施例中，工业控制器12可在安全通知发生时提供安全通知给安全服务器38（例如，以基本上实时的方式），而在其它实施例中，工业控制器12可收集某个数目（例如，2、3、4、5、10、20或其它合适数目）的安全通知，然后将其提供给安全服务器38。类似地，在某些实施例中，设备24（例如，设备24上的HMI 27和/或ToolboxST 32）也可提供例如涉及以下的安全通知给安全服务器38：由设备24执行的各个任务、访问和/或登录设备24的尝试、由设备24接收的来自用户的指令、由设备24提供给工业控制器12的指令和/或在设备24（例如，设备24上的HMI 27和/或ToolboxST 32）工作期间遇到的错误。实际上，工业控制系统10的各个设备，包括例如现场设备16、18和20，中的任何设备可提供安全通知给安全服务器38。

[0032] 为了进一步说明安全服务器38的工作，图2是说明在工业控制系统10中安全服务器38管理HMI设备安全事件50和工业控制器安全事件52的实施例的混合流程图。更具体地，图2说明设备24（例如，托管HMI 27和/或ToolboxST 32）和工业控制器12互相通信耦合（由箭头54指示），使得设备24一般可为用户提供访问和控制工业控制器12的接口。在设备24（例如，设备24上的HMI 27和/或ToolboxST 32）的整个工作期间，若干HMI安全事件50可生成并且随后传递给安全服务器38（例如，通过网络14）。此外，在工业控制器12的工作期间，若干工业控制器安全事件52可生成并且随后传递给安全服务器38（例如，通过网络14）。应该领会，表示图2的HMI安全事件50以及图2的工业控制器安全事件52的要素包括可在可产生安全通知供安全服务器38稍后消耗的设备24和工业控制器12的各自工作期间遇到的安全事件的示例的非限制性列表。

[0033] 特别地，如图2所示，潜在的HMI安全事件50的一个涉及用户尝试登录到设备24。因此，在用户尝试登录到设备24、HMI 27和/或ToolboxST 32时，设备24可生成并且提供对应于HMI安全事件的安全通知给安全服务器38。此外，提供给安全服务器38的这些安全通知可包括关于HMI安全事件的信息（例如，时间戳、用户名、各个机器和/或用户标识符、成功或失败的指示、在给定时段中尝试的数目或其它合适的信息）。类似地，在软件由设备24的处理器26执行（例如，基于来自用户的指令）时，设备24也可生成包括关于HMI安全事件的信息（例如，时间戳、正被执行的软件的名称、正被执行的软件的哈希密钥值、各个机器和/或用户标识符或其它合适信息）的安全通知。按照具体示例，当在设备24上启动（例如，开始执行）配置工具（比如ToolboxST 32）时，设备24可生成HMI安全通知。

[0034] 此外，在设备24尝试设置或强加（force）工业控制器12的变量时，设备24可生成HMI安全事件。即，工业控制器12可包括存储在工业控制器12的存储器34中的若干变量，其通常可定义工业控制系统10的参数（例如，燃气涡轮系统22的各个部件的可接受温度、压力或电压范围）。因而，用户可利用设备24（例如，HMI 27和/或ToolboxST 32）的接口以指示工业控制器12把特定变量设置或强加为指定值。此外，在设备24指示工业控制器12设置或强加特定变量时，设备24可生成待发送给安全服务器38的详细说明关于HMI安全事件的信息（例如，时间戳、用户的标识信息、机器和/或正被设置的变量、变量的指定值、变量的当前或先前值或其它合适信息）的安全通知。此外，在某些实施例中，用户可利用设备24（例如，设备24上的HMI 27和/或ToolboxST 32）的接口以上载可执行文件到工业控制器12的存储器

34，供工业控制器12的处理器36稍后执行。因而，在设备24提供可执行文件给工业控制器12时，设备24还可向安全服务器38提供包括关于HMI安全事件的信息(例如，时间戳、用户的标识信息、机器和/或正被传递的可执行文件、正被传递的可执行文件的哈希密钥值或其它合适信息)的安全通知。

[0035] 另外，如图2所示，工业控制器12还可响应于某些工业控制器安全事件52生成并且提供安全通知给安全服务器38。例如，潜在的工业控制器安全事件52的一个可在用户和/或系统尝试登录到工业控制器12时发生。因此，在用户和/或设备尝试登录到工业控制器12(例如，通过设备24上的HMI 27或ToolboxST 32)时，工业控制器12可生成对应于工业控制器安全事件的安全通知，并且接着提供安全通知给安全服务器38。此外，提供给安全服务器38的安全通知可包括关于工业控制器安全事件的信息(例如，时间戳、用户名、各个机器和/或用户标识符、成功或失败的指示、在给定时段中尝试的数目或其它合适信息)。另外，如以上陈述的，工业控制器12可接收指令(例如，来自设备24的HMI 27和/或ToolboxST 32)以在工业控制器12的存储器34中设置或强加变量。因此，在接收到指令时，工业控制器12可为工业控制器安全事件生成包括关于工业控制器安全事件的信息(例如，时间戳、用户的标识信息、机器和/或正被设置的变量、变量的指定值、变量的当前或先前值或其它合适信息)的安全通知。

[0036] 此外，如以上陈述的，工业控制器12可不时地接收来自另外系统(例如，设备24上的HMI 27和/或ToolboxST 32)的可执行文件，供在存储器34中存储和由工业控制器12的处理器36执行。因而，在工业控制器12接收来自设备24的可执行文件时，工业控制器12还可向安全服务器38提供包括关于工业控制器安全事件的信息(例如，时间戳、用户的标识信息、机器和/或正被传递的可执行文件、正被传递的可执行文件的哈希密钥值或其它合适信息)的安全通知。工业控制器安全事件52的其它示例包括：工业控制器12的重新引导、工业控制器12启动或引导的失败以及由工业控制器12遇到的通信错误。在某些实施例中，工业控制器12可工作在若干不同模式(例如，开放非限制模式和安全限制模式)，并且在改变工作的模式(例如，从开放模式到安全模式)时工业控制器12可生成安全通知。对于所有此类工业控制器安全事件52，工业控制器12通常可在关联的安全通知中提供关于安全事件的相关信息给安全服务器38。

[0037] 另外，在某些实施例中，工业控制器12可在存储器34中存储白名单文件，作为规定允许哪些可执行文件在工业控制器12的处理器36上执行的方法。即，在工业控制器12接收新的可执行文件(例如，从设备24)时，它还可接收包括每个授权可执行文件的哈希密钥值(例如，诸如循环冗余校验(CRC)、消息摘要算法(MD：Message-Digest Algorithm)、安全哈希算法(SHA)或其它合适哈希函数的哈希函数的输出)的白名单文件。因此，在某些实施例中，工业控制器12的处理器36可确定正在尝试执行的特定可执行文件的哈希密钥值，并且接着工业控制器12可检查白名单文件以确定尝试执行的特定可执行文件是否被授权。即，如果特定可执行文件的所确定哈希密钥值位于白名单文件中，那么可认为该可执行文件授权由处理器36执行。然而，如果尝试执行的特定可执行文件的所确定哈希密钥值没有位于白名单文件中，那么工业控制器12可确定该特定可执行文件没有被授权执行。此外，在工业控制器12确定工业控制器12的存储器34中的任何可执行文件没有被授权时，则工业控制器安全事件可发生。因此，工业控制器12可生成并且提供包括关于工业控制器安全事件的信

息(例如,时间戳、尝试执行的可执行文件的标识信息、白名单文件的标识信息、尝试执行的可执行文件的哈希密钥值或其它合适信息)的安全通知给安全服务器38。

[0038] 因此,如图2所示,安全服务器38通常可接收来自工业控制系统10的若干不同部件(例如,设备24、工业控制器12和其它合适的设备)的安全通知。在某些实施例中,在聚集工业控制系统10的各个部件的安全通知时,安全服务器38可把从各个部件接收的安全通知存储在安全服务器38的存储器40中。此外,在某些实施例中,安全服务器38可比较和分析从工业控制系统10的各个部件接收的安全通知。

[0039] 例如,应该领会,若干说明的工业控制器安全事件52是通常可与某些HMI安全事件50互补的安全事件。因而,该特征将导致将相应的和/或互补的安全通知从工业控制系统10的多个部件提供给安全服务器38。因此,在某些实施例中,例如,安全服务器38可比较由设备24和工业控制器12提供的相应安全通知以便验证一致性。即,例如,安全服务器38的处理器40可确保由设备24响应于用户尝试设置或强加工业控制器12的变量而提供的安全通知,对应于由工业控制器12在接收设置或强加该变量的请求时提供的互补安全通知。另外,除了检查内部一致性之外,安全服务器38的处理器40可应用各种试探法(heuristics)以在由工业控制系统10的各个部件提供的安全通知中确定趋势。例如,安全服务器38可把试探法应用到安全通知以确定:安全事件倾向于发生的日、周、月、年等的时间,工业控制系统10的哪些部件最可能产生安全通知,哪些部件最可能触发安全通知和工业控制系统10的其它部件等。

[0040] 然而,在某些实施例中,额外地或备选地,可需要提供由安全服务器38聚集的安全通知给远程设备用于比较和分析。例如,在某些实施例中,工业控制系统10可由管理安全服务提供商(MSSP)支持,MSSP通常可为工业控制系统10的各个安全方面提供支持。此外,MSSP可操作具有存储器58和处理器60的远程设备56(例如,位于工业控制系统10的外面),其通常可接收关于工业控制系统10内安全问题的信息。例如,远程设备56可接收由安全服务器38聚集的安全通知,以便比较和分析工业控制系统10的安全通知。如以上针对安全服务器38所陈述的,远程设备56可比较相应的和/或互补的安全通知以验证一致性,并且还可应用试探法以在工业控制系统10的安全通知中确定趋势。

[0041] 此外,对于利用远程设备56以比较和分析工业控制系统10的安全通知的实施例,安全服务器38可在传递安全通知给远程设备56之前对其进行打包。例如,在某些实施例中,安全服务器38可添加若干安全通知到单个文件和/或文件的档案以便于传送。另外,在某些实施例中,安全服务器38可在传送之前额外地对安全通知(例如,包含安全通知的文件和/或档案)进行压缩以减小文件大小。此外,在某些实施例中,安全服务器38可额外地加密安全通知,使得安全通知可安全地传送到远程设备56。在其它实施例中,额外地或备选地,安全服务器38可利用加密的网络连接62来传送安全通知给远程设备56。

[0042] 转到图3,提出了说明过程70的实施例的流程图,安全服务器38可通过过程70从工业控制系统10的部件收集安全通知并且提供安全通知给远程设备56用于处理。过程70始于安全服务器38的处理器40接收(框72)并存储(例如,在存储器40中)来自HMI设备(例如,设备24)的HMI设备安全通知。在基本上同一时间,安全服务器38的处理器40还可接收(框74)并存储(例如,在存储器40中)来自工业控制器12的工业控制器安全通知。应该领会,安全服务器38可接收来自工业控制系统10中任何合适设备的安全通知。随后,安全服务器38可把

接收的安全通知打包(框76)成档案，安全服务器38可压缩安全通知并且/或者安全服务器38可加密安全通知。接着，安全服务器38可发送(框78)打包的安全通知给远程设备56用于比较和分析。在其它的实施例中，额外地或备选地，安全服务器38可使用处理器42来比较和分析安全通知。此外，在某些实施例中，备选地，安全服务器38可直接发送安全通知给远程设备56，与它们在没有任何实质打包的情况下被接收一样。

[0043] 转到图4，说明了过程80的实施例的流程图，远程设备56可通过过程80接收和分析来自工业控制系统10的安全通知。过程80始于远程设备56的处理器60接收(框82)来自工业控制系统10的安全服务器38的多个安全事件。一旦接收到，远程设备56的处理器58可为工业控制系统10中的一致性而继续比较(框84)相应的和/或互补的安全事件。另外，远程设备56的处理器58可使用(框86)各种试探法以在多个安全事件内识别趋势。

[0044] 此外，在某些实施例中，当在安全事件内识别到某些趋势时，远程设备56还可通知(框88)安全服务器38和/或设备24(例如，HMI 27和/或ToolboxST 32)。例如，一旦远程系统56基于安全通知的分析已识别潜在的安全问题，远程设备56可通知安全服务器38安全问题。按照具体示例，远程设备56的处理器58可基于接收的安全通知的比较和/或分析确定特定未授权可执行文件正循环地(on a recurring basis)在某时间段期间尝试执行。因此，远程设备56可通过安全警报通知安全服务器38和/或设备24安全问题，安全警报通常可描述安全问题并且建议潜在的解决方案。例如，远程设备56可向工业控制系统10(例如，工作控制系统10的安全服务器38和/或HMI 27)提供安全警报，其包括：违规的(offending)可执行文件的身份，对违规的可执行文件何时尝试执行的所识别趋势以及来自安全通知和/或安全通知的分析的其它合适信息。应该领会，在其中安全通知的比较和/或分析由安全服务器38单独执行的实施例中，安全服务器38可通过安全警报以类似方式通知设备24(例如，设备24的HMI 27和/或ToolboxST 32)任何识别的安全问题。

[0045] 当前实施例的技术效果包括安全通知从工业控制系统10的若干不同部件到集中安全服务器38的聚集。此外，安全服务器38的当前实施例可提供安全通知的比较和/或分析、安全通知的打包(例如，包括压缩和/或加密)、传送安全通知给远程设备、接收来自远程设备的安全警报以及提供安全警报给HMI 27以通知HMI 27的一个或多个用户安全问题。另外，远程设备56的当前实施例可实现从远程设备56比较和/或分析工业控制系统10的安全通知，以及基于安全通知的比较和/或分析提供安全警报给安全服务器38和/或HMI 27。

[0046] 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。本发明的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。

[0047] 部件清单：

[0048]

10	工业控制系统
12	工业控制器
14	网络

16	现场设备
18	现场设备
20	现场设备
22	燃气涡轮系统
24	设备
25	存储器
26	处理器
27	HMI系统
29	SCADA系统
32	ToolboxST
34	存储器
36	处理器
38	安全服务器
40	存储器
42	处理器
50	HMI设备安全事件
52	工业控制器安全事件
54	箭头
56	远程设备
58	存储器
60	处理器
62	加密的网络连接
70	过程
72	接收来自HMI设备的通知
74	接收来自工业控制器的通知
76	打包通知
78	发送通知
80	过程
82	接收来自安全服务器的通知
84	比较通知
86	使用试探法识别趋势
88	通知安全服务器

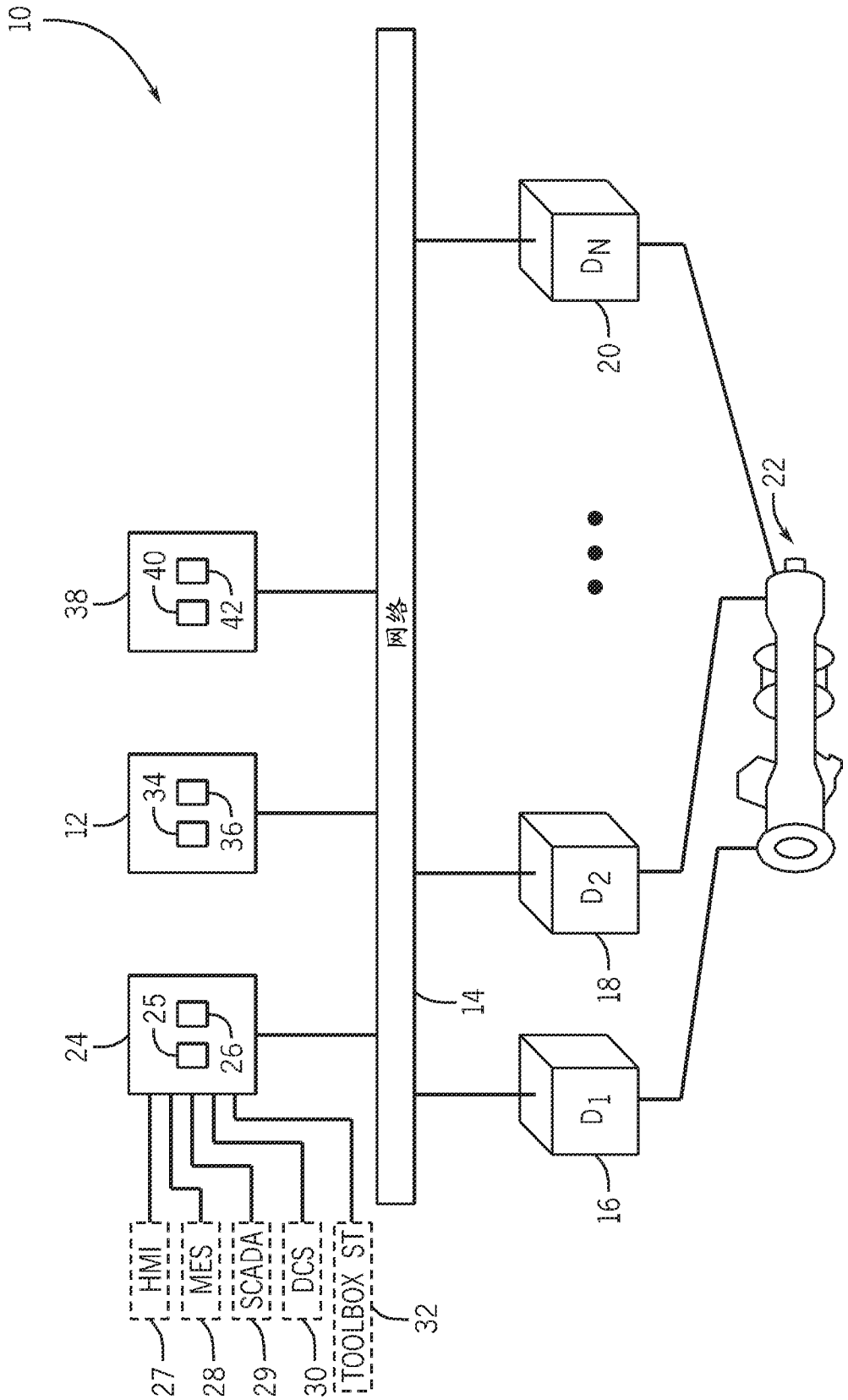

10
网络
DN
20
22
38
40
42
12
34
36
D2
18
24
25
26
14
D1
16
HMI
MES
SCADA
DCS
TOOLBOX ST
27
28
29
30
32

图 1

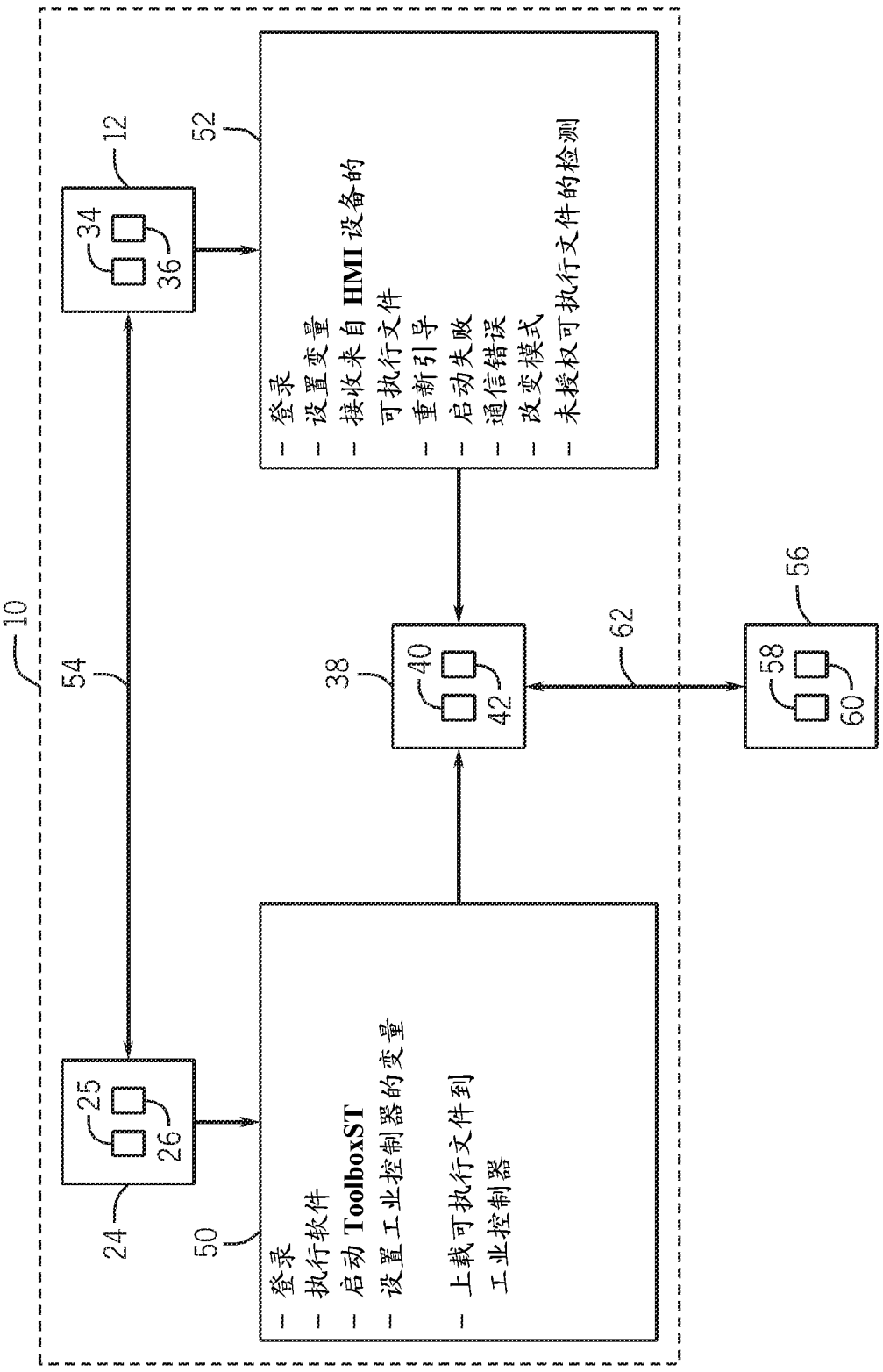

10
12
24
25
26
34
36
38
40
42
50
52
54
56
58
60
62
登录
执行软件
启动 ToolboxST
设置工业控制器的变量
上载可执行文件到
工业控制器
登录
设置变量
接收来自 HMI 设备的
可执行文件
重新引导
启动失败
通信错误
改变模式
未授权可执行文件的检测

图 2

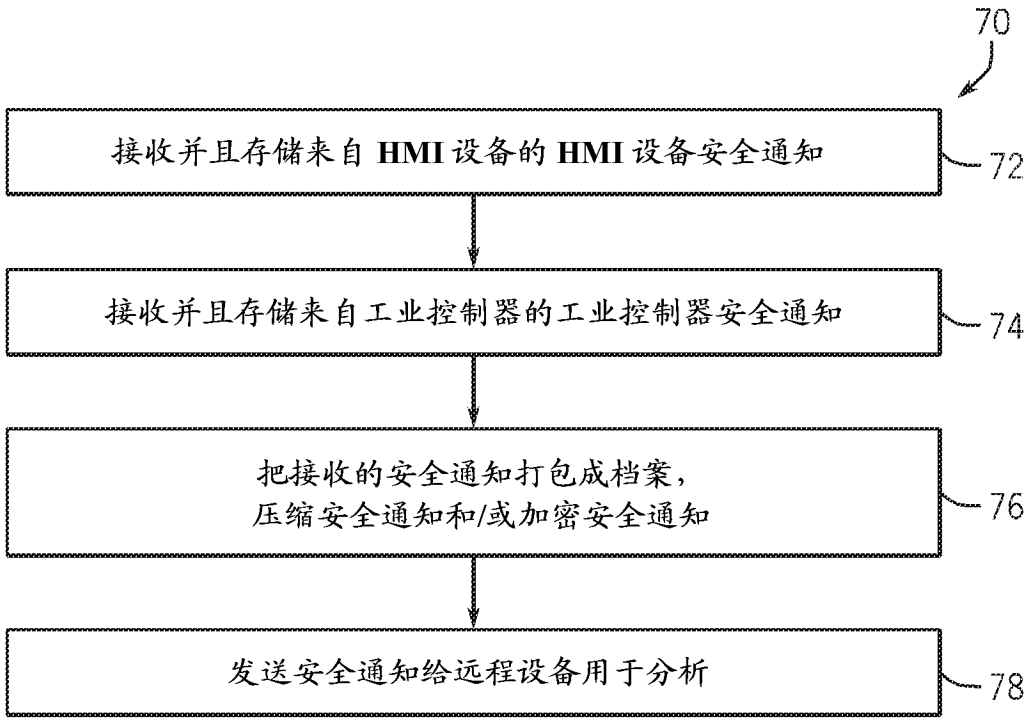

70
接收并且存储来自 HMI 设备的 HMI 设备安全通知
72
接收并且存储来自工业控制器的工业控制器安全通知
74
把接收的安全通知打包成档案，
压缩安全通知和/或加密安全通知
76
发送安全通知给远程设备用于分析
78

图 3

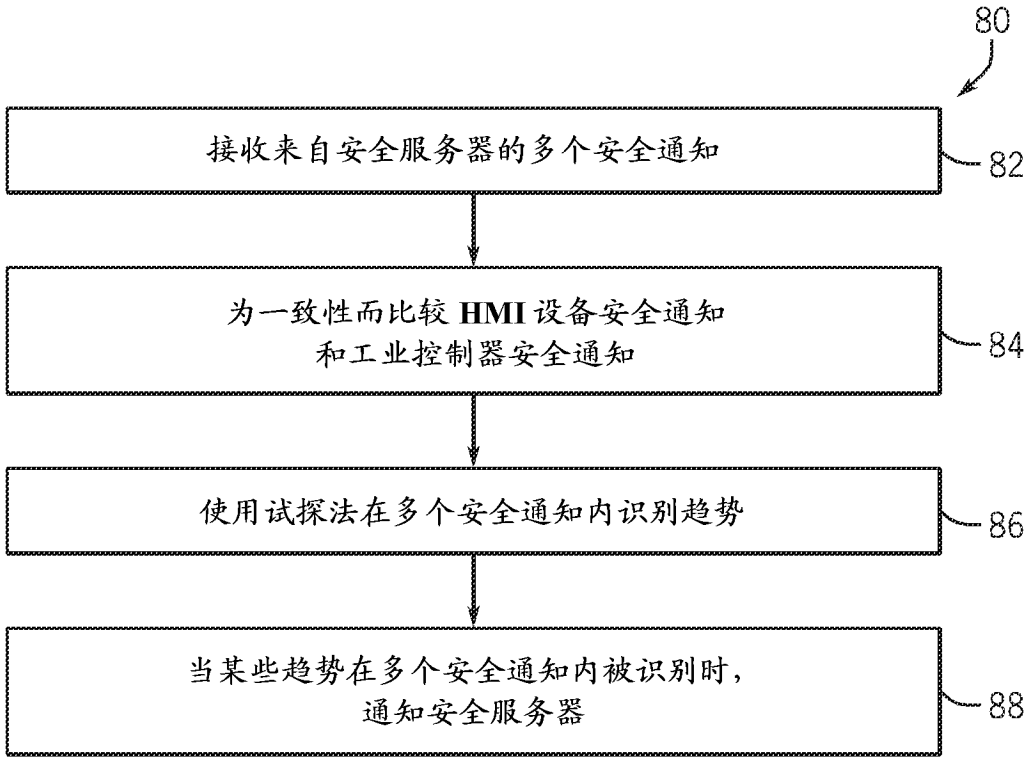

80
接收来自安全服务器的多个安全通知
82
为一致性而比较 HMI 设备安全通知
和工业控制器安全通知
84
使用试探法在多个安全通知内识别趋势
86
当某些趋势在多个安全通知内被识别时，
通知安全服务器
88

图 4