(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109690545 A
(43)申请公布日 2019.04.26

(21)申请号 201680087046.9
(22)申请日 2016.06.24
(85)PCT国际申请进入国家阶段日
2018.12.21
(86)PCT国际申请的申请数据
PCT/US2016/039237 2016.06.24
(87)PCT国际申请的公布数据
WO2017/222553 EN 2017.12.28
(71)申请人 西门子股份公司
地址 德国慕尼黑
(72)发明人 魏东
莱安德罗·弗莱格德阿吉亚尔
(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 高岩 杨林森
(51)Int.Cl.
G06F 21/53(2006.01)
G06F 21/55(2006.01)
G06F 21/57(2006.01)

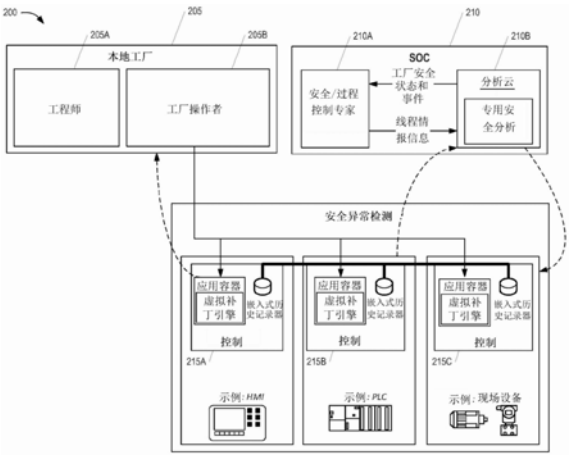
权利要求书3页 说明书8页 附图3页

(54)发明名称

PLC虚拟补丁和安全上下文的自动分发

(57)摘要

一种用于工业生产环境中的安全漏洞的虚拟补丁的系统包括工业自动化设备(例如,PLC)。工业自动化设备包括跨多个工业自动化设备并且存储一个或更多个虚拟补丁的分布式数据库的实例以及包括虚拟补丁引擎安全应用的应用容器。应用容器被配置成收集由工业自动化设备在操作期间生成的系统信息,并且将一个或更多个虚拟补丁应用于系统信息以识别一个或更多个安全攻击。



CN 109690545 A

1.一种用于工业生产环境中的安全漏洞的虚拟补丁的系统,所述系统包括:

工业自动化设备,所述工业自动化设备包括:

跨多个工业自动化设备并且存储一个或更多个虚拟补丁的分布式数据库的实例,以及

包括虚拟补丁引擎安全应用的应用容器,所述应用容器被配置成:

收集由所述工业自动化设备在操作期间生成的系统信息,以及

将所述一个或更多个虚拟补丁应用于所述系统信息以识别一个或更多个安全攻击。

2.根据权利要求1所述的系统,其中,所述一个或更多个虚拟补丁各自描述能够在所述工业自动化设备上利用的不同攻击签名。

3.根据权利要求1所述的系统,其中,所述系统信息与由所述工业自动化设备上执行的一个或更多个应用进行的系统调用对应。

4.根据权利要求1所述的系统,其中,所述系统信息包括以下中的一个或更多个:(i)执行读操作或写操作中的至少一个的存储器块;(ii)系统配置变化;以及(iii)警报状态变化。

5.根据权利要求4所述的系统,其中,所述系统信息还包括以下中的一个或更多个:(i)在所述工业自动化设备上执行的进程;(ii)在所述工业自动化设备上执行的线程;(iii)由所述工业自动化设备使用的网络连接;(iv)文件创建信息;以及(v)文件修改信息。

6.根据权利要求1所述的系统,其中,所述虚拟补丁引擎安全应用执行由所述工业自动化设备执行的控制代码的符号执行,以确定结合一个或更多个控制命令运行所述工业自动化设备的一个或更多个配置的未来后果的指示。

7.根据权利要求6所述的系统,其中,如果所述未来后果的指示与(i)不安全的系统状态或(ii)违反与所述工业生产环境相关联的一个或更多个预定安全约束对应,则所述虚拟补丁引擎安全应用阻止所述一个或更多个控制命令的未来执行。

8.根据权利要求1所述的系统,其中,在所述工业自动化设备上的第一虚拟机中执行所述分布式数据库的实例和所述应用容器。

9.根据权利要求8所述的系统,其中,所述工业自动化设备包括第二虚拟机,所述第二虚拟机执行:

利用与一个或更多个现场设备关联的自动化系统生产数据根据扫描周期更新的过程映像;

网络组件,所述网络组件被配置成发送和接收与工厂地面网络有关的自动化系统网络数据。

10.根据权利要求9所述的系统,其中,所述第二虚拟机附加地执行包括嵌入式历史记录器的实时数据库,所述嵌入式历史记录器被配置成存储经由所述过程映像收集的所述自动化系统生产数据和经由所述网络组件收集的所述自动化系统网络数据。

11.根据权利要求10所述的系统,其中,由所述虚拟补丁引擎安全应用从所述嵌入式历史记录器中检索由所述工业自动化设备在操作期间生成的所述系统信息。

12.根据权利要求1所述的系统,其中,所述虚拟补丁引擎安全应用还被配置成(i)接收由安全操作中心生成的一个或更多个新的虚拟补丁,以及(ii)将所述一个或更多个新的虚拟补丁存储在所述分布式数据库中。

13.根据权利要求12所述的系统,其中,所述虚拟补丁引擎安全应用还被配置成向所述

安全操作中心发送所述一个或更多个安全攻击的指示。

14.根据权利要求1所述的系统,其中,所述虚拟补丁引擎应用还被配置成:

识别与所述一个或更多个安全攻击关联的一个或更多个控制命令;

响应于识别出所述一个或更多个安全攻击,确定是否启用主动响应设置;

如果未启用所述主动响应设置,则执行所述一个或更多个控制命令并且向与所述工业自动化设备关联的操作者报告异常;以及

如果启用所述主动响应设置,则阻止所述一个或更多个控制命令的执行。

15.一种用于工业生产环境中的安全漏洞的虚拟补丁的系统,所述系统包括:

执行一个或更多个控制程序的第一虚拟机;

执行虚拟补丁引擎安全应用的第二虚拟机,所述虚拟补丁引擎安全应用被配置成收集与所述一个或更多个控制程序有关的系统信息,并且将所述一个或更多个虚拟补丁应用于所述系统信息以识别一个或更多个安全攻击;

内部通信信道,被配置成利于在所述第一虚拟机与所述第二虚拟机之间传输所述系统信息;以及

执行所述第一虚拟机和所述第二虚拟机的管理程序。

16.根据权利要求15所述的系统,其中,所述第二虚拟机还包括:

跨多个工业控制器并且存储所述一个或更多个虚拟补丁的分布式数据库的实例。

17.根据权利要求15所述的系统,其中,由所述虚拟补丁引擎安全应用从所述第一虚拟机中的嵌入式历史记录器中检索由所述一个或更多个控制程序在操作期间生成的所述系统信息。

18.根据权利要求17所述的系统,其中,所述第二虚拟机包括应用容器,所述应用容器被配置成执行多个应用并且在所述应用容器中执行所述虚拟补丁引擎安全应用。

19.根据权利要求15所述的系统,其中,所述系统信息包括以下中的一个或更多个:(i)执行读操作或写操作中的至少一个的存储器块;(ii)系统配置变化;以及(iii)警报状态变化。

20.根据权利要求19所述的系统,其中,所述系统信息包括以下中的一个或更多个:(i)在所述第一虚拟机上执行的进程;(ii)在所述第一虚拟机上执行的线程;(iii)由所述第一虚拟机使用的网络连接;(iv)文件创建信息;以及(v)文件修改信息。

21.一种用于工业生产环境中的安全漏洞的虚拟补丁的计算机实现的方法,所述方法包括:

由安全操作中心计算机接收适用于工业控制系统的一个或多个安全漏洞利用方法的指示;

由所述安全操作中心计算机使用模拟工业环境再现所述一个或更多个安全漏洞利用方法;

由所述安全操作中心计算机生成与所述一个或更多个安全漏洞利用方法对应的漏洞利用检测签名;

由所述安全操作中心计算机识别工业控制器的所述漏洞利用检测签名能够适用的一个或更多个用户;

针对每个所识别的用户,生成能够操作成检测所述一个或更多个安全漏洞的企图执行

的虚拟补丁并且将所述虚拟补丁分发给所识别的用户。

22.一种用于工业生产环境中的安全漏洞的虚拟补丁的计算机实现方法,所述方法包括:

由安全操作中心计算机接收适用于工业控制系统的一个或更多个攻击活动的指示;

由所述安全操作中心计算机生成与所述一个或更多个攻击活动对应的攻击检测签名;

由所述安全操作中心计算机识别工业控制器的所述攻击检测签名适用于的一个或更多个用户;以及

针对每个所识别的用户,生成能够操作成检测所述攻击检测签名的虚拟补丁并且将所述虚拟补丁分发给所识别的用户。

PLC虚拟补丁和安全上下文的自动分发

技术领域

[0001] 本发明一般涉及利用虚拟补丁和安全上下文信息的自动分发来改善控制系统相对于网络攻击的的抵抗力(resiliency)。所公开的技术可以应用于例如使用诸如可编程逻辑控制器(PLC)的工业控制器和分布式控制系统(DCS)的各种自动化生产环境。

背景技术

[0002] 安全补丁是工业控制系统(ICS)安全社区面临的最具挑战性的问题之一。为了修复给定可编程逻辑控制器(PLC)中的安全漏洞,在大多数情况下需要完全的固件更新和整个系统重启。此外,安全补丁可能引起新的故障和漏洞,这显著地增加更新实时运行的生产系统的风险和成本。

[0003] 传统上,在大多数情况下,手动执行对工业控制系统的补丁管理。根据适用标准和最佳实践的建议,附加(外部)安全控制部署措施以在等待来自应用供应商的补丁兼容性测试结果时提供额外的保护以补偿长补丁延迟(参见国际电工委员会62443.02.01_2009)。然而,这样的措施通常位于PLC之外并且受到在网络级别能够做什么的限制。

发明内容

[0004] 本发明的实施方式通过提供与用于控制系统的安全上下文信息的自动分发和虚拟补丁有关的方法、系统和装置来解决和克服上述缺点和弊端中的一个或更多个。更具体地,本文中描述的技术提供用于PLC的允许部署虚拟补丁而无需重新加载完整的软件映像/OS的自动机制(过程)、架构和安全应用(例如,app)。虚拟补丁可以提供保护以防止潜在的攻击者在漏洞公开与系统升级之间的时隙中利用未缓解的漏洞。

[0005] 根据本发明的一些实施方式,用于工业生产环境中的安全漏洞的虚拟补丁的系统包括工业自动化设备(例如,PLC)。工业自动化设备包括跨多个工业自动化设备并且存储一个或更多个虚拟补丁的分布式数据库的实例和包括虚拟补丁引擎安全应用的应用容器。应用容器被配置成收集由工业自动化设备在操作期间生成的系统信息,并且将一个或更多个虚拟补丁应用于系统信息以识别一个或更多个安全攻击。每个虚拟补丁可以描述在工业自动化设备上可利用的不同攻击签名。

[0006] 在前述系统中使用的系统信息可以与在工业自动化设备上执行的一个或更多个应用进行的系统调用对应。在一些实施方式中,系统信息包括以下中的一个或更多个:(i)执行读操作或写操作中的至少一个的存储器块;(ii)系统配置变化;(iii)警报状态化。另外地(或可替选地),系统信息可以包括以下中的一个或更多个:(i)在工业自动化设备上执行的进程;(ii)在工业自动化设备上执行的线程;(iii)由工业自动化设备利用的网络连接;(iv)文件创建信息;以及(v)文件修改信息。

[0007] 在前述系统的一些实施方式中,虚拟补丁引擎安全应用执行由工业自动化设备执行的控制代码的符号执行,以确定结合一个或更多个控制命令运行工业自动化设备的一个或更多个配置的未来后果。可以以例如安全违反、系统故障或其他不期望状态的指示的形

式来标识这些未来后果。如果未来后果的指示与例如不安全的系统状态或违反与工业生产环境关联的预定安全约束对应，则虚拟补丁引擎安全应用可以阻止控制命令的未来执行。

[0008] 在前述系统的一些实施方式中，在工业自动化设备上的第一虚拟机中执行分布式数据库的实例和应用容器。工业自动化设备还可以包括第二虚拟机，其执行：利用与一个或更多个现场设备关联的自动化系统生产数据根据扫描周期更新的处理映像；以及网络组件，其被配置成发送和接收与工厂地面网络有关的自动化系统网络数据。在一个实施方式中，第二虚拟机还执行包括嵌入式历史记录器的实时数据库，该实时数据库被配置成存储经由过程映像收集的自动化系统生产数据和经由网络组件收集的自动化系统网络数据。然后，可以由虚拟补丁引擎安全应用从嵌入式历史记录器中检索由工业自动化设备在操作期间生成的系统信息。

[0009] 在前述系统的一些实施方式中，虚拟补丁引擎安全应用还被配置成(i)接收由安全操作中心生成的新的虚拟补丁，以及(ii)将新的虚拟补丁存储在分布式数据库中。另外，虚拟补丁引擎安全应用还可以被配置成向安全操作中心发送安全攻击的指示。在一些实施方式中，虚拟补丁引擎安全应用还被配置成识别与一个或更多个安全攻击关联的一个或更多个控制命令。响应于识别出一个或更多个安全攻击，虚拟补丁引擎安全应用确定是否启用主动响应设置。如果未启用主动响应设置，则执行控制命令并且向与工业自动化设备关联的操作者报告异常。另一方面，如果启用主动响应设置，则阻止执行(一个或多个)控制命令。

[0010] 根据本发明的其他实施方式，用于工业生产环境中的安全漏洞的虚拟补丁的系统包括：两个虚拟机；内部通信信道，其被配置成利于在虚拟机之间传输系统信息；以及执行虚拟机的管理程序(hypervisor)。系统中的第一虚拟机执行一个或更多个控制程序，而第二虚拟机执行虚拟补丁引擎安全应用(例如，其在如上所述的应用容器中)。该虚拟补丁引擎安全应用被配置成收集与一个或更多个控制程序有关的系统信息，并且将一个或更多个虚拟补丁应用于系统信息以识别一个或更多个安全攻击。该系统信息可以包括，例如，以下中的一个或更多个：(i)执行读操作或写操作中的至少一个的存储器块；(ii)系统配置变化；以及(iii)警报状态变化；(iv)在第一虚拟机上执行的进程；(v)执行第一虚拟机的线程；(vi)由第一虚拟机利用的网络连接；(vii)文件创建信息；和/或(viii)文件修改信息。在一些实施方式中，第二虚拟机还包括跨多个工业控制器并且存储一个或更多个虚拟补丁的分布式数据库的实例。在一些实施方式中，通过虚拟补丁引擎安全应用从第一虚拟机中的嵌入式历史记录器中检索系统信息。

[0011] 根据本发明的其他实施方式，用于工业生产环境中的安全漏洞的虚拟补丁的计算机实现的方法包括：安全操作中心计算机接收适用于工业控制系统的安全漏洞利用方法的指示并且使用模拟工业环境再现这些安全漏洞利用方法。安全操作中心计算机生成与安全漏洞利用方法对应的漏洞利用检测签名并且识别漏洞利用检测签名适用于的工业控制器的用户。然后，针对每个识别的用户，安全操作中心计算机(i)生成可操作成检测安全漏洞利用的企图执行的虚拟补丁，以及(ii)将虚拟补丁分发给所识别的用户。

[0012] 根据本发明的其他实施方式，用于工业生产环境中的安全漏洞的虚拟补丁的计算机实现的方法包括安全操作中心计算机接收适用于工业控制系统的攻击活动的指示并且生成与攻击活动对应的攻击检测签名。该方法还包括安全操作中心计算机识别工业控制器

的攻击检测签名适用于的用户。针对每个识别的用户，安全操作中心计算机生成可操作成检测攻击检测签名的虚拟补丁并且将虚拟补丁分发给所识别的用户。

[0013] 本发明的附加特征和优点将根据参照附图进行的示例性实施方式的以下详细描述变得明显。

附图说明

[0014] 根据下面结合附图阅读的详细描述可以更好的理解本发明的前述和其他方面。出于说明本发明的目的，在附图中示出了目前优选的实施方式，但是应该理解，本发明不限于所公开的特定手段。附图中包括以下图：

[0015] 图1示出了根据一些实施方式的具有网络安全应用的高度耦合的控制安全PLC；

[0016] 图2示出了根据一些实施方式的安全异常检测和虚拟补丁的架构；以及

[0017] 图3示出了根据一些实施方式的虚拟补丁过程。

具体实施方式

[0018] 本文中描述了系统、方法和装置，其通常涉及利用虚拟补丁和安全上下文信息的自动分发来改善控制系统相对于网络攻击的抵抗力。本文中描述的虚拟补丁可以被部署为具有对操作系统和存储器的深入低级别访问的PLC内核模块应用，以检测可疑的活动或配置命令并且如果被配置的话则对其拦截。可以应用PLC的虚拟补丁来极大地缓解与实时生产系统的补丁关联的问题，因为其允许检测漏洞利用，并且在一些情况下允许攻击防范。

[0019] 2016年4月22日提交并且题为“Improving Control System Resilience by Highly Coupling Security Functions with Control”的PCT专利申请序列号PCT/US2016/28893描述了包括基于过程变量(传感器和致动器)知识的入侵检测方案的安全异常检测应用，该专利申请通过引用并入本文中。所公开的架构和应用基于无监督的机器学习对PLC提供本地保护。本文中描述的系统和方法通过提供自动地将来自安全操作中心(SOC)的低足迹攻击签名部署为虚拟补丁的机制来补充和增强该架构和应用。

[0020] 图1示出了根据一些实施方式的具有网络安全应用的高度耦合的控制安全PLC 100。该示例示出了西门子软件环境中的实现；然而，应当理解的是，图1中描述的一般构思也可以扩展到其他环境中的等效软件。PLC100具有执行多个虚拟机(VM)的多个处理器核。在一些实施方式中，每个核可以专用于不同的虚拟机。在图1的示例中，一个虚拟机105被配置成实现西门子S7固件(FW)，并且另一虚拟机110被配置成实现Windows或Linux。西门子S7PLC固件执行一个或更多个控制程序以与自动化环境中的现场设备互连。在VM1上运行的任何应用不会对VM0上运行的控制应用产生负面影响。在虚拟机105内，存在由嵌入式历史记录器驱动的实时数据库。其根据时间序列收集与一个或更多个控制程序有关的所有实时过程映像数据，例如来自一个或更多个人机接口(HMI)和制造执行系统(MES)的输入、输出、存储器变量和命令。2015年12月10日提交并且题为“Distributed Embedded Data and Knowledge Management System Integrated with PLC Historian”的PCT专利申请序列号PCT/US2015/64863提供了用于实现可以与本文中描述的高度耦合的控制安全PLC 100一起使用的历史记录器的技术的示例，该专利申请通过引用并入本文中。在Windows/Linux虚拟机110中，另一实时数据库使用内部通信信道或共享存储器(SM)与托管在Simatic S7固件

中的实时数据库(RTDB)交换数据。

[0021] 虚拟机110中的“处理”块是执行主数据处理、读/写/滤波/平滑实时数据库中的主数据的功能块。虚拟机110中的“上下文”块用作翻译器，翻译器将所有数据的含义翻译成生产知识，例如将测量值翻译成温度(例如，啤酒发酵罐的温度)。存在由虚拟机110中的应用容器托管的多个应用，其中一些应用可以针对安全功能。例如，应用1可以用于虚拟补丁应用以进行网络攻击检测/预防(如下面进一步详细讨论的)，并且应用2可以是机器预测分析应用。它们两者需要基于实时数据库中的收集的数据进行工作。在该情况下，虚拟补丁应用可以像Windows或Linux应用一样容易地添加、移除和更新。在2016年2月10日提交并且题为“Extending a Programmable Logic Controller with Apps”的美国专利申请第15/040,565号中进一步详细描述了用于在PLC中实现应用容器内的应用的方法和系统，该专利申请通过引用并入本文中。

[0022] 如本文中使用的术语“虚拟补丁”是指描述不同漏洞或攻击的可执行算法(签名)。基于以下中的一个或更多个来创建虚拟补丁：(i)对再现漏洞/攻击的分析；(ii)对PLC漏洞/攻击的潜在根本原因的确定；(iii)与漏洞根本原因关联的记录的攻击向量；(iv)允许攻击向量操作的所需启用的PLC配置(例如，启用易受攻击的服务)；以及(v)其他上下文的信息，例如生产过程类型、受控变量、连接的机器等。每个虚拟补丁可能包含由标准化语言例如网络可观测表达(CybOX™)或其衍生扩展版本(考虑了控制系统的特性)定义的攻击细节。这些细节可以包括，例如，文件模式、网络分组/流、用户会话标识符、系统事件日志等。虚拟补丁可以通过本体来描述，该本体可以解释入侵/网络安全攻击，例如来自HMI的伪命令、来自MES的被篡改的数据块以及甚至拒绝服务(DoS)攻击。本体还可以包括其他知识，例如由网络攻击引起的不利影响(例如，在生产和质量方面性能下降、机器损坏)。入侵和网络安全本体以及附加生产过程知识可以在控制器中的过程映像数据(现场数据)与其他形式的上下文知识之间进行因果连接，并且能够对异常事件进行推理。

[0023] 在每个控制器上部署虚拟补丁引擎(下面进一步详细描述)使得能够基于每种情况下特定适用的攻击场景来进行基于签名的安全入侵检测。在一些实施方式中，基于每个可用攻击向量利用的潜在风险，仅加载相关签名的小子集，这防止不必要的CPU利用。每个虚拟补丁包含有效载荷和指令，该指令允许控制设备(例如，PLC)上的检测引擎对待检查的系统离散安全事件(例如，配置变化)和可疑的数据流(网络或存储器)的给定组合连续地验证。可以在部署虚拟补丁之前，执行对虚拟补丁在给定PLC/场景下的适用性的校验和验证。

[0024] 图2示出了根据一些实施方式的安全异常检测和虚拟补丁的架构200。该示例通过活动在概念上划分为三个区域：由工程师和工厂操作者执行的本地工厂205活动；在控制器(或其他启用的设备)215A、215B和215C上实现的安全异常检测功能；以及SOC 210处的威胁管理。为了说明的目的呈现了图2中显示的箭头以示出可以在架构200中的设备之间传送信息/数据的一些潜在方式；然而，应当理解的是，这些箭头仅仅是可以使用架构200进行的各种信息/数据传输的示例，并且可以在架构200内类似地实现不同设备对之间的传输。

[0025] 工作流的本地工厂205部分包括工程师205A和工厂操作者205B。工程师205A开发异常检测应用、虚拟补丁应用和其他安全应用并且将其部署到控制器215A、215B和215C。另外，工程师205A可以配置控制器215A、215B和215C(经由部署的应用或通过其他系统设置)，以指定控制器215A、215B和215C与SOC 210之间交换信息的级别。此外，在一些实施方式中，

工程师205A可以指定SOC 210应当如何对特定威胁条件作出反应。

[0026] SOC 210包括安全/过程控制专家210A和分析云210B。安全/过程控制专家210A向分析云210B提供威胁情报信息。分析云210B利用专门的安全分析来处理威胁情报信息，以识别可以被递送到控制器215A、215B和215C的新攻击向量(如下面进一步详细描述的)。另外，分析云210B可以收集工厂安全状态信息(例如，事件等)并且与安全/过程控制专家210A共享该信息以进一步完善威胁情报信息。

[0027] 一旦部署到控制器215A、215B和215C，异常检测应用就启用每个设备上的安全行为(例如，安全事件/日志收集)。另外，在一些实施方式中，异常检测应用向控制器215A、215B和215C提供情况感知上下文。每个控制器215A、215B和215C还可以提供由应用间通信启用的分布式监测以增加抵抗力。可以使用跨包括在每个控制器215A、215B和215C中的嵌入式历史记录器的分布式数据库管理系统(DDMS)在本地和经由对等点两者来检测操纵过程控制或过程视图的任何企图。

[0028] 另外，可以使用图2中所示的该架构200来提供要被部署为本地数据库的数据点的定制安全签名。例如，可以基于来自包括在SOC 210中的分析云210B的上下文来定制递送与全局情报有关的新(外部)攻击向量。类似地，可以由控制器215A、215B和215C向SOC 210广播安全异常。定制的签名和虚拟补丁可以由SOC 210发布并且通过其分析云210B递送(可选地，客户可以决定具有其自身的SOC)。例如，在一些实施方式中，分析云210B执行一个或更多个应用，其关联外部安全信息(例如，威胁情报)、产品信息(例如，PLC技术特征)、安全漏洞信息和其他上下文相关信息，例如但不限于生产过程数据、过程配置、网络拓扑和安全配置。基于该信息，分析云210B识别适用于控制器215A、215B和215C的攻击向量。一旦识别出这些攻击向量，可以生成用于检测攻击的虚拟补丁并且在安全专家201A校验和验证网络攻击和虚拟补丁之后将其部署到控制器215A、215B和215C。还可以使用该基础结构以防止过去发生的事件(对其已知攻击签名或TTP-策略、技术和程序)在具有相同漏洞的类似基础结构中发生。

[0029] 每个控制器215A、215B和215C包括在作为DDMS运行的其相应的嵌入式历史记录器内的虚拟补丁的本地数据库。这些数据库中的每一个具有本文中称为“虚拟补丁数据库”的数据集。使用这些数据库，可以读取来自其他连接的控制设备的数据或攻击签名以确认正在发生攻击。例如，控制器215C可能能够通过分析来自控制器215A和215B的网络连接事件来确认给定的恶意模式。

[0030] 虚拟补丁数据库可以分为两个主要实例：实时和事后检验。实时实例的尺寸减小(可以安装有限数目的虚拟补丁)并且允许命令拦截。可选地，可以通过在给定可用输入和存储器状态的情况下检查所请求命令的符号执行是否导致不安全的过程状态来确认拦截命令执行。事后检验不允许拦截控制或配置命令，但是允许警告对安全损害的确认并且允许安全地收集附加取证数据。

[0031] 每个控制器215A、215B和215C的应用容器包括本文中称为“虚拟补丁引擎”(如图2所示)的内核模块安全应用。该虚拟补丁引擎与SOC 210通信以如安全聚合器那样自动地接收虚拟补丁和威胁情报。引擎使用该信息来执行检测算法，该检测算法连续扫描虚拟补丁数据库以识别指示网络攻击执行的匹配的可疑安全行为。虚拟补丁引擎可以另外收集：系统相关信息，例如正在运行的进程/线程、网络连接、文件创建/修改；以及PLC特定信息，例

如读写存储器块、系统配置变化、警报状态变化、扫描时间、块执行时间等。然后可以由虚拟补丁引擎分析所收集的信息以识别匹配的持续攻击。在一些实施方式中，每个控制器215A、215B和215C的嵌入式本地历史记录器还允许在有限时隙内对最近的系统变化进行历史分析。一旦识别出攻击，就可以由控制器在本地对其处理(例如，阻止来自特定地址的网络业务)。可替选地(或另外)，可以将与攻击有关的通知发送到工厂操作者205B以经由安全工具进一步升级或管理。

[0032] 在一些实施方式中，虚拟补丁引擎使用控制代码的符号执行来确定结合给定控制命令/控制逻辑运行给定配置的未来后果，并且如果需要的话(例如，如果它使系统处于不安全状态或违反安全约束)，则阻止它。在一些实施方式中，虚拟补丁引擎拦截试图访问PLC应用程序以及I/O和其他连接的PLC接口的所有调用。虚拟补丁引擎在允许每个调用进行之前校验每个调用。可选地可以通过安全异常检测应用(如上所述)或在适用于攻击活动期间激活虚拟补丁引擎的检测。

[0033] 图3示出了根据一些实施方式的虚拟补丁过程300。在PLC上安装两个以安全性为中心的应用时，过程300开始。更具体地，在步骤305处，安装在PLC上的异常检测应用启用行为入侵检测，并且在步骤310处，安装在PLC上的虚拟补丁应用启用基于签名的检测。尽管在某些实施方式中指示了安装顺序的应用之间可能存在依赖性，但是这些应用通常可以以任何顺序安装。一旦安装，在步骤315处，PLC进入到连续监测状态中。

[0034] 一旦检测到攻击，就由控制器执行响应操作。基于设备上的配置(例如，由工程师或操作者在一个或更多个应用内指定的配置)，不同级别的响应是可能的。在最小干预响应动作中，仅报告安全异常并且将日志导出到控制器外部。另一方面，可以拒绝配置命令并且可以触发安全关闭动作。例如，在检测到网络Heartbleed有效载荷的注入时，可以禁用由易受Heartbleed Shellshock攻击的OpenSSL库使能的运行易受攻击HTTPS服务的可用性。可替选地，可以接受命令，但是避免响应。在两个方面之间可以采用其他响应形式。

[0035] 在图3的示例中，示出了基于在控制器上是否启用“主动响应”来选择的两个可能的响应。术语“主动响应”是指指示是否应当阻止执行的控制器设置。可以例如由控制器的操作者或工程师提供该设置。如果启用主动响应，则在步骤330处，阻止执行或者可以拒绝一个或更多个命令。可替选地，如果未启用主动响应，则在步骤335处执行配置/控制命令并且(例如，经由HMI或直接向工厂操作者)报告异常。

[0036] 继续参照图3，在步骤340处，由自动化环境内的设备或由外部源公开了新的漏洞。在步骤345处，SOC验证并且再现漏洞。接下来，在步骤350处，SOC创建新漏洞利用检测签名，该新漏洞利用检测签名将使特定设备能够识别漏洞以及试图利用漏洞。然后，在步骤325处，创建虚拟补丁并且(基于例如匹配的固件版本、硬件和其他参数)将其分发给签名适用于的每个客户。在客户的站点处，由自动化系统在步骤320处部署虚拟补丁。工程师或操作者可以决定使用软件接口来批准补丁，但通常，自动化系统一旦选择/确认补丁就自动部署补丁。一旦部署，工程师或操作者可以基于补丁修改系统配置。例如，对于特定漏洞，工程师或操作者可以将控制器配置成在检测到相关漏洞利用签名时正常地或立即关闭。应当注意的是，可以在SOC与自动化环境紧密集成或者工厂操作者/工程师将一些职责委托给SOC的情况下组合步骤320和325。因此，SOC(或一些其他中间组或服务)可以直接将虚拟补丁分发给(一个或多个)控制设备并且(例如，基于由工厂的工程师或操作者提供的偏好)配置对应

的响应行为。应当注意的是，该机制可以用于检测不一定取决于漏洞的存在的攻击方法。例如，这些签名可以用于检测“暴力”类型的攻击或“资源耗尽”。此外，除了针对所公开的漏洞应用有效载荷检测算法之外，还可以通过虚拟补丁的分发来检测攻击活动。

[0037] 在一些实施方式中，通过布尔代数运算来启用虚拟补丁，其真结果指示攻击的正表征(类似于安全信息和事件管理相关性规则)。以下示例说明了该情况：

[0038] 真实攻击＝x∧(y∨(z∧¬(a＝＝1.6)))，

[0039] 其中x是匹配的认证事件，y是输入存储器块变化请求，z是匹配的输出命令值，以及a是CPU固件版本。

[0040] 图3示出了系统可以如何对出现的新攻击技术、实践和程序作出反应。在步骤355处，例如由自动化设备、由工厂工程师或操作者或由SOC本身检测到攻击活动。接下来，在步骤360处，SOC相应地进行调查和表征攻击。基于该表征，在步骤365处SOC创建攻击检测签名。然后，在步骤320和325处，分发签名并且以虚拟补丁的形式将其部署到签名应用于的每个客户。可以以与上面关于漏洞检测签名所讨论的方式类似的方式来实现分发和部署的方式。

[0041] 与传统系统相比，本文中描述的方法、系统和装置提供了几个优点。例如，本文中描述的虚拟补丁允许PLC特定安全签名的自动分发并且提供对漏洞/补丁发布与补丁安装之间的时间段的保护的可能。另外，可以在对PLC硬件产生最小影响的情况下应用本文中描述的技术，尤其是在分布式计算环境中。例如，分布式空闲CPU/存储器资源可以用于分布式异常检测，并且分布式可用存储空间可以用于分布式异常检测。分布式计算的使用还允许分散式攻击检测，这避免了传统系统中经常出现的单点故障。生成的检测签名/虚拟补丁还允许基于来自多个维度的输入数据(例如，网络行为、系统行为、生产过程行为)而不仅仅是纯网络有关的数据和事件进行检测。此外，可以创建签名以保护相邻设备。该方法提供了用于保护传统设备的实现路径。

[0042] 本文中描述的如由控制设备使用的处理器可以包括本领域中已知的一个或更多个中央处理单元(CPU)、图形处理单元(GPU)或任何其他处理器。更一般地，如本文中使用的处理器是用于执行存储在计算机可读介质上的机器可读指令、用于执行任务的设备并且可以包括硬件和固件中的任何一个或其组合。处理器还可以包括存储器，其存储可执行以用于执行任务的机器可读指令。处理器通过操纵、分析、修改、转换或传输信息来对信息起作用以供可执行程序或信息设备使用和/或通过将信息路由到输出设备来使用。处理器可以使用或包括例如计算机、控制器或微处理器的能力，并且可以使用可执行指令来调节以执行不由通用计算机执行的专用功能。处理器可以与使得能够在其间进行交互和/或通信的任何其他处理器(电和/或如包括可执行组件那样)耦合。用户接口处理器或发生器是包括电子电路或软件或两者的组合的已知元件以用于生成显示图像或其部分。用户接口包括使得用户能够与处理器或其他设备进行交互的一个或更多个显示图像。

[0043] 本文中描述的各种设备包括但不限于控制层设备和相关的计算基础设施，其可以包括至少一个计算机可读介质或存储器，用于保存根据本发明的实施方式编程的指令并且用于包含本文中描述的数据结构、表、记录或其他数据。如本文中使用的术语“计算机可读介质”是指参与向一个或更多个处理器提供用于执行的指令的任何介质。计算机可读介质可以采取许多形式，其包括但不限于非暂态、非易失性介质、易失性介质和传输介质。非易

失性介质的非限制性示例包括光盘、固态驱动器、磁盘和磁光盘。易失性介质的非限制性示例包括动态存储器。传输介质的非限制性示例包括同轴电缆、铜线和光纤，包括构成系统总线的线。传输介质还可以采用声波或光波的形式，例如在无线电波和红外数据通信期间生成的那些。

[0044] 如本文中使用的可执行应用包括代码或机器可读指令，该代码或机器可读指令用于例如响应于用户命令或输入调节处理器以实现预定功能，例如操作系统、上下文数据获取系统或其他信息处理系统的功能。可执行程序是用于执行一个或更多个特定过程的代码段或机器可读指令段、子例程或代码的其他不同部分或可执行应用的部分。这些过程可以包括接收输入数据和/或参数、对接收到的输入数据执行操作和/或响应于接收到的输入参数执行功能以及提供得到的输出数据和/或参数。

[0045] 本文中的功能和过程步骤可以响应于用户命令自动地、全部地或部分地执行。自动执行的活动(包括步骤)响应于一个或更多个可执行指令或设备操作执行而无需用户直接启动该活动。

[0046] 图中的系统和过程不是排他性的。可以根据本发明的原理导出其他系统、过程和菜单以实现相同的目的。尽管已经参考特定实施方式描述了本发明，但是应当理解，本文中示出和描述的实施方式和变型仅用于说明目的。在不脱离本发明的范围的情况下，可以由本领域技术人员实现对当前设计的修改。如本文所述的，可以使用硬件部件、软件组件和/或其组合来实现各种系统、子系统、代理、管理器和过程。本文中的任何权利要求要素不应根据35U.S.C112，第六段的规定来解释，除非使用短语“用于……的装置/手段”明确地表述该要素。

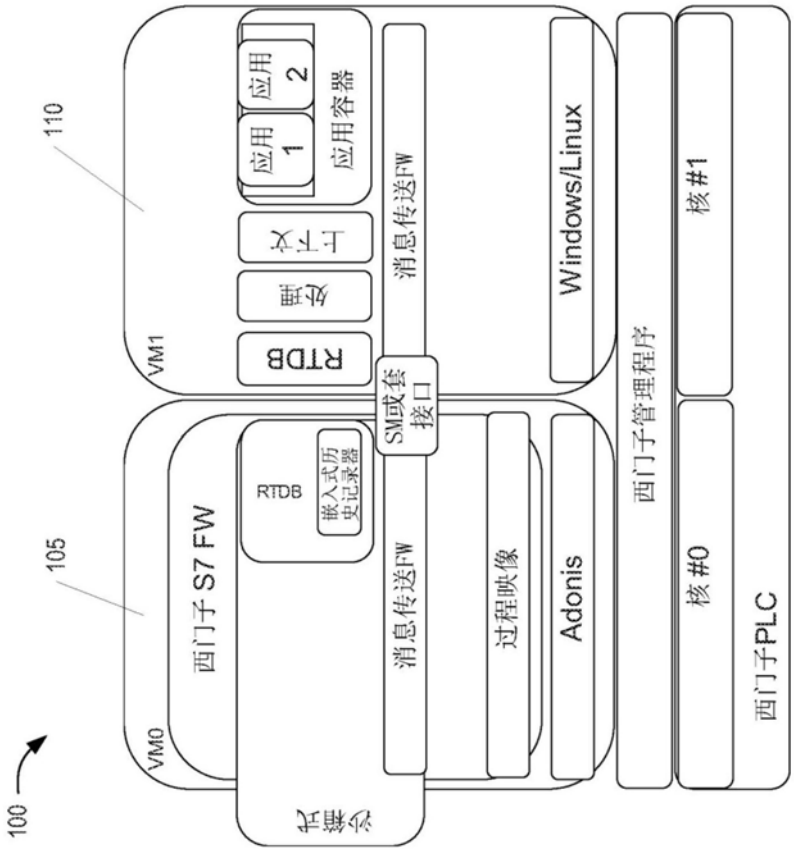

100
105
110
VM0
西门子 S7 FW
RTDB
嵌入式历史记录器
消息传送FW
过程映像
Adonis
VM1
RTDB
处理
上下文
应用 1
应用 2
应用容器
SM或套接口
消息传送FW
Windows/Linux
西门子管理程序
核 #0
核 #1
西门子PLC

图1

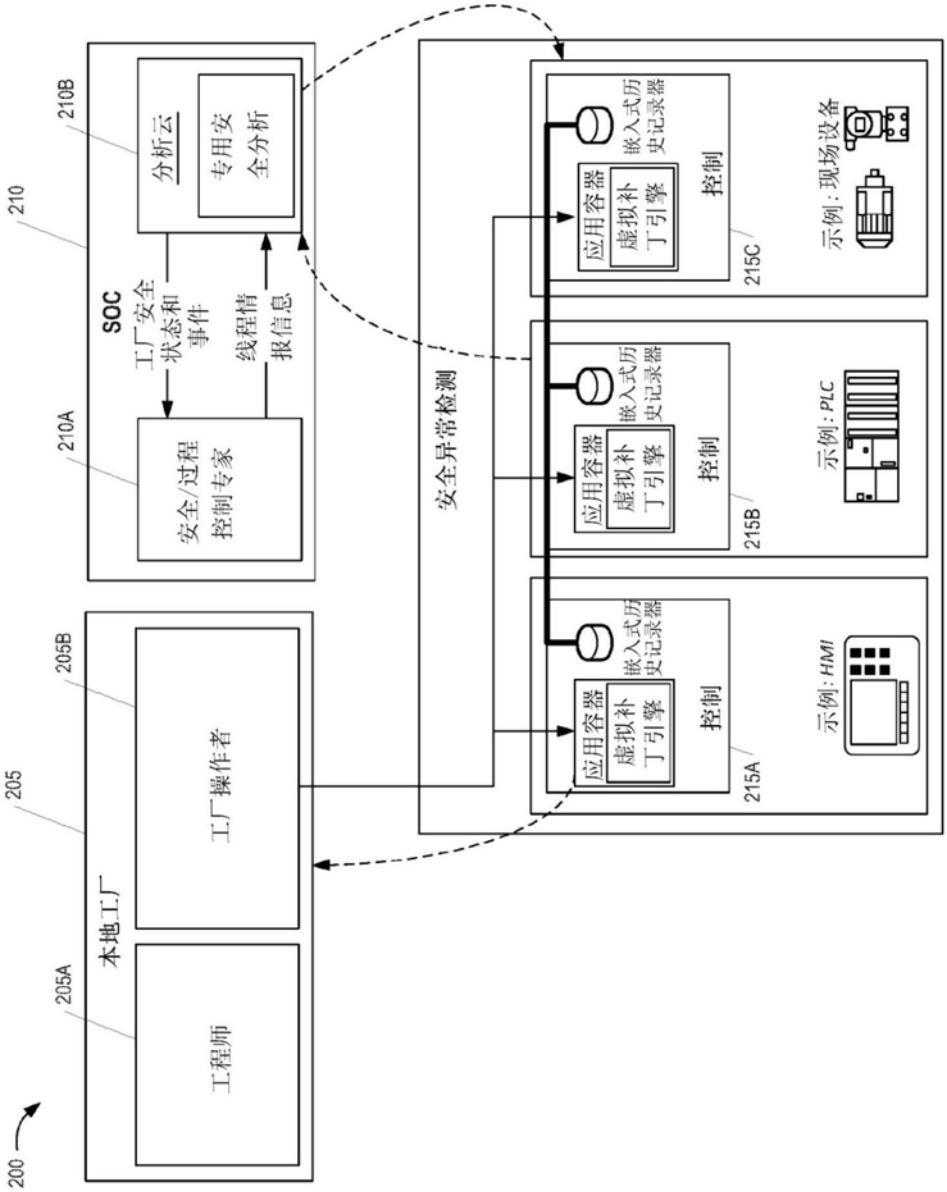

200
205
本地工厂
205A
工程师
205B
工厂操作者
210
SOC
210A
安全/过程控制专家
210B
分析云
专用安全分析
工厂安全状态和事件
线程情报信息
安全异常检测
215A
控制
应用容器
虚拟补丁引擎
嵌入式历史记录器
示例：HMI
215B
控制
应用容器
虚拟补丁引擎
嵌入式历史记录器
示例：PLC
215C
控制
应用容器
虚拟补丁引擎
嵌入式历史记录器
示例：现场设备

图2

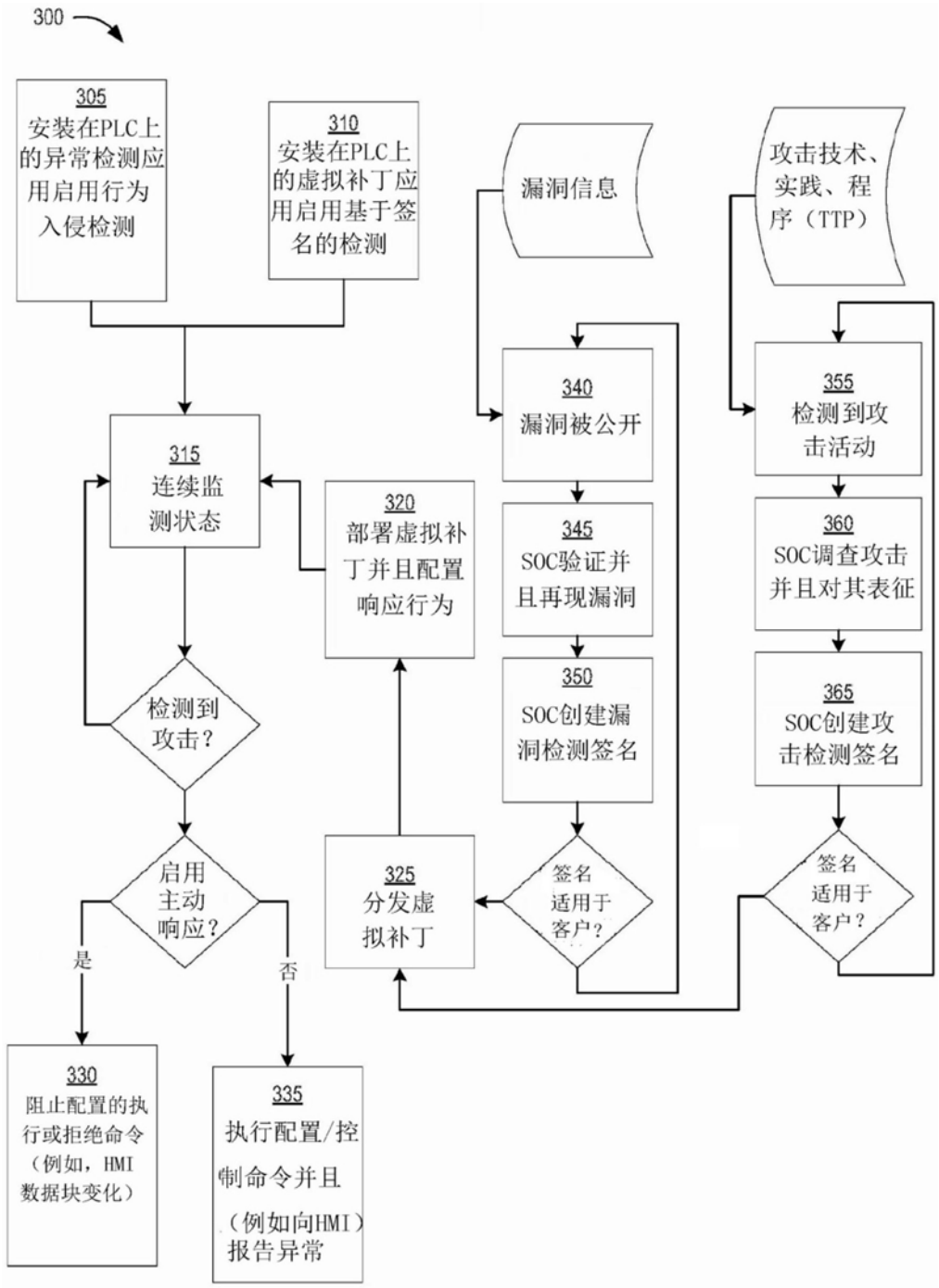

300
305
安装在PLC上的异常检测应用启用行为入侵检测
310
安装在PLC上的虚拟补丁应用启用基于签名的检测
漏洞信息
攻击技术、实践、程序（TTP）
340
漏洞被公开
355
检测到攻击活动
315
连续监测状态
320
部署虚拟补丁并且配置响应行为
345
SOC验证并且再现漏洞
360
SOC调查攻击并且对其表征
检测到攻击？
350
SOC创建漏洞检测签名
365
SOC创建攻击检测签名
启用主动响应？
325
分发虚拟补丁
签名适用于客户？
签名适用于客户？
是
否
330
阻止配置的执行或拒绝命令（例如，HMI数据块变化）
335
执行配置/控制命令并且（例如向HMI）报告异常

图3