(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 106375273 A
(43)申请公布日 2017.02.01

(21)申请号 201610475429.5

(22)申请日 2016.06.24

(30)优先权数据
15177824.8 2015.07.22 EP

(71)申请人 西门子公司
地址 德国慕尼黑

(72)发明人 安娜·帕尔明

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 余刚 李慧

(51)Int.Cl.
H04L 29/06(2006.01)

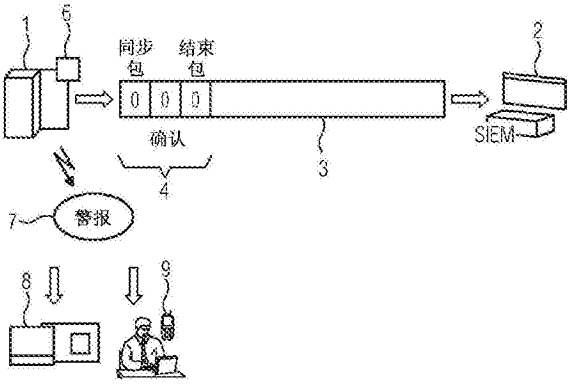
权利要求书2页 说明书4页 附图1页

(54)发明名称

用于监视数据包传输安全的自动化网络和方法

(57)摘要

本发明涉及一种用于监视数据包传输安全的自动化网络和用于监视数据包传输安全的方法，自动化网络包括设置用于传输来自一个设备部件的数据包并进入到一个设备部件中的至少一个第一数据处理器(1)和第二数据处理器中，其中，至少第一数据处理器(1)与第二数据处理器双向地为了传输数据包而相互连接，其中，在将数据包从第一数据处理器(1)发送到第二数据处理器时，由第二数据处理器获得数据包并且生成响应包(5)，其由第二数据处理器发回到第一数据处理器(1)，其中，第一数据处理器(1)包括响应过滤器(6)，利用其能执行对响应包(5)的检查和随后的拒绝/接收。



CN 106375273 A

1.一种用于监视数据包传输安全的自动化网络，包括设置用于传输来自一个设备部件的数据包并进入到一个设备部件中的至少一个第一数据处理器(1)和第二数据处理器，其中，至少所述第一数据处理器(1)与所述第二数据处理器双向地为了传输所述数据包而相互连接，其中，在将所述数据包从所述第一数据处理器(1)发送到所述第二数据处理器时，由所述第二数据处理器获得所述数据包并且生成响应包(5)，所述响应包由所述第二数据处理器发回到所述第一数据处理器(1)，其特征在于，所述第一数据处理器(1)包括响应过滤器(6)，利用所述响应过滤器能执行对所述响应包(5)的检查和随后的拒绝/接收。

2.根据权利要求1所述的用于监视数据包传输安全的自动化网络，其特征在于，所述第二数据处理器为了与所述第一数据处理器(1)通信而包括服务器。

3.根据权利要求2所述的用于监视数据包传输安全的自动化网络，其特征在于，所述服务器是Syslog服务器或者Syslog-ng服务器或者Rsyslog服务器。

4.根据权利要求2所述的用于监视数据包传输安全的自动化网络，其特征在于，所述服务器是安全信息和事件管理服务器(2)。

5.根据前述权利要求中任一项所述的用于监视数据包传输安全的自动化网络，其特征在于，所述第一数据处理器(1)为了与所述第二数据处理器通信而包括基于TCP的客户端。

6.根据权利要求5所述的用于监视数据包传输安全的自动化网络，其特征在于，所述基于TCP的客户端包括协议堆栈并且所述响应过滤器(6)设置在所述协议堆栈中。

7.根据前述权利要求中任一项所述的用于监视数据包传输安全的自动化网络，其特征在于，所接受的响应包(5)至少设计为同步包和/或结束包和/或确认包(4)。

8.根据前述权利要求中任一项所述的用于监视数据包传输安全的自动化网络，其特征在于，所述数据包是安全事件。

9.根据前述权利要求中任一项所述的用于监视数据包传输安全的自动化网络，其特征在于，在拒绝响应包(5)时，实现服务装置上的警报信号(7)的发送。

10.根据前述权利要求中任一项所述的用于监视数据包传输安全的自动化网络，其特征在于，至少在所述第一数据处理器(1)中设置防火墙以用于检查所述数据包。

11.一种用于在自动化网络中监视数据包传输安全的方法，所述自动化网络具有用于传输来自一个设备部件的数据包并进入到一个设备部件中的至少一个第一数据处理器(1)和第二数据处理器，其中，至少所述第一数据处理器(1)与所述第二数据处理器双向地为了用于传输所述数据包而相互连接，其中，在将数据包从所述第一数据处理器(1)发送到所述第二数据处理器时，由所述第二数据处理器获得所述数据包并且生成响应包(5)，所述响应包由所述第二数据处理器发回到所述第一数据处理器(1)，其特征在于，通过设置在所述第一数据处理器(1)中的响应过滤器(6)进行对所述响应包(5)的检查和随后的拒绝/接收，从而能够实现无反作用的发送。

12.根据权利要求11所述的用于监视数据包传输安全的方法，其特征在于，所述响应过滤器(6)始终是活跃的。

13.根据权利要求11或12所述的用于监视数据包传输安全的方法，其特征在于，在拒绝响应包时，生成警报信号(7)，所述警报信号在服务器装置上用以显示。

14.根据权利要求11至13中任一项所述的用于监视数据包传输安全的方法，其特征在于，在拒绝所述响应包(5)时，取消收到从所述第一数据处理器(1)到所述第二数据处理器

的所述响应包(5)的确认。

15.根据权利要求11至14中任一项所述的用于监视数据包传输安全的方法,其特征在于,所述第二数据处理器借助于服务器与所述第一数据处理器(1)通信。

16.根据权利要求11至15中任一项所述的用于监视数据包传输安全的方法,其特征在于,所述第一数据处理器(1)借助于传输控制协议与所述第二数据处理器通信。

17.根据权利要求15所述的用于监视数据包传输安全的方法,其特征在于,所述第二数据处理器借助于Syslog服务器或者Syslog-ng服务器或者Rsyslog服务器或者安全信息和事件管理服务器(2)与所述第一数据处理器(1)通信。

用于监视数据包传输安全的自动化网络和方法

技术领域

[0001] 本发明涉及一种用于监视数据包传输安全的自动化网络，包括设置用于传输来自一个设备部件的数据包并进入到一个设备部件中的至少一个第一数据处理器和第二数据处理器，其中，至少一个第一数据处理器与第二数据处理器双向地为了传输数据包而相互连接，其中，在将数据包从第一数据处理器发送到第二数据处理器时，由第二数据处理器获得该数据包并且生成响应包，其由第二数据处理器发回到第一数据处理器。此外本发明涉及一种用于监视数据包传输安全的方法。

背景技术

[0002] 工业化的自动化网络从数据处理的视界来说由数据网络以及数据处理器组成，数据处理器为了执行数据通信通过数据网络相互连接。例如为了能够实现由远程站点通过自动化网络操作自动化的工业设备，自动化网络能够例如借助于网关连接到公共网络、例如互联网上。实现现代的自动化网络的若干优点导致了IT技术如以太网和互联网协议(IP)的增强的利用。然而，这导致了安全风险的增高，例如通过从外部到相应的自动化网络中的未授权的干涉。

[0003] 自动化网络的概念在接下来应当理解为自动化系统、控制设备、生产设备、制造设备或者诸如此类的。对此，自动化设备的自动化装置能够设计用于执行计算任务。为了该目的，自动化装置能够包括计算装置、例如处理器(CPU)。此外，自动化装置能够包括输入/输出装置，其能够获取过程参量并且能够发出相应的调整信号(Stellsignale)。

[0004] 在2012年3月公开于atp中34至40页的Anna Palmin、Stefan Runde和Pierre Kobes的文章“整体全系统的安全管理-用于自动化支持的工具(Ganzheitliches anlagenweites Security Management-Werkzeuge für die automatisierte Unterstützung)”中描述了用于改善工业化的自动化网络中的安全性的措施。整体安全管理的范畴中的主要措施中的一个是获取并且评估那些在事件中能够由自动化网络的不同部件生成并且也许能够识别入侵的消息。上级的单元收集消息并且对其进行评估，以便从所申报的单个事件或者多个事件的组合中识别是否实际发生了入侵，并且在可能的情况下将其申报在某个位置，从而能够采用合适的措施作为对识别的入侵的反应。该功能性被称为安全事件管理(SEM)。另一个功能性涉及生成报告，以便证明遵守规则。这被称为安全信息管理(SIM)。如果一个单元联合了两个所述的功能性，那么其就被称为安全信息和事件管理(SIEM)。具有在自动化网络中用于实现SIEM的软件工具的计算单元在上述文章中被设置为安全站点。安全站点在结构上布置在过程控制系统(PLS)中。操作站点和安全站点能够共同在一台个人电脑(PC)或两台分开的PC上运行。安全站点同样能够在已经存在的维护站点上实现。其用于将安全管理集成到过程控制系统中，并且能够与设备自动化并行地运行。因此，在设备上现存的视界(Sicht)、例如运行视界和维护视界被补充了附加的集成的安全视界。此外，能够使用存在于自动化网络中的注册和存档系统，以便处理对于安全相关的事件生成的消息。替代集成的软件工具，安全站点能实现为独立于特定的产品的并且具有明确

定义的接口的工具。因此，其能灵活地在上下文中由PLS和SCADA系统(Supervisory Control and Data Acquisition，监管控制和数据获取)采用。安全站点的软件工具用于监视自动化网络中的安全，更确切地是根据消息的获取和评估进行，这些消息由通常被称为操作站点的操作单元、可编程逻辑控制器、所谓的控制器、网络部件、例如路由器、交换机或网关、或者现场装置、例如用于压力、温度或流量的测量变换器或调节机构(Stellglieder)生成。这些装置在此概括地被称为数据处理器或简称为事件源，并且基于其相应的预配置而在安全相关的事件中生成相应的消息。作为安全相关的事件的实例有在PC上的在windows事件日志中获取的识别出的错误登录尝试，或者对通过防火墙防御的并且在可能的情况下写入到日志文件中的IP地址的识别出的未授权入侵。在SIEM系统的所谓的连接口(Konnektoren)中进行对申报的事件的归一化。归一化通常实现为从各个组件或者参数到SIEM的数据结构的映射。

[0005] SIEM系统通常在工程阶段、即在自动化技术设备的规划和投入使用中进行配置。此外，配置此外在应用相应的连接口的情况下包括从可以作为用于安全相关的事件的消息的源的数据处理器到SIEM系统的连接。在此的目的为，SIEM系统不与对于其来说不了解的事件消息的源进行通信，因为这将妨碍安全监视的可靠性。同样地，对此关心的是，在安全相关的事件中通过所涉及的数据处理器生成实际相应的消息。

[0006] 在自动化设备中采用的SIEM系统的主要目的在于立刻识别和评估入侵尝试或偏离正常状态的指示。通过SIEM系统应当能够实现的是，立刻并且恰当地、以及在安全相关的信息的长期存储中和报告的生成中对入侵尝试和异常做出反应。

发明内容

[0007] 因此，本发明的目的在于，提出一种自动化网络和方法，其改善了自动化网络中对入侵尝试或偏离正常状态的指示进行识别的质量和/或可靠性。

[0008] 有关自动化网络的目的通过给出用于监视数据包传输安全的自动化网络实现，其包括设置用于将数据包从一个设备部件中传输出来并传输到一个设备部件中的至少一个第一数据处理器和第二数据处理器，其中，至少第一数据处理器与第二数据处理器双向地为了传输数据包而相互连接，其中，在将数据包从第一数据处理器发送到第二数据处理器时，由第二数据处理器获得数据包并且生成响应包，该响应包由第二数据处理器发回到第一数据处理器，其中，第一数据处理器包括响应过滤器，利用其能执行对响应包的检查和随后的拒绝/接收。

[0009] 有关方法的目的通过给出用于在自动化网络中监视数据包传输安全的方法实现，该自动化网络具有用于传输来自一个设备部件的数据包并进入到一个设备部件中的至少一个第一数据处理器和第二数据处理器，其中，至少第一数据处理器与第二数据处理器双向地为了传输数据包而相互连接，其中，在将数据包从第一数据处理器发送到第二数据处理器时，由第二数据处理器获得数据包并且生成响应包，该响应包由第二数据处理器发回到第一数据处理器，其中，通过设置在第一数据处理器中的响应过滤器进行对响应包的检查和随后的拒绝/接收，从而能够实现无反作用的发送。

[0010] 根据本发明已知的是，设备部件和系统的第一数据处理器与第二数据处理器的通信不是单向的而是双向的。第二数据处理器根据TCP协议将响应值发回到部件和系统。如果

在设备部件的第一数据处理器和第二数据处理器之间采用防火墙，那么通常能够通过开放相应的端口对总体的基于TCP的通信放行。

[0011] 根据本发明，当前在设备部件的第一数据处理器中集成了响应过滤器。其准确地检查第二数据处理器、例如Syslog(系统日志)服务器或SIEM服务器的包，并且仅接受选择作为允许包的包。所有另外的包由相关的设备部件的第一数据处理器拒绝。通过该集成的响应过滤器保障安全事件和另外的信息从设备部件或者设备系统的第一数据处理器中到第二数据处理器的无反作用的传输。安全事件从不同设备部件和设备系统的第一数据处理器到在设备中采用的第二数据处理器的传输并不负面地影响设备的保护水平和可用性，即传输无反作用地进行。此外有利地，能证明并且因此保障安全事件和另外的信息的传输的无反作用性。设备的针对未授权入侵和最大可能的设备可用性所包括的保护的保证的目的对于第二数据处理器的数据传输的所要求的能证明的无反作用性来说很重要。

[0012] 优选地，第二数据处理器为了与第一数据处理器通信而包括服务器。其能够设计为Syslog(系统日志)服务器或者Syslog-ng(下一代系统日志)服务器或者Rsyslog(快速系统日志)服务器。该服务器也能够设计为SIEM(安全信息和事件管理)服务器。显而易见，也能够应用其它的服务器。

[0013] 优选地，第一数据处理器为了与第二数据处理器通信而包括基于TCP的客户端。此外，基于TCP的客户端能够包括协议堆栈，其中，响应过滤器设置在协议堆栈中。

[0014] 优选地，所接受的响应包至少设计为同步包和/或结束包和/或确认包。然而，也能够接受其它的响应包。优选地，所有另外的包由相关的设备部件的第一数据处理器拒绝。在该情况中取消包的确认。

[0015] 优选地，数据包是安全事件、例如事件、威胁数据以及风险数据。

[0016] 在本发明的一个优选的设计方案中，在拒绝响应包时，实现服务器装置上的警报信号的发送。也就是说，其生成了相应的消息，其根据实施的配置例如发送到过程控制系统或SCADA系统或者通过SMS发送给负责人(例如设备操作者、管理员或IT专业人员)并且告知其以下信息，即设备部件中的第一数据处理器已经从第二数据处理器收到不允许的响应值。该信息是非常重要的，因为由此用信号传递的是，所采用的第二数据处理器、例如SIEM服务器或Syslog服务器有可能是不值得信赖的。

[0017] 为了提高安全还能够至少在第一数据处理器中设置防火墙以用于检查数据包。

[0018] 有利地，响应过滤器始终是活跃的。由此所保障的保护能够因此既不刻意地也不由于错误而被取消。这特别地相对于能通过采用防火墙实现过滤数据包而具有优点，即，根据本发明的集成的响应过滤器是更合适的、开销更小、配置更少以及更可靠的，因为例如防火墙在可能的情况下会被无意或恶意地进行操纵。

附图说明

[0019] 参照任意的附图从下述实施例的说明中得出了本发明的另外的特性、特征和优点。在此示意性地示出：

[0020] 图1是根据现有技术的安全事件和另外的信息的传输，

[0021] 图2是通过集成的响应过滤器的安全事件和另外的信息的无反作用的传输。

具体实施方式

[0022] 尽管通过优选的实施例在细节上详细地阐述并描述了本发明，但本发明并不局限于所公开的实例。其他的变体能够由此由专业人员推导出，这并不脱离本发明的保护范围。

[0023] 图1示出了基于TCP的Syslog版本，其基于通过接收包的回复所保障的可靠性而优于基于UDP的版本。这所导致的是，设备部件的第一数据处理器1与SIEM服务器或Syslog服务器2的通信不是单向的而是双向3的。因为SIEM服务器或Syslog服务器2根据TCP协议至少将同步包、结束包和确认4作为响应值发回到设备部件的第一数据处理器1，这些设备部件由第一数据处理器1获得确认、即所谓的响应包5。如果在设备部件和设备系统之间采用防火墙，那么通常能够通过开放相应的端口对总体的基于TCP的通信放行。此外，通过采用防火墙以过滤设备部件/系统的第一数据处理器1和Syslog/SIEM服务器2之间的通信为目的将导致高附加成本、用于配置和监视防火墙的高开销以及在可能的情况下的对性能的负面影响。此外，考虑到安全所出现的风险在于，所采用的防火墙故意或无意地被篡改，这例如能够导致过滤器的去激活和/或消息的去激活或者发出错误警报。

[0024] 现在，这通过本发明解决了。图2示出了安全事件和另外的信息通过集成的响应过滤器的无反作用的传输。在使用基于TCP的Syslog以用于将来自自动化部件和自动化系统的安全事件和另外的信息传输到系Syslog服务器或SIEM服务器2时，在第一数据处理器1中执行的TCP中集成有响应过滤器6。其准确地检查由Syslog服务器或SIEM服务器2获得的响应值，并且仅接受同步包、结束包和确认4、即仅仅带有SYN、ACK或FIN标记的包作为允许的响应值。

[0025] 所有另外的包由相关的设备部件或者其第一数据处理器1拒绝。在该情况中取消包的确认。附加地，生成相应的消息(警报信息7)，其根据实施的配置例如发送到过程控制系统或SCADA系统8或者通过SMS 9发送给负责人(例如设备操作者、管理员或IT专业人员)并且告知其以下信息，即相关的设备部件已经从Syslog服务器或SIEM服务器2收到不允许的响应值。该信息是非常重要的，因为由此用信号传递的是，所采用的SIEM服务器2或Syslog服务器是不值得信赖的。通过集成的响应过滤器6保障了来自设备部件的第一数据处理器1的安全事件和另外的信息到Syslog服务器或SIEM服务器2的无反作用的传输。集成在第一数据处理器1的TCP堆栈中的响应过滤器6能够始终是活跃的，由此能够既不刻意地也由于错误而取消由此所保障的保护。

[0026] 由此特别地，相对能通过采用防火墙实现过滤数据包得到的优点在于，能够实现更合适的、开销更小、配置更少以及更可靠的利用。这是特别的情况，因为防火墙在可能的情况下会被无意或恶意地篡改。

[0027] 另一个优点在于简单的能证明性。其根据消息实现，这些消息是在识别出的“不允许的”响应值的情况下生成并且发送到过程控制系统或SCADA系统8或者通过SMS 9发送给负责人、例如设备操作者、管理员或IT专业人员的消息。

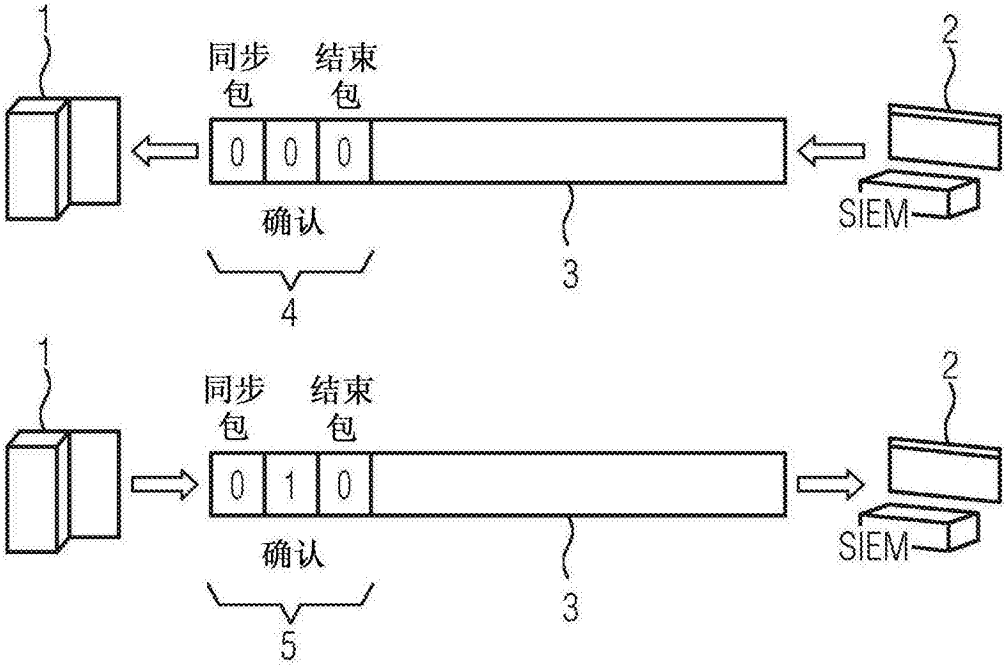

1
同步
包
结束
包
0
0
0
2
SIEM
确认
4
3
1
同步
包
结束
包
0
1
0
2
SIEM
确认
5
3

图1

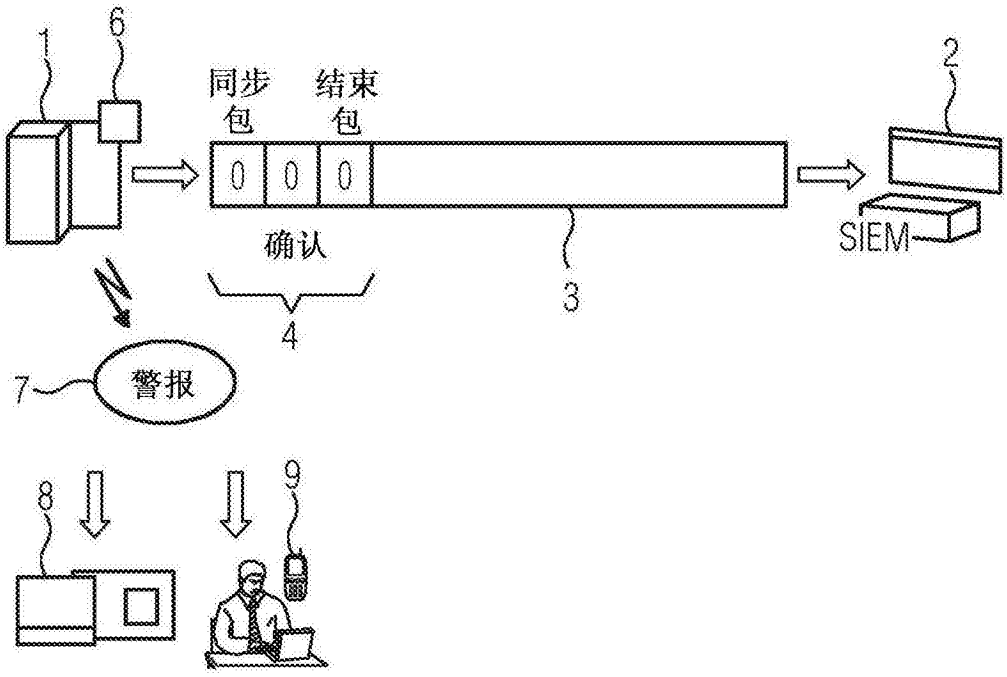

1
6
同步
包
结束
包
0
0
0
2
SIEM
确认
4
3
7
警报
8
9

图2