(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 104991526 B
(45)授权公告日 2017.09.26

(21)申请号 201510221450.8

(22)申请日 2015.05.04

(65)同一申请的已公布的文献号
申请公布号 CN 104991526 A

(43)申请公布日 2015.10.21

(73)专利权人 中国科学院软件研究所
地址 100190 北京市海淀区中关村南四街4号

(72)发明人 李昊 陈震宇 迟佳琳 张敏 苏璞睿 秦宇

(74)专利代理机构 北京君尚知识产权代理事务所(普通合伙) 11200
代理人 司立彬

(51)Int.Cl.
G05B 19/418(2006.01)
G06F 21/57(2013.01)

(56)对比文件
CN 104573516 A,2015.04.29,
CN 104573549 A,2015.04.29,
CN 104077244 A,2014.10.01,
CN 103532927 A,2014.01.22,
KR 20130021641 A,2013.03.06,

审查员 王雅彬

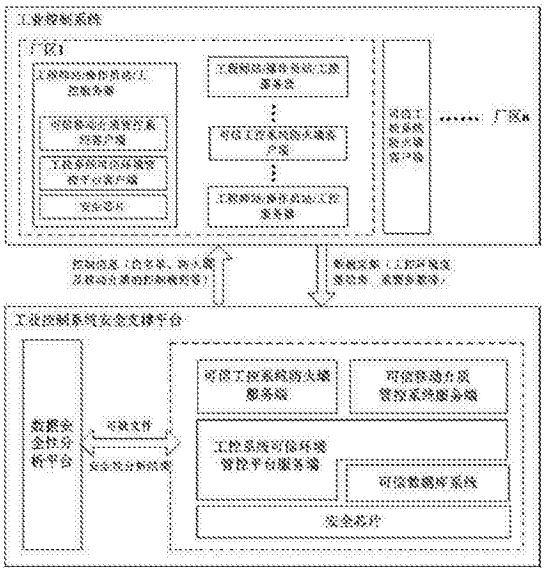
权利要求书2页 说明书7页 附图2页

(54)发明名称

工业控制系统安全支撑框架及其数据安全传输和存储方法

(57)摘要

本发明公开了工业控制系统安全支撑框架及其数据安全传输和存储方法。本发明的安全支撑框架包括若干设有安全芯片的安全服务器和若干设有安全芯片的客户端;其中,客户端与所述安全服务器通过网络连接,服务器上设有工控系统可信环境管控平台的服务端、可信移动介质管控系统的服务端、可信工控防火墙的服务端和可信数据库系统,客户端上设有可信工控系统防火墙的客户端、可信环境管控平台的客户端、可信移动介质管控系统的客户端,其中:可信数据库系统,负责为存储在数据库中的设定敏感数据提供机密性和完整性保护服务,将设定敏感数据与可信的工控系统环境绑定。本发明能阻止恶意代码在工控环境中的运行、传播,同时确保敏感数据不被泄漏和篡改。



CN 104991526 B

1.一种工业控制系统安全支撑架构，其特征在于，包括若干设有安全芯片的安全服务器和若干设有安全芯片的客户端；其中，所述客户端与所述安全服务器通过网络连接，所述安全服务器上设有工控系统可信环境管控平台的服务端、可信移动介质管控系统的服务端、可信工控防火墙的服务端、新鲜性保护模块和可信数据库系统，所述客户端上设有可信工控系统防火墙的客户端、可信环境管控平台的客户端、可信移动介质管控系统的客户端，其中：

所述工控系统可信环境管控平台，负责基于安全芯片的身份凭证来标识所述客户端的身份，并保护它们之间的数据通信；

所述可信数据库系统，负责基于安全芯片为存储在数如果据库中的设定敏感数据提供机密性和完整性保护服务，将设定敏感数据与可信的工控系统环境绑定；

所述可信工控系统防火墙，负责对工控系统的网络实施分层隔离，并按照设定的控制规则控制在不同网络分层之间的数据交互；

所述可信移动介质管控系统，负责根据工控终端接入移动介质的规则对插入所述客户端的移动介质进行认证和准入控制；

所述新鲜性保护模块，用于对所述可信数据库系统的数据库文件进行初始化度量，并对度量结果保存到一新鲜性保护数据表中；并在所述可信数据库系统每次启动前度量所述可信数据库系统的数据库文件的哈希值，并利用签名私钥对其进行签名后更新到新鲜性保护数据表中；

其中，设定的敏感数据包括设定的控制规则和工控终端接入移动介质的规则。

2.如权利要求1所述的工业控制系统安全支撑架构，其特征在于，所述工控系统可信环境管控平台，还负责基于安全芯片对工控系统中的工控终端及工控服务器环境进行可信的度量，并设置可信进程的白名单。

3.如权利要求1所述的工业控制系统安全支撑架构，其特征在于，所述新鲜性保护模块申请安全芯片中的非易失存储区空间用于存放新鲜性保护的根。

4.如权利要求1或2所述的工业控制系统安全支撑架构，其特征在于，所述安全服务器还包括一数据安全性分析平台，负责对出入工控系统中的工控终端、工控服务器的数据文件的安全性进行分析，确保数据文件中没有包含恶意代码，同时还负责为工控系统可信环境管控平台提供应用软件白名单认证服务，确保工控系统环境中运行的应用软件不包含恶意行为。

5.如权利要求1所述的工业控制系统安全支撑架构，其特征在于，所述客户端包括工程师站、操作员站、工控服务器。

6.一种工业控制系统安全支撑架构的信息传输方法，其步骤为：

1)进行数据传输的源主机S与目的主机D首先进行双向的远程证明，证明通过后，双方互相保存对方身份密钥对中的公钥及对方的系统环境状态；其中，主机S的身份密钥对为(pks,sks)，环境状态记为C_s，D的身份密钥对为(pkd,skd)，环境状态记为C_d；

2)远程证明结束后，主机S向主机D发送一个随机数r以及利用私钥sks对r的签名$sig_{sks}(r)$；

3)主机D用主机s的公钥pks验证签名$sig_{sks}(r)$；若正确，则主机D中的安全芯片产生一对密钥(pk,sk)，且指定该密钥的使用环境为C_d；然后将该密钥对(pk,sk)、不可迁移性、使

用环境C_d、随机数r以及采用自己的私钥skd对该密钥对(pk,sk)、不可迁移性、使用环境C_d、随机数r的签名数据发送给主机S;

4)主机S用主机D的公钥pkd验证收到的签名数据,若正确,则检验随机数r的正确性;若r正确,则判定使用环境C_d是否为符合主机S设定的安全需求,若符合设定安全需求,则主机S产生一密钥k,并利用该密钥k加密待传输数据Data得到$enc_k(Data)$,采用公钥pk对该密钥k进行加密得到$enc_{pk}(k)$,然后将数据$enc_{pk}(k)$,$enc_k(Data)$,r,$sig_{sks}(enc_{pk}(k),enc_k(Data),r)$发送给主机D;其中,$sig_{sks}(enc_{pk}(k),enc_k(Data),r)$为主机S采用自己私钥sks对数据$enc_{pk}(k)$、$enc_k(Data)$、r的签名数据;

5)主机D用主机S的公钥pks对收到的签名数据进行验证,若正确,则检验随机数r的正确性;若r正确,则利用受安全芯片保护的私钥sk解密出密钥k,再利用该密钥k解密出数据Data。

7.如权利要求6所述的方法,其特征在于,所述密钥(pk,sk)为一对不可迁移的非对称加密密钥(pk,sk)。

8.如权利要求6所述的方法,其特征在于,所述密钥k为对称密钥。

9.一种基于权利要求1所述工业控制系统安全支撑架构的信息存储方法,其步骤为:

1)安全服务器的可信数据库系统第一次启动前,新鲜性保护模块调用安全服务器的安全芯片产生一对受安全芯片保护的签名密钥(pkf,skf),将私钥skf的使用环境绑定为新鲜性保护模块正常运行的环境;

2)新鲜性保护模块在可信数据库系统中建立一个新鲜性保护数据表T(FileID,Sig_{skf}(File)),用于记录数据库文件名FileID与该文件哈希值的签名Sig_{skf}(File)的对应关系;

3)新鲜性保护模块对新鲜性保护数据表T进行哈希运算,并用私钥skf签名产生Sig_{skf}(T),然后将Sig_{skf}(T)作为新鲜性保护的根存放在安全芯片的非易失存储区中;

4)在后续每次可信数据库系统启动前,新鲜性保护模块重新度量每个数据库文件的哈希值,并从新鲜性保护数据表T(FileID,Sig_{skf}(File))中查询其对应的签名值,验证该文件的签名值和哈希值是否正确;如果未通过验证,则退出启动流程;如果验证通过,则进一步对新鲜性保护数据表T进行哈希运算,并从安全芯片的非易失存储区中查询签名Sig_{skf}(T),验证T的签名值和哈希值的正确性,若不正确则退出启动流程,否则正常启动;在可信数据库系统关闭后,新鲜性保护模块重新度量每个数据库文件的哈希值,并利用skf对其进行签名,然后更新到新鲜性保护数据表T(FileID,Sig_{skf}(File))中;然后新鲜性保护模块对新鲜性保护数据表T进行哈希运算,并用私钥skf签名产生Sig_{skf}(T),再存储到安全芯片的非易失存储区中。

工业控制系统安全支撑框架及其数据安全传输和存储方法

技术领域

[0001] 本发明以可信计算技术为基础提出一种工业控制系统安全支撑框架及其数据安全传输和存储方法，属于工业控制安全领域。

背景技术

[0002] 由于工业生产对工控系统可用性的严格要求，工控系统在部署完成后通常不会及时地进行升级、打补丁或杀毒软件病毒库的更新等安全操作。因为新升级或更新后的病毒、木马查杀工具可能在查杀病毒的同时对系统环境造成破坏，进而导致系统崩溃。相比于普通IT系统，工控系统如果停机维护，就会带来巨大的影响，例如重大经济损失、环境污染等。工控系统中通常需要确定这些病毒、木马查杀工具不会对现有系统造成损害的情况下，才对它们进行更新或升级，而不像普通IT系统那样及时。也就是说，相比于传统信息系统，工控系统的安全防护措施存在一定的滞后性。

[0003] 而随着信息化和工业化的融合，许多工业生产领域的企业管理网与工业控制网开始逐渐地互联互通，以实现管理与控制一体化。在这种情况下，工控系统安全防护措施的滞后性就会为工控系统带来更为严重的安全问题。首先，在系统环境安全方面，现有工控系统主要采用的是各类病毒、木马查杀工具，将这些工具部署于工程师站、操作员站等工控终端以及工控服务器上。这些工具通常是基于代码和行为的特征对系统环境进行检测，需要维护一个病毒、木马的特征库，并及时进行更新。但是，如前所述现有工控系统在升级和打补丁方面存在滞后性，因此工程师站、操作员站等工控终端及工控服务器的系统环境安全性就较难确保。其二，在敏感数据安全方面，由于前述系统环境安全性较难保障的问题，存放在数据库中的业务数据将面临着篡改和泄漏两方面的威胁。例如，攻击者可以入侵系统环境，并对数据库中存放的工艺配方等敏感数据进行篡改，则可能引发生产事故，带来经济损失甚至人员伤亡。此外，数据库中存放的生产计划等数据若被泄漏给竞争对手也会给企业造成巨大影响。其三，在网络安全方面，通常工业控制系统的网络可以划分为现场设备层、车间监控层、生产管理层、企业经营管理层等层次，不同层次间要部署防火墙进行网络的隔离，以阻止攻击在网络间进行蔓延传播。而相比于普通信息系统中的防火墙，工控系统的防火墙需要能够深入分析工业控制协议，具有更细粒度的访问控制，以阻止针对工控通信协议和控制设备自身安全缺陷和漏洞的攻击。这是目前普通的IT防火墙所不具备的。最后，移动介质安全性对于工控系统尤其重要。工业控制系统中经常采用移动介质，例如U盘、移动硬盘等，进行数据拷贝、系统安装和维护，因此，移动介质成为工控系统中病毒或木马等恶意代码传播的重要途径。工控系统需要比普通IT系统更为严格的移动介质安全管控，包括移动介质的认证、恶意代码检测。

[0004] 总之，为了应对工控系统现有安全防护措施的滞后性以及信息化和工业化的两化融合带来的新的安全威胁，有必要在上述系统环境安全、敏感数据安全、网络安全、移动介质安全四个方面采用新的技术和方法来提高工控系统的整体安全性。

发明内容

[0005] 针对上述技术问题，本发明的目的是提供一种以可信计算技术为基础的工业控制系统安全支撑框架及其数据安全传输和存储方法，用于加强工业控制系统的安全性，阻止恶意代码在工控环境中的运行、及通过网络和移动介质进行传播，同时确保工控系统中敏感数据不被泄漏和篡改。

[0006] 为了实现上述技术目的，本发明的工业控制系统安全支撑架构主要包括四个必选部分：工控系统可信环境管控平台、可信数据库系统、可信工控系统防火墙、可信移动介质管控系统，以及一个可选部分：数据安全性分析平台，其中：

[0007] 所述工控系统可信环境管控平台负责基于安全芯片的身份凭证来标识工控系统中的工控终端及工控服务器身份，并保护它们之间的数据通信，同时还负责基于安全芯片对工控系统中的工控终端及工控服务器环境进行可信的度量，并通过白名单方式，仅允许白名单规定的可信进程运行，从而确保工控系统环境的可信性，此外，白名单等安全关键数据将采用所述可信数据库进行保护。

[0008] 所述可信数据库系统负责基于安全芯片为存储在数据库中的设定敏感数据提供机密性和完整性保护服务，将设定敏感数据与可信的工控系统环境绑定，并将方案的安全性建立在硬件安全芯片基础上，以阻止来自系统环境或内部人员的攻击，进而防止数据泄漏和遭受篡改。

[0009] 所述可信工控系统防火墙负责对工控系统的网络实施分层隔离，并对工控协议进行高效地分析，进而按照设定的控制规则来控制在不同网络分层之间的数据交互，而这些规则将采用可信数据库系统进行存储保护。

[0010] 所述可信移动介质管控系统负责根据工控终端接入移动介质的规则对插入工控终端的移动介质进行认证和准入控制，该控制规则将采用可信数据库系统进行安全存储，此外还将利用数据安全性分析平台对移动介质中的数据进行安全性分析，对分析出的恶意代码或文件进行删除或隔离。

[0011] 所述数据安全性分析平台负责对出入工控系统中的工控终端、工控服务器的数据文件的安全性进行分析，确保数据文件中没有包含漏洞利用代码等恶意代码，同时还负责为工控系统可信环境管控平台提供应用软件白名单认证服务，确保工控系统环境中运行的应用软件不包含恶意行为。

[0012] 上述框架中每个组成部分的具体实现方式可以采用公知的任意方式来实现。本发明内容主要为上述部分组成的工业控制系统安全支撑平台的框架，即各部分如何在框架中相互结合发生作用，来确保工业控制系统的安全性。因此，下面将进一步详细阐述这些组成部分之间的重要数据的安全传输及安全存储方法。这些重要数据包括：工控系统可信环境管控平台的白名单、可信工业控制防火墙的网络规则、可信移动介质管控系统的管控规则，及其他一些工业控制系统的生产相关的重要数据，例如生产计划、生产配方等。

[0013] (一)安全传输方法：

[0014] 上述框架中的每个组成部分所部署的主机(台式机、笔记本、服务器)应该装有安全芯片。这些组成部分可能采用客户端/服务端的架构实现，因此同一个组成部分可能其客户端与服务端位于两台不同的主机上。本发明中，不论是不同组件之间的通信，还是同一组

件的客户端及服务端之间的通信都要采用本发明中的方法进行安全的数据传输。

[0015] 数据传输的双方分别记作源主机S与目的主机D。

[0016] (1)S与D首先进行双向的远程证明，相互证明自己的安全芯片的身份及主机系统环境的状态，S的身份密钥对为(pks,sks)，环境状态记为C_s，D的身份密钥对为(pkd,skd)，环境状态记为C_d。远程证明后，双方互相知道对方的身份密钥对的公钥及对方的系统环境的当前状态。因为工控环境中没有匿名需求，所以这里的远程证明方法不必采用匿名证明，可以为公知的任意可信计算方法；

[0017] (2)远程证明结束后，S向D发送一个随机数r，和对r的签名$sig_{sks}(r)$，用于防止重放攻击；

[0018] (3)D用pks验证签名$sig_{sks}(r)$，若正确，则D中的安全芯片产生一对不可迁移的非对称加密密钥(pk,sk)，且指定该密钥的使用环境为C_d。并将该密钥对(pk,sk)、不可迁移性non-migratable、使用环境信息C_d及随机数r采用skd签名，然后发送给S。即D向S发送：(pk,sk),non-migratable,C_d,r,sig_{skd}((pk,sk),non-migratable,C_d,r)；

[0019] (4)S用pkd验证sig_{skd}((pk,sk),non-migratable,C_d,r)的正确性，若正确，则进一步检验随机数r的正确性。若r正确，则再判定C_d是否为符合S设定安全需求的目的主机环境(比如两者使用环境相同)。若符合安全需求，则S产生一个对称的加密密钥k，并利用k加密重要数据Data，然后采用pk将k进行加密。S向D发送$enc_{pk}(k)$,$enc_k(Data)$,r,$sig_{sks}(enc_{pk}(k),enc_k(Data),r)$；

[0020] (5)D用pks验证签名$sig_{sks}(enc_{pk}(k),enc_k(Data),r)$的正确性，若正确，则进一步检验随机数r的正确性。若r正确，则利用受安全芯片保护的sk来解密k，再利用k解密出重要数据Data。

[0021] 在上述步骤(5)中，由于(pk,sk)为受安全芯片保护的不可迁移的密钥对，且sk的使用环境被指定为C_d，因此重要数据在传输过程及传输到目的主机D后，都必须在源主机S认可的目的主机d及其安全环境C_d下解密。一旦目的主机D在传输过程中或数据到达后，环境遭受了破坏，则重要数据Data就无法被解密，也就不会造成数据泄漏。此外，若为双向数据传输，则上述过程中的步骤(2)至(5)要由源主机和目的主机互换角色，重新执行一遍即可。

[0022] (二)安全存储方法

[0023] 在本框架中虽然采用了可信数据库系统对存储于其中的数据提供了基于安全芯片的机密性和完整性保护，但是对于重要数据的存储保护仍然不够，这主要是由于数据的新鲜性仍然能够被破坏。例如，攻击者可以通过将操作系统中存储数据库的文件全部替换为旧版本文件，从而达到攻击目的——白名单被替换为旧版本，生产配方被替换为旧版本等。该攻击是无法通过版本号或时间戳来抵御的，因为版本号只是对数据处于的某个状态进行了编号，而时间戳只能表明在某个时间点数据已经存在，它们都无法表明数据是否为最新的。本发明提供如下的基于安全芯片的新鲜性保护方法来进一步加强重要数据的存储安全性。

[0024] 在可信数据库系统所部署的主机(台式机、笔记本、服务器)上，增加一个新鲜性保护模块，它与可信数据库及安全芯片相互配合，实现可信数据库中存放的数据的新鲜性保护，主要包括如下几个过程：

[0025] (1)初始化过程

[0026] 可信数据库系统安装完毕,第一次启动前,新鲜性保护模块要完成初始化过程:

[0027] a)新鲜性保护模块调用安全芯片产生一对受安全芯片保护的签名密钥(pkf,skf),该密钥对的私钥skf的使用环境被绑定为新鲜性保护模块正常运行的环境,同时申请安全芯片中的非易失存储区空间;

[0028] b)新鲜性保护模块在可信数据库中建立一个新鲜性保护数据表T(FileID,Sig_{skf}(File)),它记录了操作系统中的存储数据库表的数据库文件名FileID与该文件哈希值的签名Sig_{skf}(File)的所有对应关系;

[0029] c)新鲜性保护模块对新鲜性保护数据表T进行哈希运算,并签名,产生Sig_{skf}(T),并将Sig_{skf}(T)作为新鲜性保护的根存放在安全芯片的非易失存储区中。

[0030] (2)可信数据库系统启动过程

[0031] 在每次可信数据库系统启动前,都必须由新鲜性保护模块完成如下过程:

[0032] a)新鲜性保护模块重新度量操作系统中的每个数据库文件的哈希值,并从新鲜性保护数据表T(FileID,Sig_{skf}(File))中查询其对应的签名值,验证该文件的签名值和哈希值是否正确;

[0033] b)若在新鲜性保护数据表T中,有某文件查询不到它对应的签名值,则向管理员报警,并退出启动流程;

[0034] c)若存在某文件的签名值或哈希值不正确,则向管理员报警,并退出启动流程;

[0035] d)若操作系统中所有数据库文件都有对应的签名值,且其签名值或哈希值都正确,则进一步对新鲜性保护数据表T进行哈希运算,并从安全芯片的非易失存储区中查询签名Sig_{skf}(T),验证T的签名值和哈希值的正确性,若不正确则向管理员报警,并退出启动流程,否则继续可信数据库系统的正常启动。

[0036] (3)可信数据库系统关闭过程

[0037] 在每次可信数据库系统关闭后,都必须由新鲜性保护模块完成如下过程:

[0038] a)新鲜性保护模块重新度量操作系统中的每个数据库文件的哈希值,并利用skf对其进行签名,然后更新到新鲜性保护数据表T(FileID,Sig_{skf}(File))中;

[0039] b)新鲜性保护模块对新鲜性保护数据表T进行哈希运算,并用skf签名产生Sig_{skf}(T),再存储到安全芯片的非易失存储区中。

[0040] 在上述过程中,由于可信数据库系统运行期间受到工控系统可信环境管控平台对其运行环境的保护,因此攻击者无法在其运行过程中侵入系统环境,并进行重放攻击。而上述过程又保证了可信数据库系统在关闭后到开启前一段时间内,攻击者对存储于硬盘上的数据库文件的新鲜性破坏能够被检测出来,因此能够确保存储于可信数据库中的重要数据的新鲜性。

[0041] 本发明的有益效果如下:

[0042] (一)可以通过数据安全性分析平台对所有进程进行分析,安全管理员再基于分析结果来建立白名单,并通过工控系统可信环境管控平台来阻止白名单之外的进程在工控系统中运行。因此,确保了实际运行中的工控系统环境只含有经过分析的可信的进程。

[0043] (二)将工控系统中的一些重要参数等敏感数据及本发明中工控系统安全支撑平台的安全相关数据都存储在可信数据库系统中,可以有效确保它们的机密性和完整性。这

种安全保护是建立在安全芯片的硬件基础上，因此具有更高的安全性。

[0044] (三)在工控网络中部署可信工控系统防火墙能够对网络中的攻击行为进行有效隔离，提高工控网络的安全性。

[0045] (四)可信移动介质管控系统的部署能够有效抑制病毒、木马等恶意代码通过移动介质在工控系统中进行传播。

[0046] (五)数据安全性分析平台能够为工控系统安全管理员提供对未知文件、进程的安全性分析，并且不需要特征库的支持，也避免的频繁升级和更新，更加适合工控系统。

[0047] (六)在上述组成部分之间的重要数据的传输和存储都基于安全芯片实施了保护，覆盖了数据传输和存储的完整的三个阶段——数据从源主机到目的主机的传输阶段、数据到达目的主机后及被存储前的阶段、数据存储阶段，有效确保了本发明的工业控制系统安全支撑平台各组成部分相互之间可信的数据流动，进而加强了整体系统的安全性。

附图说明

[0048] 图1是工业控制系统安全支撑平台架构示意图；

[0049] 图2是工业控制系统安全支撑平台部署及实施方法示意图。

具体实施方式

[0050] 下面将对发明内容中所描述的工业控制系统安全支撑平台的具体部署和实施方法进行示例性解释，但不以这种解释限制发明的范围。

[0051] 首先，工控系统可信环境管控平台通常实现为客户端/服务端架构。客户端部署于需要可信环境管控的工控终端或工控服务器上，例如工程师站、操作员站等。而为了不影响现有工控系统的架构，服务端通常部署于独立的安全服务器上。这种实现方式不会对工控系统的稳定性和可靠性造成影响。

[0052] 可信数据库系统部署于数据库服务器上，与工控系统可信环境管控平台、可信工控系统防火墙、可信移动介质管控系统这三个安全支撑平台的其他组成部分连接，为安全相关数据提供安全存储。此外，它还会与工业控制系统进行连接，为一些非实时的工控系统敏感数据提供安全存储。

[0053] 可信工控系统防火墙部署于工控网络的不同网络层之间，实现它们之间的隔离，例如现场设备层与车间监控层之间等。具体地，可信工控防火墙也将采用客户端/服务端架构，即在需要隔离的网络之间部署防火墙的客户端来执行具体的网络规则，而其服务端部署于前述的安全服务器上来管理和维护这些网络规则。

[0054] 可信移动介质管控系统通常也被实现为客户端/服务器架构。客户端部署于需要移动介质管控的工控终端或工控服务器上，例如工程师站、操作员站等。而服务端则往往部署于独立的安全服务器上，可以与工控系统可信环境管控平台的服务端位于同一安全服务器。

[0055] 而数据安全性分析平台需要对可能恶意的文件进行分析，因此需要单独位于一个安全服务器上，并在它与安全支撑平台其他部分之间部署可信工控系统防火墙进行隔离。该分析平台的分析结果一般会包括两个方面的内容：其一，通过模拟文件的预期使用环境，并收集该文件在该模拟环境下的运行情况，得到文件在预期环境下的所有行为；其二，依据

预先定义的恶意行为判定规则，这些行为是否具有恶意性。对于后者，管理员可以直接利用它对工控系统的整体安全性进行管理和维护。而前者可以被用于进一步的分析，以不断提高恶意行为判定规则的准确性。

[0056] 而发明内容中用于连接各个部件，并保护其中数据传输和存储安全性的安全传输方法和安全存储方法，可以采用软件调用安全芯片相应功能的方式来实现，而软件实现的部分必须位于本发明的工控系统可信环境管控平台所保护的系统环境中，即白名单列表中。

[0057] 最后，给出一个具体的例子来进一步解释说明本发明内容。

[0058] 首先，工控系统的工程师站等工控终端或工控服务器在部署了工控系统可信环境管控平台的客户端后，将按照服务端预先定义且签名过的进程白名单对本地的系统环境进行可信管理，阻止一切白名单外的进程启动。也就是通过可信计算技术实现系统的安全启动，在启动过程及后继新启动进程时对进程进行度量，并与白名单进行比较，确保度量结果和比较结果的可信性。若该进程不在白名单中，则被阻止运行。而白名单是可以由管理员在服务端进行审核和管理的。因此，能够确保工控系统中运行的进程都是经过管理员批准的，恶意或未知的进程都是无法在系统中运行的。

[0059] 其二，可信数据库能够基于可信芯片提供的存储信任根将上述白名单及其他的一些敏感数据进行安全保护。可信数据库可以利用存储信任根生成并保护两对公私钥，分别用于加密和签名。加密密钥用于对存储在数据库中的敏感数据进行机密性保护，签名密钥则用于完整性保护。并且在可信计算技术中，这两对密钥的使用环境可以被管理员指定为预期的安全环境。在这种情况下，一旦环境发生变化，则加密密钥和签名密钥就无法被正常使用，数据库中的敏感数据则无法被解密，也无法产生正确的签名值，从而确保敏感数据的使用必须在安全环境中。而存储信任根又位于安全芯片内部，攻击者要非法获取它就必须攻破硬件芯片，极大地提高了数据的安全性。

[0060] 其三，可信工控系统防火墙被用于不同网络层或区域之间的隔离。通过对工控协议的解析，能够识别出一些恶意的数据包。例如，包含有非法的控制符或使用了可疑端口等的数据包将被防火墙阻拦，并发出警报。虽然防火墙的具体访问控制规则需要管理员根据实际的环境进行配置，但是防火墙对于工控协议解析的支持是不可或缺的。只有防火墙能够解析更多的协议，其对于访问控制规则的描述和实施能力才会更强。这些访问控制规则将采用上述的可信数据库进行安全存储，以确保不会被攻击者篡改。

[0061] 其四，可信移动介质管控系统的客户端将被部署于每个可以插入移动介质的主机上，由其为主机执行移动介质的识别，并依照预先定义的规则进行准入控制。例如，移动介质A不允许插入主机X等规则。这些规则是由可信移动介质管控系统的服务端进行统一配置和管理的。而这些规则也将被存入可信数据库进行安全保护，以确保不会被攻击者篡改。此外，用户在使用移动介质前，移动介质中存放的未知数据文件还将被提交给数据安全性分析平台进行分析，一旦发现恶意文件，则该移动介质将被禁止使用。

[0062] 最后，数据安全性分析平台是为整个工业控制系统安全支撑平台提供恶意代码分析支持的。也就是说，通过网络或移动介质方式出入工控系统的工控终端、工控服务器的数据文件都可以提交给数据安全性分析平台，对其行为进行分析检测，判定其是否为恶意的。此外，在工控系统初始化安装或后期升级时，对于要新加入工控系统可信环境管控平台白

名单的进程，管理员可以利用数据安全性分析平台对它们进行分析，确保其不包含漏洞利用代码等恶意代码，然后再将它们加入白名单，从而确保工控系统可信环境管控平台根据白名单所维护的环境是真正安全的。

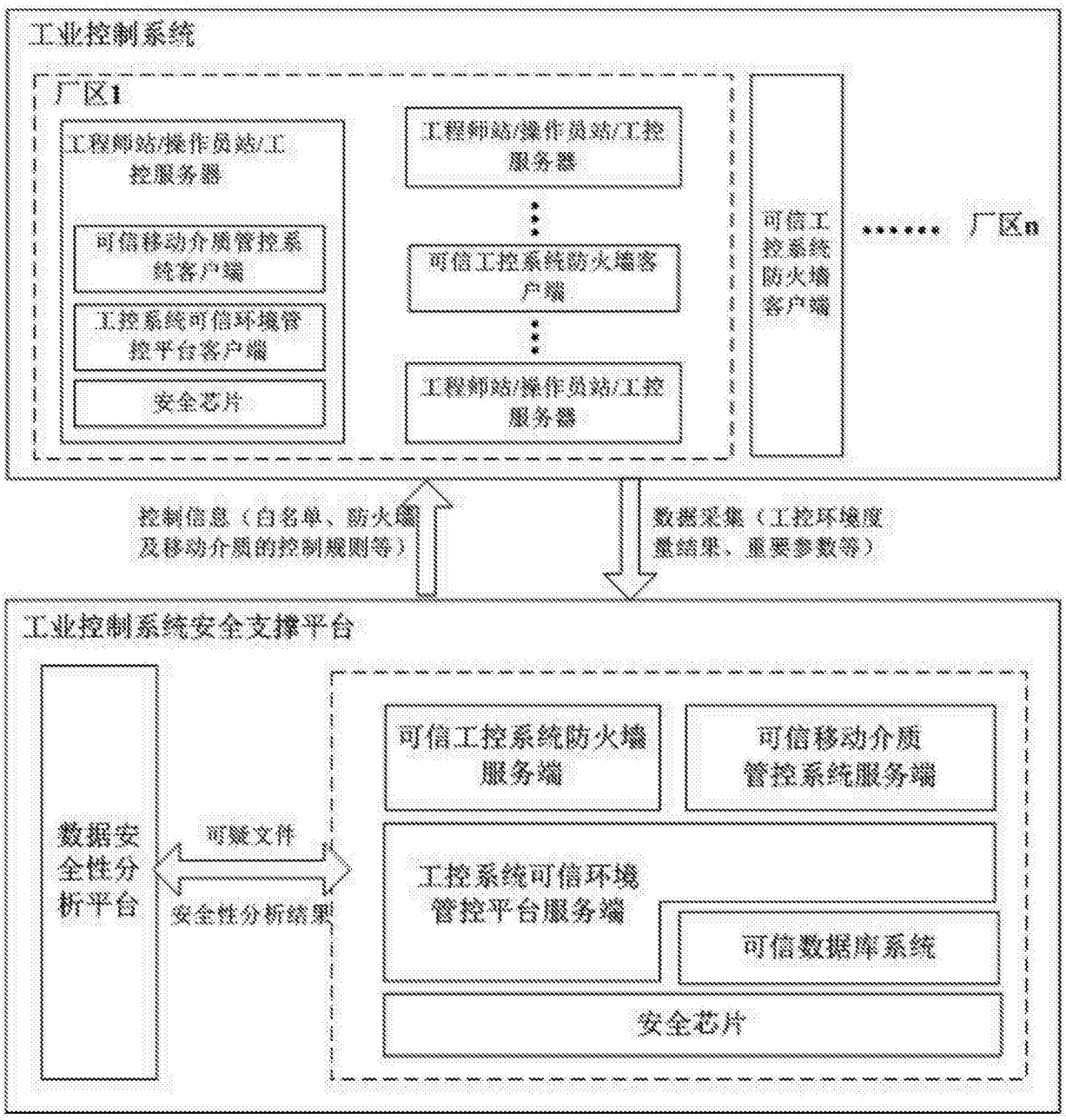

工业控制系统
厂区1
工程师站/操作员站/工控服务器
可信移动介质管控系统客户端
工控系统可信环境管控平台客户端
安全芯片
工程师站/操作员站/工控服务器
可信工控系统防火墙客户端
工程师站/操作员站/工控服务器
可信工控系统防火墙客户端
厂区n
控制信息（白名单、防火墙及移动介质的控制规则等）
数据采集（工控环境度量结果、重要参数等）
工业控制系统安全支撑平台
数据安全性分析平台
可疑文件
安全性分析结果
可信工控系统防火墙服务端
可信移动介质管控系统服务端
工控系统可信环境管控平台服务端
可信数据库系统
安全芯片

图1

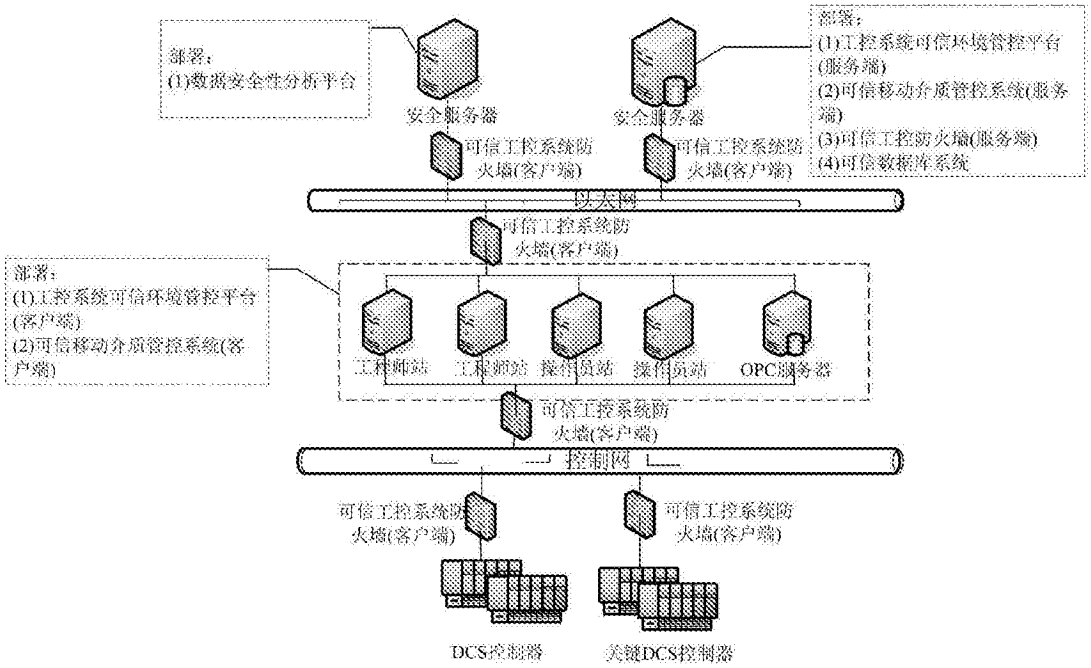

部署：
(1)数据安全性分析平台
安全服务器
安全服务器
部署：
(1)工控系统可信环境管控平台(服务端)
(2)可信移动介质管控系统(服务端)
(3)可信工控防火墙(服务端)
(4)可信数据库系统
可信工控系统防火墙(客户端)
可信工控系统防火墙(客户端)
以太网
可信工控系统防火墙(客户端)
部署：
(1)工控系统可信环境管控平台(客户端)
(2)可信移动介质管控系统(客户端)
工程师站
工程师站
操作员站
操作员站
OPC服务器
可信工控系统防火墙(客户端)
控制网
可信工控系统防火墙(客户端)
可信工控系统防火墙(客户端)
DCS控制器
关键DCS控制器

图2