(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 104756132 B
(45)授权公告日 2018.07.31

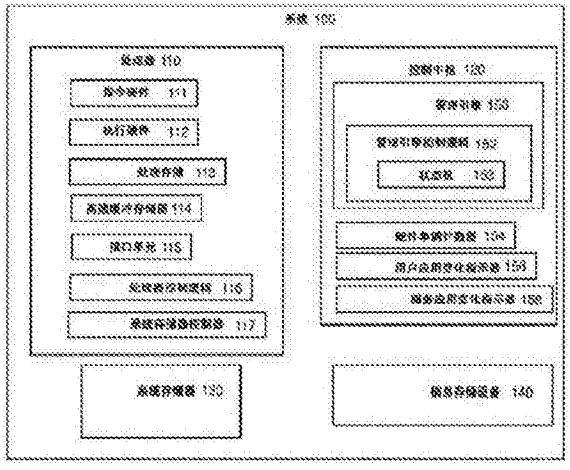
(21)申请号 201380057240.9
(22)申请日 2013.06.24
(65)同一申请的已公布的文献号
申请公布号 CN 104756132 A
(43)申请公布日 2015.07.01
(30)优先权数据
13/690,111 2012.11.30 US
(85)PCT国际申请进入国家阶段日
2015.04.30
(86)PCT国际申请的申请数据
PCT/US2013/047257 2013.06.24
(87)PCT国际申请的公布数据
WO2014/084908 EN 2014.06.05
(73)专利权人 英特尔公司
地址 美国加利福尼亚州
(72)发明人 S·查博拉 R·拉尔 J·马丁 D·涅米罗夫
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 高见
(51)Int.Cl.
G06F 21/71(2013.01)
G06F 21/50(2013.01)
G06F 21/54(2013.01)
(56)对比文件
US 2008/0320263 A1,2008.12.25,说明书第36段.
Luis F. G. Sarmenta,et al.Virtual Monotonic Counters and Count-Limited Objects using a TPM without a Trusted OS.《New York:ACM,2006》.2006,正文第1,5,6页,第7页第1栏,第12页第1栏,附图1.
审查员 陈玲
权利要求书2页 说明书7页 附图4页

(54)发明名称

虚拟化硬件单调计数器

(57)摘要

公开了用于虚拟化硬件单调计数器的发明的各实施例。在一种实施例中,一种装置包括硬件单调计数器、虚拟化逻辑、第一非易失性存储位置和第二非易失性存储位置。虚拟化逻辑从硬件单调计数器创建虚拟单调计数器。第一非易失性存储位置存储硬件单调计数器的计数已经变化的指示器。第二非易失性存储位置存储虚拟单调计数器的计数已经变化的指示器。



CN 104756132 B

1.一种用于虚拟化硬件单调计数器的装置,包括:

硬件单调计数器;

虚拟化逻辑,用于从所述硬件单调计数器创建虚拟单调计数器;

第一可清除非易失性存储位置,用于存储指示对所述硬件单调计数器的变化的第一指示器;

第二可清除非易失性存储位置,用于存储指示对所述虚拟单调计数器的变化的第二指示器;以及

逻辑,用于检测是否所述第一指示器已被设置而所述第二指示器尚未被设置,用于检测是否所述第一指示器和所述第二指示器已被设置,以及用于检测是否所述第一指示器已被清除而所述第二指示器已被设置,从而在掉电时提供所述虚拟单调计数器的正确操作。

2.如权利要求1所述的装置,其特征在于,进一步包括安全飞地逻辑,用于创建存储所述虚拟单调计数器计数的计数的第一安全飞地。

3.如权利要求2所述的装置,其特征在于,所述安全飞地逻辑也创建使用所述虚拟单调计数器的所述计数的第二安全飞地。

4.一种用于虚拟化硬件单调计数器的方法,包括:

将虚拟单调计数器的计数存储在数据结构中;

使用硬件单调计数器的计数密封所述数据结构;

响应于接收到递增所述硬件单调计数器的请求设置第一可清除非易失性存储位置中的服务应用变化指示器,以指示对所述硬件单调计数器的变化;

递增所述虚拟单调计数器的所述计数且设置第二可清除非易失性存储位置中的用户应用变化指示器,以指示对所述虚拟单调计数器的变化;以及

检测是否所述服务应用变化指示器已被设置而所述用户应用变化指示器尚未被设置,检测是否所述服务应用变化指示器和所述用户应用变化指示器已被设置,以及检测是否所述服务应用变化指示器已被清除而所述用户应用变化指示器已被设置,从而在掉电时提供所述虚拟单调计数器的正确操作。

5.如权利要求4所述的方法,其特征在于,进一步包括将用户标识符存储在所述数据结构中,以标识所述虚拟单调计数器的用户。

6.如权利要求5所述的方法,其特征在于,进一步包括使用所述虚拟单调计数器的所述计数来密封数据团。

7.如权利要求6所述的方法,其特征在于,进一步包括创建用于存储所述数据结构的服务安全飞地。

8.如权利要求7所述的方法,其特征在于,进一步包括创建用于存储所述数据团的用户安全飞地。

9.如权利要求8所述的方法,其特征在于,进一步包括在所述用户安全飞地和所述服务安全飞地之间创建第一可信路径。

10.如权利要求9所述的方法,其特征在于,进一步包括在所述服务安全飞地和拥有对所述硬件单调计数器的访问权的会话管理器之间创建第二可信路径。

11.如权利要求10所述的方法,其特征在于,进一步包括由在所述用户安全飞地中运行的用户应用调用在所述服务安全飞地中运行的服务应用,以递增所述虚拟单调计数器。

12.如权利要求10所述的方法，其特征在于，进一步包括由所述服务应用响应于接收到递增所述虚拟单调计数器的请求调用所述会话管理器，以递增所述硬件单调计数器。

13.如权利要求12所述的方法，其特征在于，进一步包括在所述硬件单调计数器变化已经传播到所述服务安全飞地之后清除所述服务应用变化指示器。

14.如权利要求12所述的方法，其特征在于，进一步包括在所述虚拟单调计数器变化已经传播到所述用户安全飞地之后清除所述用户应用变化指示器。

15.一种用于虚拟化硬件单调计数器的系统，包括：

管理引擎，包括

硬件单调计数器，

虚拟化逻辑，用于从所述硬件单调计数器创建虚拟单调计数器，

第一可清除非易失性存储位置，用于存储指示所述硬件单调计数器已经变化的第一指示器，

第二可清除非易失性存储位置，用于存储指示所述虚拟单调计数器已经变化的第二指示器；以及

逻辑，用于检测是否所述第一指示器已被设置而所述第二指示器尚未被设置，用于检测是否所述第一指示器和所述第二指示器已被设置，以及用于检测是否所述第一指示器已被清除而所述第二指示器已被设置，从而在掉电时提供所述虚拟单调计数器的正确操作；以及

处理器，包括安全飞地逻辑，所述安全飞地逻辑用于创建存储所述虚拟单调计数器计数的计数的第一安全飞地和使用所述虚拟单调计数器计数的所述计数的第二安全飞地。

16.如权利要求15所述的系统，其特征在于，所述安全飞地逻辑包括用于加密由安全飞地存储的信息的加密单元。

17.如权利要求15所述的系统，其特征在于，所述安全飞地逻辑包括用于把安全存储器空间分配给安全飞地的安全飞地范围寄存器。

18.如权利要求15所述的系统，其特征在于，所述安全飞地逻辑包括用于防止访问由安全飞地高速缓存的未加密信息的访问控制逻辑。

19.一种或多种其上存储有指令的计算机可读介质，所述指令当由计算机处理器执行时使所述处理器执行如权利要求4至14中任一项所述的方法。

20.一种用于虚拟化硬件单调计数器的设备，包括用于执行如权利要求4至14中任一项所述的方法的装置。

虚拟化硬件单调计数器

[0001] 背景

[0002] 1.领域

[0003] 本公开内容涉及信息处理的领域，且尤其涉及信息处理系统中的安全性的领域。

[0004] 2.相关领域的描述

[0005] 在信息处理系统中，保护信息的安全性的技术可以包括使用单调计数器。例如，可以在消息中包括单调计数器值，以便保护该消息免遭重放攻击。

[0006] 附图简述

[0007] 在附图中，作为示例而非限制阐释本发明。

[0008] 图1阐释其中可以根据本发明的一个实施例虚拟硬件单调计数器的系统。

[0009] 图2阐释的一种系统架构。

[0010] 图3阐释根据本发明的一个实施例初始化虚拟单调计数器的方法。

[0011] 图4阐释根据本发明的一个实施例使用虚拟单调计数器的方法。

[0012] 详细描述

[0013] 描述用于虚拟化硬件单调计数器的发明的各实施例。在这一描述中，可以陈述诸如组件和系统配置之类的众多特定细节，以便提供对本发明的更透彻的理解。然而，本领域中的技术人员应明白，无需这样的特定的细节就可以实践本发明。另外，没有详细示出一些众所周知的结构、电路和其他特征，以免不必要地模糊本发明。

[0014] 在下列描述中，对“一种实施例”、“实施例”、“示例实施例”、“各种实施例”等等的引用表示本发明的(多个)实施例可以包括具体的特征、结构或特性，但是多于一种的实施例可以包括、且并非每一实施例必定包括这些具体的特征、结构或特性。进一步，一些实施例可以拥有针对其他实施例所描述的特征中的一些、全部或没有这些特征。

[0015] 而且，可以使用术语“比特”、“标志”、“字段”、“条目”等等来描述寄存器、表、数据库或其他数据结构中的任何类型的存储位置，无论是以硬件实现还是以软件实现，但不预期把本发明的各实施例限制在任何具体存储位置内的任何具体类型的存储位置或比特或其他元素的数量。可以使用术语“清除”来表示把逻辑值0存储在一个存储位置中或以另外方式引起0逻辑值被存储在一个存储位置中，且可以使用术语“设置(set)”来表示把逻辑值1、全部1或某种其他所指定的值存储在一个存储位置中或以另外方式引起它们被存储在一个存储位置中；然而，这些术语不旨在把本发明的各实施例限制在任何具体的逻辑约定，这是因为在本发明的各实施例内可以使用任何逻辑约定。术语“递增”可以用来表示增加1，但其中“递增”可以表示增加固定值的本发明的各实施例是可能的，且在其他实施例中可能的情况是递减或减少而不是递增或增加。然而，不描述每一种这样的可能性。

[0016] 如权利要求中所使用的，除非以另外方式指定，否则，使用序数形容词“第一”、“第二”、“第三”等等来描述一个元素仅仅表示所提及的类似元素的不同实例，且不旨在暗示所述的元素必须处于具体的序列，无论是时间上、空间上、排名上或任何其他方式。

[0017] 如背景部分中所描述的，信息处理系统中的单调计数器可以用于保护信息的安全性的技术。然而，信息处理系统可以拥有有限数量的硬件单调计数器。因此，可以期望本发

明的各实施例通过虚拟化提供额外的单调计数器的使用。可以根据需要增加可供使用的虚拟单调计数器的数量，即使在硬件单调计数器的数量受到限制的时候也是如此，在这一意义上，本发明的各实施例是可扩展的。例如，通过即使在掉电的时候也提供正确的操作，使得使用虚拟单调的计数器密封的信息的安全性不受重置或断电攻击危害，本发明的各实施例也是稳健的。

[0018] 图1阐释系统100，系统100是本发明的一种实施例可以在其中存在和/或操作信息处理系统。系统100可以表示任何类型的信息处理系统，例如服务器、台式计算机、便携式计算机、机顶盒、手持式设备或嵌入式控制系统。系统100包括处理器110、控制中枢120、系统存储器130和信息存储设备140。实现本发明的系统可以包括任何数量的这些组件中的每一个和任何其他组件或其他元件，例如外围设备和/或输入/输出设备。任何系统实施例中的组件或其他元件中的任何或全部可以通过任何数量的总线、对等或其他有线或无线连接相互连接、耦合或以另外方式通信。

[0019] 处理器110可以表示被集成在单个衬底上或被封装在单个封装内的一个或多个处理器，其中的每一个都可以包括以任何组合的多个线程和/或多个执行核。被表示为处理器110的每一处理器可以是任何类型的处理器，包括通用微处理器，例如英特尔®Core®处理器系列、英特尔®Atom®处理器系列或英特尔®公司的其他处理器系列中的处理器，或来自另一公司的另一处理器，或专用处理器或微控制器。处理器110可以包括指令硬件111、执行硬件112、处理存储113、高速缓冲存储器114、接口单元115和处理器控制逻辑116。处理器110也可以包括图1中未示出的任何其他电路、结构或逻辑和/或图1中其他地方示出或描述的任何电路、结构或逻辑。例如，系统存储器控制器117可以被集成在处理器110的衬底上或被封装在处理器110的封装内。

[0020] 指令硬件111可以表示用于提取、接收、解码和/或调度指令的任何电路、结构或其他硬件，例如指令解码器。在本发明的范围内可以使用任何指令格式；例如，指令可以包括操作码和一个或多个操作数，其中操作码可以被解码成供由执行硬件112执行的一个或多个微指令或微操作。

[0021] 执行硬件112可以包括用于处理数据和执行指令、微指令和/或微操作的任何电路、结构或其他硬件，例如运算单元、逻辑单元、浮点单元、移位器等等。

[0022] 处理存储113可以表示在处理器110内可用于任何目的任何类型的存储；例如，它可以包括任何数量的数据寄存器、指令寄存器、状态寄存器、配置寄存器、控制寄存器、其他可编程或硬编码寄存器或寄存器堆、或任何其他存储结构。

[0023] 高速缓冲存储器114可以表示信息处理系统100中的存储器层次中的、以静态随机存取存储器或任何其他存储器技术实现的任何一个或多个级别的高速缓冲存储器。高速缓冲存储器114可以包括专用于在处理器110内的任何一个或多个执行核心或处理器或在它们当中共享的、根据在信息处理系统中缓存的任何已知方法的高速缓冲存储器的任何组合。

[0024] 接口单元115可以表示任何电路、结构或其他硬件，例如总线单元、消息收发单元或任何其他单元、端口或接口，以便允许处理器110通过任何类型的总线、点对点或其他连接直接地与系统100中的其他组件通信，或通过诸如存储器控制器或总线桥之类的任何其他组件与系统100中的其他组件通信。

[0025] 处理器控制逻辑116可以包括任何逻辑、电路、硬件或其他结构，包括微代码、状态机逻辑或可编程逻辑，以便控制处理器110的各单元和其他元件的操作以及在处理器110内、进入到处理器110、离开处理器110的数据传输。例如通过引起处理器110执行指令硬件111所接收的指令和从指令硬件111所接收的指令导出的微指令或微操作，处理器控制逻辑116可以引起处理器110执行或参与本发明的方法实施例(例如下面描述的方法实施例)的执行。

[0026] 控制中枢120可以包括任何逻辑、电路或其他硬件，以便控制或促进在处理器110、系统存储器130、信息存储设备140和信息处理系统100中的任何其他组件之间、和/或信息处理系统100的任何其他操作或功能性之间的信息传输。控制中枢120可以包括管理引擎150，管理引擎150可以表示处理器、控制器或任何其他逻辑、电路或其他硬件，以便向独立于处理器110的信息处理系统的信息处理系统100提供可管理性、维护、安全和/或虚拟化功能。例如，管理引擎150可以表示支持英特尔®主动管理技术的可管理性引擎。

[0027] 管理引擎150可以包括管理引擎控制逻辑152、一个或多个硬件单调计数器154，用户应用变化指示器156和服务应用变化指示器158。管理引擎控制逻辑152可以包括任何逻辑、电路、硬件或其他结构，包括微代码、状态机逻辑、可编程逻辑或固件，以便控制管理引擎150的操作并引起管理30引擎150执行或参与本发明的方法实施例的执行。

[0028] 硬件单调计数器(monotonic counter)154可以包括根据任何已知的方法实现单调计数器的电路或其他硬件。在一种实施例中，硬件单调计数器154可以表示被用于根据本发明的各实施例使用、指定或者保留以供使用的一组硬件单调计数器中的一个；例如，它可以表示英特尔®可管理性引擎的一组五个硬件单调计数器中的一个。

[0029] 用户应用变化指示器156和服务应用变化指示器158都可以是存储根据本发明的方法实施例使用的诸如一比特之类的指示器的非易失性数据存储元件。在一种实施例中，管理引擎控制逻辑152可以包括状态机153，状态机153可以使用用户应用变化指示器156和服务应用变化指示器158的状态来确保稳健性，即使在掉电时也是如此，如下面所描述。

[0030] 系统存储器130可以包括动态随机存取存储器和/或可由处理器110访问的任何其他类型的介质，且可以被用来存储由处理器110和/或任何其他组件使用或产生的数据和/或指令。

[0031] 信息存储设备140可以表示任何类型的非易失性信息存储设备，例如闪速存储器或硬盘驱动器。

[0032] 图2阐释根据本发明的一种实施例的系统架构200，示出执行、被加载到或以另外方式出现在诸如信息处理系统100之类的信息处理系统内的服务应用261和用户应用271。在图2中，服务应用261和用户应用271可以各自表示在诸如下面所描述的安全飞地(enclave)之类的安全的、受保护的或隔离的环境内的应用。对于本描述的目的，这样的环境的每一实例都可以被称为安全飞地，尽管本发明的各实施例不限于把安全飞地用作服务应用261和用户应用271的环境的那些。在图2中，服务应用261被示出为处于服务安全飞地260，且用户应用271被示出为处于用户安全飞地270。

[0033] 可以使用英特尔®Core®处理器系列或来自英特尔®公司其他处理器系列中的处理器的指令集中的指令来创建和维护安全飞地，其支持硬件由处理器210中的安全飞地逻辑216表示，处理器210可以对应于图1中的处理器110。安全飞地逻辑216可以被包括在处理

器210的任何一个或多个单元内，例如对应于处理器110的指令硬件111、执行硬件112和处理器控制逻辑116的那些单元。安全飞地逻辑216可以包括加密单元212，加密单元212可以包括执行一种或多种加密算法和相应的解密算法的任何逻辑、电路或其他硬件。

[0034] 可以在系统存储器空间230内给在系统架构200内创建的每一安全飞地分配安全的或受保护的空间。例如，可以把服务安全存储器空间262分配给用于服务应用261的安全飞地，且可以把用户安全存储器空间272分配给用于用户应用271的安全飞地。可以使用已知的虚拟存储器、安全飞地或其他系统存储器编址技术来创建、分配和维护每一个这样的存储器空间，以使得可以在各个时刻把在每一这样的存储器空间内的信息存储在信息存储设备140、系统存储器130、高速缓冲存储器114和/或在信息处理系统100内任何其他存储器或存储区域的任何组合内。

[0035] 在安全飞地的存储器空间内的信息仅可由在该安全飞地中运行的应用访问。例如，分配给安全飞地的存储器页面上的信息在被存储在系统存储器130、存储设备140或外置于处理器210的任何其他存储器或存储中之前，可以由加密单元212来加密。尽管被存储在处理器210外，但这一信息受到加密和完整性检查技术的保护。当这一存储器页面被在处理器210上、在分配给它的安全飞地内运行的应用或进程加载到高速缓冲存储器114时，由加密单元212解密该存储器页面，然后，经解密的信息仅可由在安全飞地内运行的应用或进程访问。由安全飞地逻辑216强加这些加载和访问限制，出于这一目的，安全飞地逻辑216可以包括安全飞地范围寄存器213、访问控制逻辑214和任何其他已知的逻辑、电路或其他硬件。

[0036] 在图2中，用户应用271和服务应用261可以通过可信路径265相互通信，且在管理引擎250上运行的服务应用261和会话管理器251可以通过可信路径255相互通信。可信路径255和265可以各自表示根据确保通信的完整性和机密性的任何已知方法实现的可信路径或信道。可信路径255的机制可以包括会话管理器251和服务应用261的相互认证；可信路径265的机制可以包括服务应用261和用户应用271的相互认证。可信信道255和265上的认证和/或通信协议可以使用密钥；例如，每当服务应用261被重启时，会话管理器251和服务应用261可以使用主密钥257来导出辅密钥259；服务应用261和用户应用271可以使用密钥267。

[0037] 图3阐释根据本发明的一个实施例用于初始化虚拟单调计数器的方法300。尽管本发明的方法实施例不限于这一方面，但可以参见图1和图2的元素来帮助描述图3的方法实施例。

[0038] 在方法300的框310中，可以清除用户应用变化指示器156和服务应用变化指示器158，例如，作为管理引擎150的初始化序列或进程的一部分。

[0039] 在框320中，可以创建安全飞地(例如，服务安全飞地260)，用于运行服务应用(例如，服务应用261)。运行服务应用261的一个目的可以是提供虚拟化硬件单调计数器(例如，硬件单调计数器154)。在框322中，可以创建另一安全飞地(例如，用户安全飞地270)，用于运行用户应用(例如，用户应用271)。可以出于任何目的运行用户应用271，且可以期望用户应用271把单调计数器用于任何目的。

[0040] 例如，可以期望用户应用271把单调计数器用于提供经密封的存储，其中可保护信息(例如，数据二进制大对象或“团(blob)”295)免遭重放攻击。在本描述中，对使用单调计

数器来为信息提供密封存储的任何引用都可以包括把当前单调计数器值附加到数据团，以使得在读取该数据团时，可以判断该数据是否已经被重放(例如，如果所附加的单调计数器值比当时的单调计数器值旧)或被攻击(例如，如果所附加的单调计数器值比当时的单调计数器值新)，或任何其他这样的已知方法。也可以把其他值(例如在单调计数器已被重置时产生的随机数)附加到数据团，以使得在读取该数据团时，可以判断自从存储了该数据团之后该单调计数器是否已被重置，以及/或者附加完整性检查值。任何这些方法可以包括使用防重放(anti-replay)表，在防重放表中存储对应于数据团的单调计数器值、随机数和/或完整性检查值。任何这样的已知方法可以用于本发明的各实施例，且本描述中对把单调计数器值附加到数据团的任何引用也可以包括根据这些方法的技术。

[0041] 在框324中，为在用户应用271和服务应用261之间的双向通信建立可信路径(例如，可信路径265)。在框326中，为在服务应用261和会话管理器251之间的双向通信建立可信路径(例如，可信路径255)。

[0042] 在框330中，用户应用271通过可信路径265向服务应用261发送使用单调计数器的请求。

[0043] 在框340中，服务应用261创建用来提供单调计数器的虚拟化的数据结构(例如，数据库280)。数据库280可以是包括任何数量的条目的数据表，且每一条目(例如，条目281)可以包括用于存储用户应用的标识符的第一字段(例如，ID字段282)和用于存储被分配给相应用户应用的虚拟单调计数器的当前计数值的第二字段(例如，虚拟计数字段283)。在框342中，服务应用261把ID字段282设置为用户应用271和/或用户安全飞地270的标识符；例如，它可以是对用户应用271和/或用户安全飞地270来说唯一的值，该值从出于身份、完整性或任何其他目的而做出的度量或其他报告导出。

[0044] 在框350中，服务应用261通过可信路径255向会话管理器251发送对硬件单调计数器154的当前计数值的请求。在框352中，服务应用261接收硬件单调计数器154的当前计数值155。在框354中，服务应用261把硬件单调计数器154的当前计数值155存储在服务安全存储器空间262中的硬件计数字段263中。

[0045] 在框中354，可以把虚拟计数字段283初始化成例如预先确定的初始化值、硬件单调计数器154的当前计数值或任何其他值。在框356中，可以把虚拟计数字段283的值发送给用户应用271以便初始化用户安全存储器空间272中的用户计数字段293，该字段表示由服务应用261提供给用户应用271的虚拟单调计数器(例如，虚拟单调计数器294)的计数。

[0046] 在框360中，服务应用261使用硬件计数字段263中的值来密封数据库280，例如通过把硬件计数字段263中的值附加到表示数据库280的内容的数据团并将该结果存储在服务安全存储器空间262中。

[0047] 在框370中，服务应用261为递增虚拟单调计数器294的请求做好准备。数据库280的条目281的ID字段282正在存储用户应用271和/或用户安全飞地270的标识符。数据库280的条目281的虚拟计数字段283和用户安全存储器空间272中的用户计数字段293存储相同的值。服务安全存储器空间262中的硬件计数字段263存储硬件单调计数器154的当前计数值155。已经用硬件计数字段263中的值密封服务安全存储器空间262中的数据库280。用户应用变化指示器156和服务应用变化指示器158已经被初始化为零。

[0048] 图4阐释根据本发明的一个实施例使用虚拟单调计数器的方法400。尽管本发明的

方法实施例不限于这一方面，但可以参见图1、图2和图3的元素来帮助描述图4的方法实施例。该方法可以被描述为在电源失效的时候继续进行到特定的框；在一些实施例中，电源故障也可以是指包括其他中断。

[0049] 在方法400的框410中，服务应用261为递增虚拟单调计数器294的请求做好准备，例如，方法400的框410可以对应于方法300的框370。数据库280的条目281的ID字段282存储用户应用271和/或用户安全飞地270的标识符。数据库280的条目281的虚拟计数字段283和用户安全存储器空间272中的用户计数字段293存储相同的值。服务安全存储器空间262中的硬件计数字段263存储硬件单调计数器154的当前计数值155。已经用硬件计数字段263中的值密封服务安全存储器空间262中的数据库280。用户应用变化指示器156和服务应用变化指示器158已经被初始化为零。

[0050] 在框420中，用户应用271调用服务应用261以便递增虚拟单调计数器294。在框422中，服务应用261调用会话管理器251以便递增硬件单调计数器154。

[0051] 在框424中，会话管理器251递增硬件单调计数器154，且会话管理器251把服务应用变化指示器158设置为指示对硬件单调计数器154的变化可能尚未传播到服务应用261。在框中426，会话管理器251返回到服务应用261。

[0052] 在框430中，服务应用261递增虚拟计数字段283并且把用户应用变化指示器156设置为指示对虚拟计数字段283的变化可能尚未传播到用户应用271。在框432中，服务应用261递增硬件计数字段263。在框434中，服务应用261使用硬件计数字段263来密封数据库280。

[0053] 在框440中，服务应用261调用会话管理器251以便清除服务应用变化指示器158。在框中442，会话管理器251清除服务应用变化指示器158。在框中444，会话管理器251返回到服务应用261。在框中446，服务应用261返回到用户应用271。

[0054] 在框中450，用户应用271递增用户计数字段293。在框中452，用户应用271使用用户计数字段293来密封数据团295。在框中454，用户应用271调用服务应用261来清除用户应用变化指示器156。在框中456，服务应用261调用会话管理器251来清除用户应用变化指示器156。在框中458，会话管理器251清除用户应用变化指示器156。

[0055] 在框中460，会话管理器251返回到服务应用261。在框中462，服务应用261返回到用户应用271。

[0056] 服务应用变化指示器158和用户应用变化指示器156可以被用来在电源失效的情况下提供稳健性。在电源失效来自框424或426中的任何的情况下，该流程可以在框430中继续，这是因为可以检测到已经设置了服务应用变化指示器156但是没有设置用户应用变化指示器158。在电源失效来自框430、432、434或440中的任何的情况下，该流程可以在框432中继续，这是因为可以检测到已经设置了服务应用变化指示器156和用户应用变化指示器158。在电源失效来自框442、444、446、450、452、454或456中的任何的情况下，该流程可以在框450中继续，这是因为可以检测到已经清除了服务应用变化指示器158但已经设置了用户应用变化指示器156。

[0057] 在本发明的各种实施例中，可以以不同的次序执行图3和4中所阐释的方法，且可以组合或省略所阐释的框，且可以添加额外的框，或者带有重新排序的、组合的、省略的或附加的框的组合。

[0058] 如上所述，本发明的各实施例或各实施例的部分可以被存储在任何形式的机器可读介质上。例如，可以以被存储在处理器110和/或管理引擎150可读的介质上的软件或固件指令实现方法200的全部或部分，在由处理器110和/或管理引擎150执行时，这些软件或固件指令引起处理器110和/或管理引擎150执行本发明的一种实施例。而且，可以以被存储在机器可读介质上的数据实现本发明的各方面，其中该数据表示设计或可用于制造处理器110和/或管理引擎150的全部或部分的其他信息。

[0059] 因而，已经描述了用于虚拟化硬件单调计数器的发明的各实施例。尽管已经描述且在附图中示出了某些实施例，但应理解，这样的实施例仅仅是说明而非限制广泛的发明，且本发明不限于所示出和描述的特定的构造和布置，这是由于本领域中的普通技术人员在研读本公开内容后可以看出各种其他修改。在快速发展且不容易预测进一步的进展的诸如本领域的技术领域中，可以容易地在排列和细节方面修改所公开的各实施例，通过允许不偏离本公开内容的原理或所附权利要求的范围的技术进步，可以促进这一点。

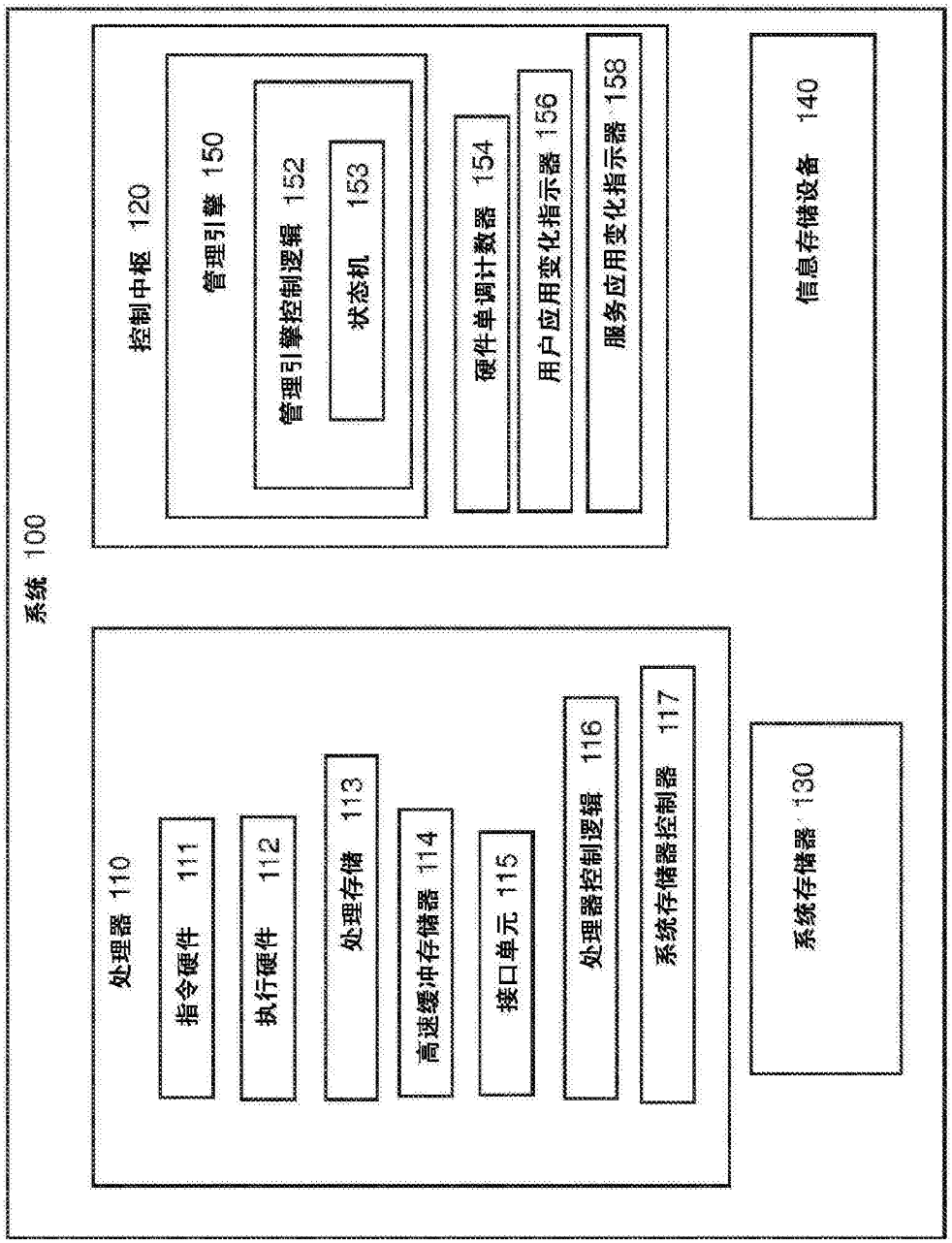

系统 100
处理器 110
指令硬件 111
执行硬件 112
处理存储 113
高速缓冲存储器 114
接口单元 115
处理器控制逻辑 116
系统存储器控制器 117
系统存储器 130
控制中枢 120
管理引擎 150
管理引擎控制逻辑 152
状态机 153
硬件单调计数器 154
用户应用变化指示器 156
服务应用变化指示器 158
信息存储设备 140

图1

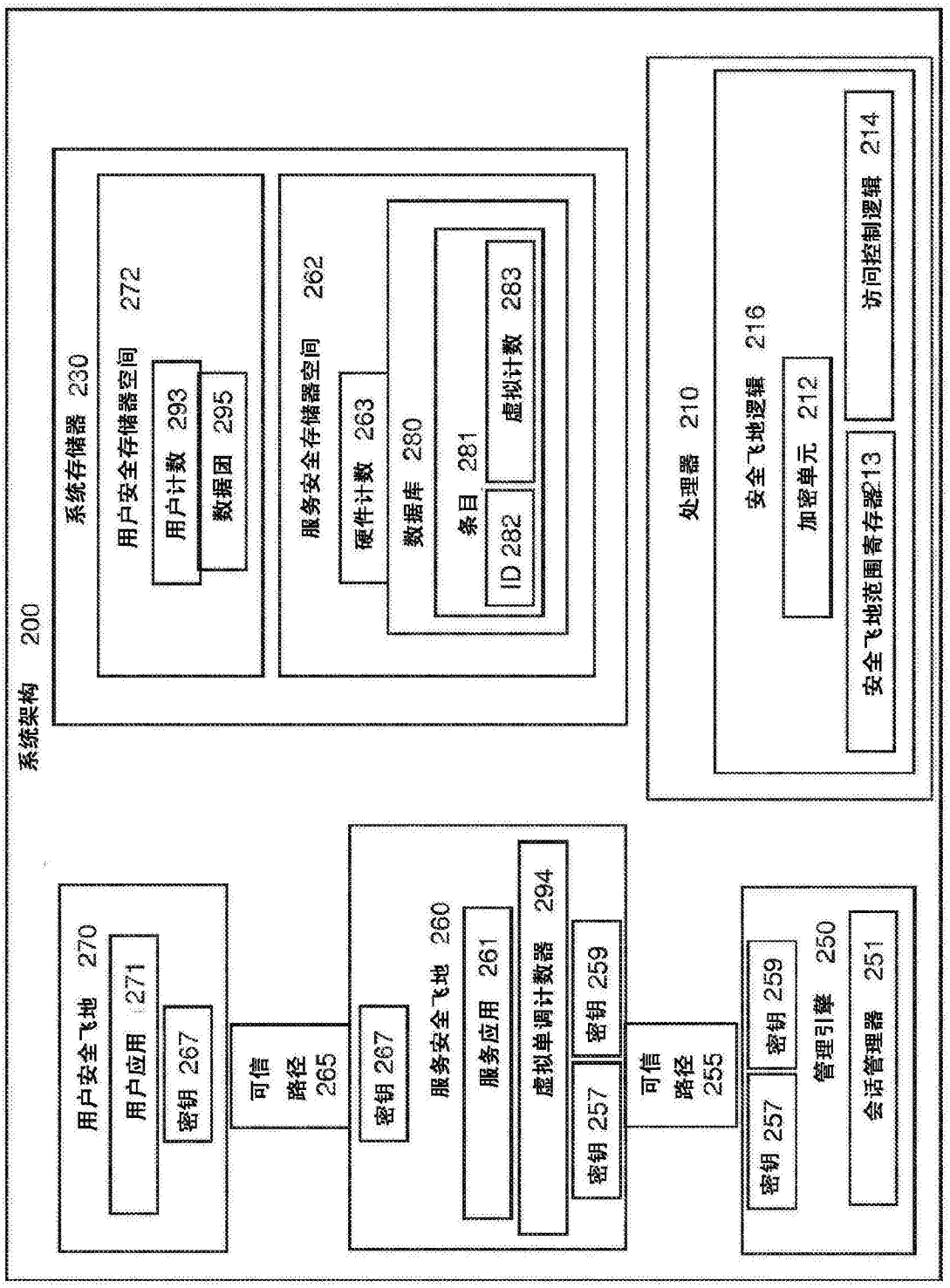

系统架构 200
系统存储器 230
用户安全存储器空间 272
用户计数 293
数据团 295
服务安全存储器空间 262
硬件计数 263
数据库 280
条目 281
ID 282
虚拟计数 283
处理器 210
安全飞地逻辑 216
加密单元 212
安全飞地范围寄存器213
访问控制逻辑 214
用户安全飞地 270
用户应用 271
密钥 267
可信路径 265
密钥 267
服务安全飞地 260
服务应用 261
虚拟单调计数器 294
密钥 257
密钥 259
可信路径 255
密钥 257
密钥 259
管理引擎 250
会话管理器 251

图2

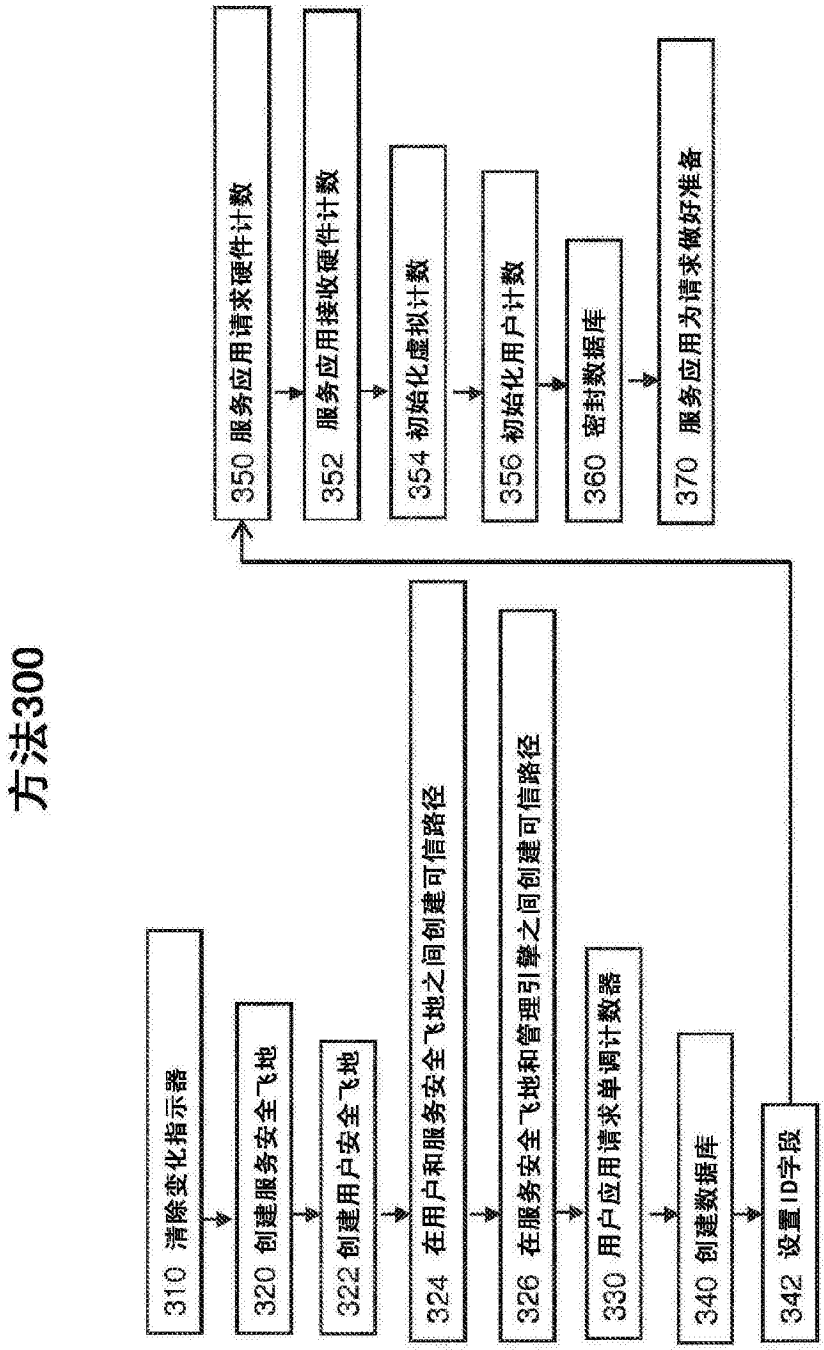

方法300
310 清除变化指示器
320 创建服务安全飞地
322 创建用户安全飞地
324 在用户和服务安全飞地之间创建可信路径
326 在服务安全飞地和管理引擎之间创建可信路径
330 用户应用请求单调计数器
340 创建数据库
342 设置ID字段
350 服务应用请求硬件计数
352 服务应用接收硬件计数
354 初始化虚拟计数
356 初始化用户计数
360 密封数据库
370 服务应用为请求做好准备

图3

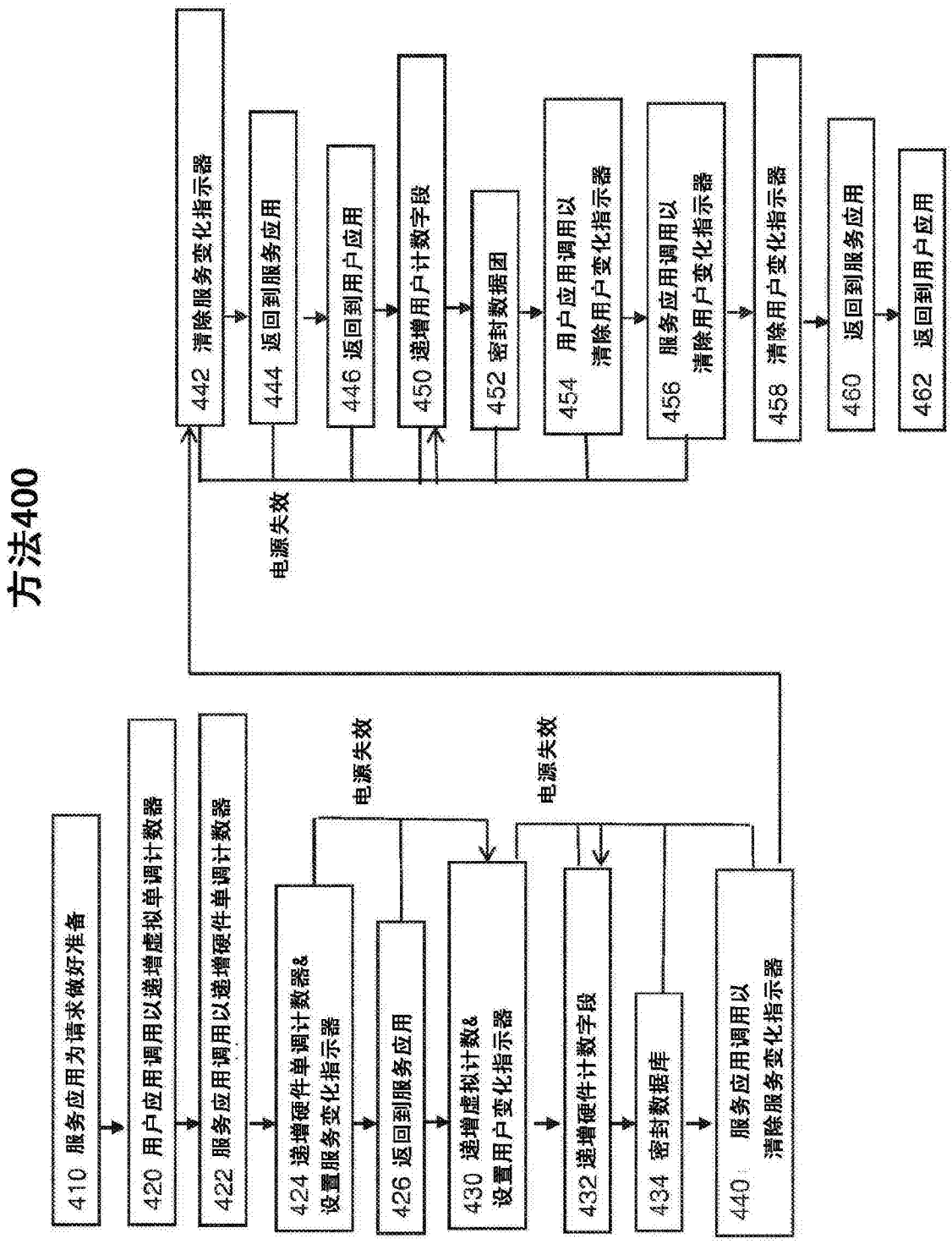

方法400
410 服务应用为请求做好准备
420 用户应用调用以递增虚拟单调计数器
422 服务应用调用以递增硬件单调计数器
424 递增硬件单调计数器&
设置服务变化指示器
426 返回到服务应用
430 递增虚拟计数&
设置用户变化指示器
432 递增硬件计数字段
434 密封数据库
440 服务应用调用以
清除服务变化指示器
电源失效
电源失效
442 清除服务变化指示器
444 返回到服务应用
446 返回到用户应用
450 递增用户计数字段
452 密封数据团
454 用户应用调用以
清除用户变化指示器
456 服务应用调用以
清除用户变化指示器
458 清除用户变化指示器
460 返回到服务应用
462 返回到用户应用
电源失效

图4