[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
B05D 1/36 (2006.01)
G06F 9/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200580006193.0

[43] 公开日 2007 年 3 月 7 日

[11] 公开号 CN 1925926A

[22] 申请日 2005.3.14
[21] 申请号 200580006193.0
[30] 优先权
[32] 2004. 3.24 [33] US [31] 10/809,316
[86] 国际申请 PCT/US2005/008616 2005.3.14
[87] 国际公布 WO2005/101197 英 2005.10.27
[85] 进入国家阶段日期 2006.8.28
[71] 申请人 英特尔公司
地址 美国加利福尼亚州
[72] 发明人 D·德拉姆 V·齐默 C·史密斯
R·亚瓦特卡 T·斯齐露斯勒
D·拉森 C·罗扎斯

[74] 专利代理机构 上海专利商标事务所有限公司
代理人 刘 佳

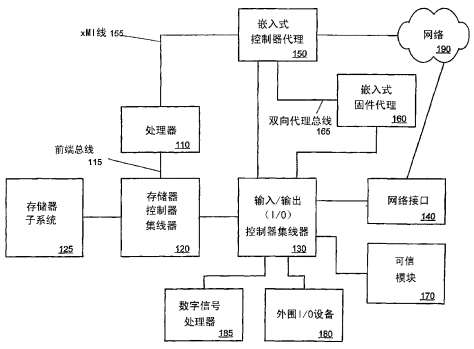
权利要求书 6 页 说明书 10 页 附图 8 页

[54] 发明名称

协作嵌入式代理

[57] 摘要

电子装置具有含有供选择性地以管理模式操作的嵌入式固件代理以及独立于主机操作系统操作并选择性地调用管理模式的嵌入式控制器代理。双向代理总线在嵌入式固件代理与嵌入式控制器代理之间耦合以便在两个代理之间传输消息。可对具有这些协作嵌入式代理的主机系统执行可管理性和安全性操作。



1．一种装置，包括：

嵌入式固件代理，它含有使得所述嵌入式固件代理选择性地以期间主机操作系统释放对所述嵌入式固件代理所驻留的主机系统的控制的管理模式操作的指令；

嵌入式控制器代理，它独立于所述主机操作系统操作，并选择性地调用所述管理模式，所述嵌入式控制器代理具有允许所述嵌入式控制器代理在独立于所述主机操作系统的网络上通信的网络接口；以及

双向代理总线，它耦合在所述嵌入式固件代理与所述嵌入式控制器代理之间以便在所述嵌入式固件代理与所述嵌入式控制器代理之间传输消息。

2．如权利要求 1 所述的装置，其特征在于，还包括与所述嵌入式固件代理和所述嵌入式控制器代理耦合的可信模块，所述可信模块执行密码操作以支持由所述嵌入式控制器代理进行的操作。

3．如权利要求 1 所述的装置，其特征在于，所述嵌入式控制器代理发出管理中断信号来调用所述管理模式。

4．如权利要求 1 所述的装置，其特征在于，所述嵌入式控制器代理和所述嵌入式固件代理交互来向所述主机系统提供可管理性特征。

5．如权利要求 4 所述的装置，其特征在于，所述可管理性特征是在加载所述主机操作系统之前提供的。

6．如权利要求 4 所述的装置，其特征在于，所述可管理性特征是在加载所述主机操作系统之后提供的。

7．如权利要求 4 所述的装置，其特征在于，所述可管理性特征是与加载所述主机操作系统并发提供的。

8．如权利要求 4 所述的装置，其特征在于，所述可管理性特征包括经由所述嵌入式控制器代理对闪存设备的独立于主机操作系统的更新。

9．如权利要求 4 所述的装置，其特征在于，所述可管理性特征包括经由所述嵌入式控制器代理监视主机功能并向远程设备报告。

10．如权利要求 4 所述的装置，其特征在于，所述可管理性特征包括经由所述嵌入式控制器代理向所述主机系统提供引导服务。

11．如权利要求 4 所述的装置，其特征在于，所述可管理性特征包括经由所

述嵌入式控制器代理提供紧急运行时服务。

12．如权利要求 1 所述的装置，其特征在于，所述嵌入式控制器代理与所述嵌入式固件代理交互来向所述主机系统提供安全性特征。

13．如权利要求 12 所述的装置，其特征在于，所述安全性特征是在加载所述主机操作系统之前提供的。

14．如权利要求 12 所述的装置，其特征在于，所述安全性特征是在加载所述主机操作系统之后提供的。

15．如权利要求 12 所述的装置，其特征在于，所述安全性特征是与加载所述主机操作系统并发提供的。

16．如权利要求 12 所述的装置，其特征在于，所述安全性特征包括经由所述嵌入式控制器代理执行对所述主机系统的验证并选择性地将结果报告给远程设备。

17．如权利要求 12 所述的装置，其特征在于，所述安全性特征包括经由所述嵌入式控制器代理执行病毒恢复操作。

18．如权利要求 12 所述的装置，其特征在于，所述安全性特征包括经由所述嵌入式控制器代理为所述主机系统提供认证服务。

19．如权利要求 12 所述的装置，其特征在于，所述安全性特征包括为网络通信会话的相互认证提供支持。

20．一种方法，包括：

调用主机系统中的管理模式，其中主机操作系统使用嵌入式控制器代理暂时释放对所述主机系统的控制，所述嵌入式控制器代理具有独立于所述主机操作系统操作的网络连接；以及

通过由经由双向代理总线与所述嵌入式控制器代理通信，使用嵌入式固件代理在所述管理模式期间服务来自所述嵌入式控制器代理的请求。

21．如权利要求 20 所述的方法，其特征在于，所述嵌入式固件代理通过与提供密码操作的可信模块交互来服务来自所述嵌入式控制器代理的请求。

22．如权利要求 20 所述的方法，其特征在于，所述调用管理模式包括：

使用所述嵌入式控制器代理发出管理中断；以及

响应于所述管理中断进入所述管理模式。

23．如权利要求 20 所述的方法，其特征在于，所述嵌入式控制器代理与所述嵌入式固件代理交互以便向所述主机系统提供可管理性特征。

24．如权利要求 23 所述的方法，其特征在于，所述可管理性特征是在加载所

述主机操作系统之前提供的。

25．如权利要求23所述的方法，其特征在于，所述可管理性特征是在加载所述主机操作系统之后提供的。

26．如权利要求23所述的方法，其特征在于，所述可管理性特征是与加载所述主机操作系统并发提供的。

27．如权利要求23所述的方法，其特征在于，所述可管理性特征包括经由所述嵌入式控制器代理对闪存设备的独立于主机操作系统的更新。

28．如权利要求23所述的方法，其特征在于，所述可管理性特征包括经由所述嵌入式控制器代理监视主机功能并向远程设备报告。

29．如权利要求23所述的方法，其特征在于，所述可管理性特征包括经由所述嵌入式控制器代理向所述主机系统提供引导服务。

30．如权利要求23所述的方法，其特征在于，所述可管理性特征包括经由所述嵌入式控制器代理提供紧急运行时服务。

31．如权利要求20所述的方法，其特征在于，所述嵌入式控制器代理与所述嵌入式固件代理交互来向所述主机系统提供安全性特征。

32．如权利要求31所述的方法，其特征在于，所述安全性特征是在加载所述主机操作系统之前提供的。

33．如权利要求31所述的方法，其特征在于，所述安全性特征是在加载所述主机操作系统之后提供的。

34．如权利要求31所述的方法，其特征在于，所述安全性特征是与加载所述主机操作系统并发提供的。

35．如权利要求31所述的方法，其特征在于，所述安全性特征包括经由所述嵌入式控制器代理执行对所述主机系统的验证并选择性地将结果报告给远程设备。

36．如权利要求31所述的方法，其特征在于，所述安全性特征包括经由所述嵌入式控制器代理执行病毒恢复操作。

37．如权利要求31所述的方法，其特征在于，所述安全性特征包括经由所述嵌入式控制器代理为所述主机系统提供认证服务。

38．如权利要求31所述的方法，其特征在于，所述安全性特征包括为网络通信会话的相互认证提供支持。

39．一种包含其上存储指令的计算机可读介质的制品，所述指令当被执行时，使一个或多个处理元件：

调用主机系统中的管理模式，其中主机操作系统使用嵌入式控制器代理暂时释放对所述主机系统的控制，所述嵌入式控制器代理具有独立于所述主机操作系统操作的网络连接；以及

通过经由双向代理总线与所述嵌入式控制器代理通信，使用嵌入式固件代理在所述管理模式期间服务来自所述嵌入式控制器代理的请求。

40．如权利要求 39 所述的制品，其特征在于，所述嵌入式固件代理通过与提供密码操作的可信模块交互来服务来自所述嵌入式控制器代理的请求。

41．如权利要求 39 所述的制品，其特征在于，所述使一个或多个处理元件调用管理模式的指令包括当被执行时使一个或多个处理元件进行以下操作的指令：

使用所述嵌入式控制器代理发出管理中断；以及

响应于所述管理中断进入所述管理模式。

42．如权利要求 39 所述的制品，其特征在于，所述嵌入式控制器代理与所述嵌入式固件代理交互以便向所述主机系统提供可管理性特征。

43．如权利要求 42 所述的制品，其特征在于，所述可管理性特征是在加载所述主机操作系统之前提供的。

44．如权利要求 42 所述的制品，其特征在于，所述可管理性特征是在加载所述主机操作系统之后提供的。

45．如权利要求 42 所述的制品，其特征在于，所述可管理性特征是与加载所述主机操作系统并发提供的。

46．如权利要求 42 所述的制品，其特征在于，所述可管理性特征包括经由所述嵌入式控制器代理对闪存设备的独立于主机操作系统的更新。

47．如权利要求 42 所述的制品，其特征在于，所述可管理性特征包括经由所述嵌入式控制器代理监视主机功能并向远程设备报告。

48．如权利要求 42 所述的制品，其特征在于，所述可管理性特征包括经由所述嵌入式控制器代理向所述主机系统提供引导服务。

49．如权利要求 42 所述的制品，其特征在于，所述可管理性特征包括经由所述嵌入式控制器代理提供紧急运行时服务。

50．如权利要求 39 所述的制品，其特征在于，所述嵌入式控制器代理与所述嵌入式固件代理交互来向所述主机系统提供安全性特征。

51．如权利要求 50 所述的制品，其特征在于，所述安全性特征是在加载所述主机操作系统之前提供的。

52．如权利要求 50 所述的制品，其特征在于，所述安全性特征是在加载所述主机操作系统之后提供的。

53．如权利要求 50 所述的制品，其特征在于，所述安全性特征是与加载所述主机操作系统并发提供的。

54．如权利要求 50 所述的制品，其特征在于，所述安全性特征包括经由所述嵌入式控制器代理执行对所述主机系统的验证并选择性地将结果报告给远程设备。

55．如权利要求 50 所述的制品，其特征在于，所述安全性特征包括经由所述嵌入式控制器代理执行病毒恢复操作。

56．如权利要求 50 所述的制品，其特征在于，所述安全性特征包括经由所述嵌入式控制器代理为所述主机系统提供认证服务。

57．如权利要求 50 所述的制品，其特征在于，所述安全性特征包括为网络通信会话的相互认证提供支持。

58．一种系统，包括：

总线；

与所述总线耦合的数字信号处理器；

与所述总线耦合的嵌入式固件代理，它含有使得所述嵌入式固件代理选择性地以期间主机操作系统释放对所述嵌入式固件代理所驻留的主机系统的控制的管理模式操作的指令；

嵌入式控制器代理，它独立于所述主机操作系统操作并选择性地调用所述管理模式，所述嵌入式控制器代理具有允许所述嵌入式控制器代理在独立于所述主机操作系统的网络上通信的网络接口；以及

双向代理总线，它耦合在所述嵌入式固件代理与所述嵌入式控制器代理之间以便在所述嵌入式固件代理与所述嵌入式控制器代理之间传输消息。

59．如权利要求 58 所述的系统，其特征在于，还包括与所述嵌入式固件代理和所述嵌入式控制器代理耦合的可信模块，所述可信模块执行密码操作以支持由所述嵌入式控制器代理进行的操作。

60．如权利要求 58 所述的系统，其特征在于，所述嵌入式控制器代理发出管理中断信号来调用所述管理模式。

61．如权利要求 58 所述的系统，其特征在于，所述嵌入式控制器代理和所述嵌入式固件代理交互来向所述主机系统提供可管理性特征。

62．如权利要求 61 所述的系统，其特征在于，所述可管理性特征是在加载所

述主机操作系统之前提供的。

63．如权利要求61所述的系统，其特征在于，所述可管理性特征是在加载所述主机操作系统之后提供的。

64．如权利要求61所述的系统，其特征在于，所述可管理性特征是与加载所述主机操作系统并发提供的。

65．如权利要求61所述的系统，其特征在于，所述可管理性特征包括经由所述嵌入式控制器代理对闪存设备的独立于主机操作系统的更新。

66．如权利要求61所述的系统，其特征在于，所述可管理性特征包括经由所述嵌入式控制器代理监视主机功能并向远程设备报告。

67．如权利要求61所述的系统，其特征在于，所述可管理性特征包括经由所述嵌入式控制器代理向所述主机系统提供引导服务。

68．如权利要求61所述的系统，其特征在于，所述可管理性特征包括经由所述嵌入式控制器代理提供紧急运行时服务。

69．如权利要求58所述的系统，其特征在于，所述嵌入式控制器代理与所述嵌入式固件代理交互来向所述主机系统提供安全性特征。

70．如权利要求69所述的系统，其特征在于，所述安全性特征是在加载所述主机操作系统之前提供的。

71．如权利要求69所述的系统，其特征在于，所述安全性特征是在加载所述主机操作系统之后提供的。

72．如权利要求69所述的系统，其特征在于，所述安全性特征是与加载所述主机操作系统并发提供的。

73．如权利要求69所述的系统，其特征在于，所述安全性特征包括经由所述嵌入式控制器代理执行对所述主机系统的验证并选择性地将结果报告给远程设备。

74．如权利要求69所述的系统，其特征在于，所述安全性特征包括经由所述嵌入式控制器代理执行病毒恢复操作。

75．如权利要求69所述的系统，其特征在于，所述安全性特征包括经由所述嵌入式控制器代理为所述主机系统提供认证服务。

76．如权利要求69所述的系统，其特征在于，所述安全性特征包括为网络通信会话的相互认证提供支持。

协作嵌入式代理

技术领域

本发明的实施例涉及具有协作嵌入式代理的电子系统。更具体地，本发明的实施例涉及具有耦合来与各种系统组件交互的嵌入式代理，该嵌入式代理与具有独立网络连接的另一嵌入式代理通信，同时该嵌入式代理协作来向电子系统提供可管理性、安全性和/或其它功能。

背景

自从英特尔公司引入了386SL处理器以来，在32位英特尔体系结构（IA32）处理器上提供了系统管理模式（SMM），它作为对操作系统隐藏的执行由基本输入/输出系统（BIOS）或固件加载的代码的操作模式。该模式被认为是“隐藏的”是因为SMM操作独立于操作系统（OS）和软件应用程序存在。

使IA32处理器能够经由系统管理中断（SMI）信号进入SMM。被称为处理器管理中断（PMI）信号的类似信号与SMI信号大致功能相同，它被用于Itanium™类处理器，也是由英特尔公司提供的。为简明起见，SMI和PMI信号两者均可称为xMI。

迄今为止，利用SMM能力的大多数BIOS实现仅登记在BIOS建立期间创建的整块代码部分，以便支持使用BIOS系统专用的一特定功能或一组功能。在当今的系统中没有提供对第三方SMM代码的登记或执行，因此不允许对SMM框架的扩展性。而这样的扩展性通常是被期望的。例如，如果由原始设备制造商（OEM）或BIOS销售商提供的SMM代码所提供的功能不充分，则开发员或增值转售商（VAR）必须许可来自BIOS销售商或OEM的现有代码并试图将他们自己的逻辑嫁接于他们对SMM代码的实现。

此外，当今对IA32处理器的实现限于16位的处理器模式，因此限制了代码的大小和利用32位或64位软件工程技术的可能性。一般，BIOS对SMM功能的更新是否有效是成问题的，且因为OS已经由其自己的驱动程序模型而具有硬件可扩展性机制，因此BIOS销售商和OEM在提供这些类型的BIOS更新上动力较小。

附图简述

本发明的实施例经由示例而非限制示出，在附图的图中，相同的参考标号指的是类似的元素。

图 1 是具有协作嵌入式代理的电子系统的一个实施例的框图。

图 2 是嵌入式控制器代理、嵌入式固件代理与可信模块之间的交互的一个实施例的概念性框图。

图 3 是嵌入式控制器代理的操作的一个实施例的流程图。

图 4 是嵌入式固件代理的操作的一个实施例的流程图。

图 5 是嵌入式固件代理的初始化处理的一个实施例的流程图。

图 6 是嵌入式固件代理的一个实施例的框图。

图 7 是嵌入式控制器代理的一个实施例的框图。

图 8 是可信模块的一个实施例的框图。

详细描述

在以下描述中，描述了各种特定细节。然而，可无需这些特定细节而实现本发明的实施例。在其它实例中，未详细示出公知的电路、结构和技术以便不模糊对本说明书的理解。

图 1 是具有协作嵌入式代理的电子系统的一个实施例的框图。图 1 的框图旨在表示具有网络接口的电子系统的宽泛的范畴。该电子系统可以是例如台式计算机系统、移动计算机系统、服务器、个人数字助理（PDA）、手机、机顶盒、游戏控制台、卫星接收器等。

在一个实施例中，处理器 110 可由前侧（front side）总线 115 耦合至存储器控制器集线器 120。尽管图 1 的电子系统被描述为具有单处理器，但也可支持多处理器的实施例。在替换实施例中，处理器 110 可由共享的系统总线耦合至存储器控制器集线器 120。处理器 110 可以是本领域中已知的任何类型的处理器，例如，来自加利福尼亚州圣克拉拉市的英特尔公司的 Pentium®系列处理器、Itanium®系列处理器、Xeon®系列处理器的处理器。也可使用其它处理器。

存储器控制器集线器 120 可向可包含将与电子系统一起使用的任何类型的存储器的存储器子系统 125 提供接口。存储器控制器集线器 120 也可与输入/输出（I/O）控制器集线器（ICH）130 耦合。在一个实施例中，ICH 130 可提供系统与

外围 I/O 设备 180 之间以及系统与网络接口 141 之间的接口，后者可向外部网络 190 提供接口。网络 190 可以是任何类型的网络，无论有线还是无线，例如局域网或广域网。存储器控制器集线器 120 也可与数字信号处理器 185 耦合。

在一个实施例中，ICH 130 可与可信模块 170 耦合，后者可提供安全性和/或加密功能。在一个实施例中，可信模块 170 可被实现为可信平台模块（TPM），这将在以下详细描述。可信模块 170 能以安全的方式向 ICH 130 或其它系统组件提供例如加密密钥的安全标识符。

嵌入式控制器代理 150 可与 ICH 130 以及网络 190 耦合。嵌入式控制器 150 的网络连接可以独立于系统的操作，且独立于由处理器 110 执行的操作系统。在一个实施例中，嵌入式控制器代理 150 可包括微控制器或其它类型的处理电路、存储器和接口逻辑。将在以下详细描述嵌入式控制器代理 150 的一个实施例。

在一个实施例中，嵌入式控制器代理 150 可经由中断接口与处理器 110 耦合。例如，嵌入式控制器代理 150 可与 Pentium®处理器的 SMI 插脚或与 Itanium®处理器的 PMI 插脚（总称，xMI 线 155）耦合。对其它处理器可使用其它系统中断信号。

ICH 130 也可与嵌入式固件代理 160 耦合。在一个实施例中，嵌入式固件代理 160 可以是允许以一个或多个软件驱动程序形式的可执行内容被加载到英特尔 32 位微处理器系列（即，IA-32 处理器）的系统管理模式（SMM）中或带有 PMI 信号激活的基于 Itanium 处理器的固有模式。IA32 SMM 中的代码的执行状态由 SMI 信号启动，且 Itanium™ 处理器中的代码执行状态由 PMI 信号激活启动；为简单起见，这些总称为 SMM。

在一个实施例中，嵌入式固件代理 160 为 SMM 操作可允许安装可能由不同方编写的多个驱动程序。可登记驱动程序的代理的示例运行在可扩展固件接口（EFI）引导服务模式（即，操作系统启动之前的模式）中，且可由绑定驱动程序与提取 xMI（PMI 或 SMI）信号的芯片组控制的平台组件的处理器专用组件组成。

在一个实施例中，存储在嵌入式固件代理 160 中的代码可在主机系统的启动期间被复制到存储器子系统 125 的存储器组件中。例如，在支持 SMM 操作的体系结构中，将在 SMM 期间使用的代码可被影复制到存储器子系统 125 的 SMRAM 部分。当在 SMM 中操作时，处理器 110 可执行存储在 SMRAM 中的指令。

在一个实施例中，嵌入式控制器代理 150 可经由双向代理总线 165 与嵌入式固件代理 162 耦合。通过经由双向代理总线 162 通信，嵌入式控制器代理 150 和嵌入式固件代理 160 可被配置成向系统提供可管理性和/或安全性功能。

在一个实施例中，嵌入式控制器代理 150 可为安全性起见提供对系统的完整性检查，例如在经由网络 190 建立与远程设备的安全即可信连接之前。嵌入式控制器代理可执行系统的病毒扫描，来确定与远程设备的通信是否是安全的和/或远程设备是否请求支持。嵌入式固件代理 160 可提供独立于操作系统的安全存储，供嵌入式控制器代理 150 在执行完整性检查中使用。

在操作期间，嵌入式控制器代理 150 可执行周期性完整性检查以提供相比单个完整性检查增长的安全性。嵌入式控制器代理 150 也可在与远程管理设备通信之前执行完整性检查。以下将描述嵌入式控制器代理 150 与嵌入式固件代理 160 之间的双向通信的使用的其它示例。

在图 1 的描述中，按照分开的系统元件描述了嵌入式控制器代理 150、嵌入式固件代理 160 和双向代理总线 165。在物理实现中，嵌入式控制器代理 150、嵌入式固件代理 160 和双向代理总线 165 可以是一个或多个组件的逻辑组件。双向代理总线 165 可以是可允许嵌入式控制器代理 150 与嵌入式固件代理 160 的功能组件之间的双向通信的任何通信机制或消息通信接口。

如此处所述的嵌入式控制器代理 150 和嵌入式固件代理 160 用于为主机系统提供功能的操作可以在加载到主机操作系统之前和/或加载主机操作系统之后完成。因此，此处所述的体系结构提供宽泛范畴的可管理性和/或安全功能。

图 2 是嵌入式控制器代理、嵌入式固件代理与可信模块之间的交互的一个实施例的概念性框图。当嵌入式控制器代理 150 经由网络 190 启动或响应于与远程设备的通信，嵌入式控制器代理 150 可通过发出（assert）如上所述的 xMI 信号启动管理模式 210。使用英特尔处理器，管理模式 210 可对应于系统管理模式（SMM）。使用其它处理器，则可使用其它管理模式。因为管理模式 210 用于由嵌入式控制器代理 150 进行的操作，这些操作可独立于操作系统 200 执行。

在一个实施例中，当嵌入式控制器代理 150 调用管理模式 210 时，嵌入式固件代理 160 提供执行由嵌入式控制器代理 150 请求的操作的中断服务例程。在一个实施例中，嵌入式固件代理 160 是允许在例如可访问嵌入式固件代理 160 的闪存的存储器中编写和存储中断处理例程的 EFI 设备，该中断处理例程将响应于来自嵌入式控制器代理 150 的 xMI 信号而被使用。

在调用管理模式 210 之后，嵌入式控制器代理 150 可执行独立于操作系统 200 的可管理性和/或安全操作。如果例如嵌入式控制器代理 150 参与网络 190 上的与远程设备的安全通信，则嵌入式控制器代理 150 可在管理模式 210 中与可信模块

170 通信以便认证嵌入式控制器代理 150 所属于的系统。因为该认证是独立于操作系统 200 的，嵌入式控制器代理 150 隔离于涉及操作系统 200 的病毒和/或安全攻击。

在一个实施例中，将管理模式操作卸载给嵌入式控制器 150 以便与操作系统 200 共享处理资源。例如，来自微软公司的大多数 Windows®操作系统使用定时器来检查指令的中型以及当自从最后一条指令以来经过了过长时间（例如，200ms）时可调用调试或故障操作。通过卸载管理模式操作，嵌入式控制器代理 150 可当执行例如访问诸如例如来自可信模块 170 的数据等系统资源的操作时周期性地发出 xMI 信号。

图 3 是嵌入式控制器代理的操作的一个示例的流程图。响应于复位，嵌入式控制器代理可执行初始化过程，并初始化网络连接，300。代理初始化可包括准备操作代理所需的任何操作。这些操作可以包括例如从具有对该代理的初始化指令的只读存储器或闪存中检索指令。

在一个实施例中，当完成初始化过程时，代理可开始频带外通信，310。网络通信被称为频带外的，是因为嵌入式控制器代理的网络通信是独立于其中嵌入式控制器代理驻留的系统上执行的操作系统的。频带外网络通信可包括例如与在网络中登记主机系统相关的操作、响应于远程网络节点的可管理性操作、安全性操作等。

在一个实施例中，嵌入式控制器代理可等待系统事件，320。系统事件可以是与将独立于操作系统执行的操作相关的任何类型的事件。例如，如果主机操作系统已经是病毒或木马的受害者，则系统事件可由病毒检测软件触发，以便检索病毒消除程序或禁用系统网络连接以便阻止病毒或木马的传播。

响应于系统事件，嵌入式控制器代理可发出 xMI 信号（对 Intel®处理器），330。对 xMI 信号的发出可引起处理器进入 SMM，其中操作系统将对主机系统的控制释放给可存储在例如对操作系统不可访问的系统管理存储器中的 SMM 中断处理器。系统事件可被处理，340。

图 4 是嵌入式固件代理的操作的一个实施例的流程图。响应于复位，嵌入式控制器代理可执行初始化过程，400。以下将参考图 5 详细描述初始化过程的一个实施例。

在一个实施例中，嵌入式固件代理可确定嵌入式控制器代理是否准备好，410。在一个实施例中，嵌入式控制器代理可经由双向代理总线向嵌入式固件代理指示初始化的完成。在一个实施例中，当嵌入式固件代理与嵌入式控制器代理均被初始化

时，对主机系统的控制可被授予主机操作系统，420。

通过允许嵌入式固件代理和嵌入式控制器代理两者在将对主机系统的控制传递给主机操作系统之前完成初始化，可在将控制授予主机操作系统之前执行安全性、可管理性和/或其它功能。如果 xMI 发生，430，则主机系统可进入管理模式（MM），440。当处于 MM 中时，嵌入式控制器代理、嵌入式固件代理和/或可信模块可操作来处理 xMI，450。

图 5 是嵌入式固件代理的初始化过程的一个实施例的流程图。图 5 的示例描述了与使用 Intel®处理器的 SMM 操作相关的特定操作；然而，也可使用支持其它类似功能的处理器。

响应于复位条件，嵌入式固件代理可初始化主机存储器和一个或多个输入/输出（I/O）设备，500。在一个实施例中，该初始化可以是传统由基本输入/输出系统（BIOS）执行的初始化操作的部分或所有。在一个实施例中，当对存储器的初始化之后，嵌入式固件代理可测试存储器，设置纠错码（ECC），启动系统管理存储器（SMRAM）和/或加载系统管理码的核心（SMM 核心），510。

在一个实施例中，如果嵌入式固件代理检测到 SMM 驱动程序，520，则嵌入式固件代理可为 SMM 驱动程序分配 SMRAM 的区域，然后可进入 SMM 将 SMM 驱动程序从引导服务存储器重新定位到 SMRAM。如果嵌入式固件代理未检测到 SMM 驱动程序，520，则嵌入式固件代理可检查固件驱动程序，540。

在一个实施例中，如果嵌入式固件代理检测到固件驱动程序，540，则嵌入式固件代理可加载来自磁盘或闪存的驱动程序，并将该驱动程序重新定位到系统存储器，且可散列扩展可信模块的寄存器（例如，可信平台模块（TPM）平台配置寄存器（PCR）），550。如果嵌入式固件代理未检测到固件驱动程序，540，则嵌入式固件代理可检查其它驱动程序，560。

在一个实施例中，如果嵌入式固件代理检测到其它驱动程序，560，则嵌入式固件代理可返回来检查其它驱动程序，以确定该其它驱动程序是否是 SMM 驱动程序，520。如果嵌入式固件代理未检测到其它驱动程序，560，则嵌入式固件代理可确定嵌入式控制器代理是否准备好，570。如果嵌入式控制器代理准备好，570，则嵌入式固件代理可将控制转移给主机操作系统，580。

嵌入式固件代理、嵌入式控制器代理和/或可信模块的交互可提供以下描述的可管理性和/或安全性特征的一个或多个。以下的特征的列表是示例的列表，而不旨在是如此处所述的嵌入式固件代理、嵌入式控制器代理和可信模块可具备的特征

的穷尽清单。

可按照使用如此处所述的技术的安全的方式更新可包含在嵌入式固件代理、嵌入式控制器、可信模块和/或主机系统中的闪存。因为可从远程设备向嵌入式控制器提供更新，而无需操作系统的交互，因此即使当操作系统未正确运行时也可提供更新，且因为攻击涉及操作系统，因而可提供额外的安全性。远程更新可提供用于在多个客户机设备上更新闪存的有效的技术。

在一个实施例中，嵌入式控制器代理可监视操作系统的操作，并基于操作系统的条件或模式修改安全性策略。例如，可当操作系统运行时应用第一安全性策略，而当主机系统处于 SMM 中时可应用第二安全性策略。

嵌入式控制器代理、嵌入式固件代理和/或可信模块可提供独立于或不同于由操作系统提供的监视的对主机系统的监视和记录。例如，嵌入式控制器代理和嵌入式固件代理可监视处理器性能计数器和处理器负载，且如果超过预置阈值，则可经由嵌入式控制器代理的网络连接向远程设备发送消息。

嵌入式控制器代理、嵌入式固件和/或可信模块可提供对主机磁盘驱动程序的主机保护区域（HPA）的支持。HPA 可用于凭证存储、大型日志归档等。通过能够访问可信模块，并具有由可信模块提供的增加的密码功能，嵌入式控制器代理、嵌入式固件代理和可信模块可一起作用来为网络通信提供相互的认证功能。

在一个实施例中，可将预引导执行环境（PXE）操作从主机处理器卸载到嵌入式控制器代理和/或嵌入式固件代理。而且，对 PXE 服务器的 PXE 发现可由嵌入式固件代理、嵌入式控制器代理和/或可信模块执行。

使用例如安全套接字层（SSL）会话的相互认证可通过使用由可信模块提供的认证功能来完成，以便向服务器提供认证。在一个实施例中，例如病毒扫描的安全性操作可在嵌入式固件代理将对主机系统的控制转移给主机操作系统之前执行。如果检测到病毒，则嵌入式控制器代理可响应于所检测到的病毒使用嵌入式控制器代理的网络连接与远程设备交互。

在一个实施例中，嵌入式控制器代理可使用可扩展标记语言数字签名（XML DSIG）以便经由独立网络连接将安全消息发送给远程设备。嵌入式控制器代理可经由 SMM 中的嵌入式固件代理与可信模块交互，以便提供密码操作。这些安全性操作是独立于主机操作系统的，从而可用于认证主机系统。

图 6 是嵌入式固件代理的一个实施例的框图。在图 6 的示例中，嵌入式固件代理可以是如由 2003 年 11 月 26 日发布的来自加利福尼亚州圣克拉拉市的英特尔

公司的 EFI 规范，版本 1.10 定义的可扩展固件接口（EFI）。在替换实施例中，也可使用其它固件组件。

在一个实施例中，嵌入式固件代理可包括与系统接口 605 耦合的代理总线 600。系统接口 605 可提供一接口，经由该接口嵌入式固件代理可与主机系统通信。嵌入式固件代理还可包括可与总线 600 耦合以便允许嵌入式固件代理与如上所述的嵌入式控制器代理通信的双向代理总线接口 650。

在一个实施例中，嵌入式固件代理还包括可与代理总线 600 耦合的动态存储器 610。动态存储器 610 可提供对将在操作期间使用的指令和/或数据的存储。嵌入式固件代理还可包括可与代理总线 600 耦合来存储静态数据和/或指令的非易失性存储 620。

在一个实施例中，嵌入式固件代理可包括与代理总线 600 耦合可执行控制操作和/或执行由动态存储器 610 和/或非易失性存储 620 提供的指令的控制电路 630。嵌入式固件代理也可包括与代理总线 600 耦合的 SMM 模块 640。SMM 模块 640 可以是向主机系统提供 SMM 功能的元件的任何组合。例如，当处于 SMM 中时，嵌入式固件代理可提供基于动态存储器 610 和/或非易失性存储 620 中所存储的数据和/或指令的 SMI 处理操作。

在一个实施例中，在 SMM 期间选择性地激活控制电路 630。即，当主机系统不处于 SMM 中时，控制电路 630 可空闲，或甚至处于不活动状态。在一个实施例中，嵌入式固件代理可访问主机系统中的所有存储器。这包括，例如 SMRAM、HPA 以及具有访问限制的可能的其它存储区域。

图 7 是嵌入式控制器代理的一个实施例的框图。在图 7 的示例中，嵌入式控制器代理可以是可如此处所述操作的基于微控制器的系统组件。在替换实施例中，也可使用其它控制器组件。

在一个实施例中，可信模块可包含与系统接口 705 耦合的代理总线 700。系统接口 705 可提供一接口，经由该接口嵌入式控制器代理与主机系统通信。嵌入式控制器代理还可包括可与总线 700 耦合以便允许嵌入式控制器代理与上述嵌入式固件代理通信的双向代理总线接口 760。

在一个实施例中，嵌入式控制器代理还包括可与代理总线 700 耦合的动态存储器 710。动态存储器 710 可为将在操作期间使用的指令和/或数据提供存储。嵌入式控制器代理还可包括可与代理总线 700 耦合来存储静态数据和/或指令的非易失性存储 720。

在一个实施例中，嵌入式控制器代理可包括与代理总线 700 耦合可被实现为执行控制操作和/或执行由动态存储器 710 和/或非易失性存储 720 提供的指令的微控制器的控制电路 730。可使用本领域中已知的任何类型的微控制器或类似的控制电路。

嵌入式控制器代理也可包括与代理总线 700 耦合的代理/网络接口 740。代理/网络接口 740 可为嵌入式控制器代理提供独立于主机系统的操作系统和网络接口的网络连接。代理/网络接口 740 可允许嵌入式控制器代理与独立于主机系统的操作系统的远程设备通信。这允许嵌入式控制器代理以与操作系统控制下执行的可管理性、安全性和/或其它功能相比更安全和透明的方式执行类似的操作。

在一个实施例中，控制电路 730 未处于不活动状态中。这允许控制电路 730 和嵌入式控制器代理响应于内部和外部事件。在一个实施例中，嵌入式控制器代理不能访问主机系统的所有存储器。在这样的实施例中，依赖于受保护存储区域的存储器访问和/或指令执行可由嵌入式固件代理访问。

图 8 是可信模块的一个实施例的框图。在图 8 的示例中，可信模块可以是如由俄勒冈州波特兰市 Trusted Computing Group 于 2003 年 10 月 2 日发布的 TPM 规范版本 1.2 定义的被信任平台模块（TPM）。在替换实施例中，可使用被信任模块的其它实现，例如安全存储设备，以便为安全性操作提供支持。

在一个实施例中，可信模块可包括与系统接口 805 耦合的总线 800。系统接口可提供一接口，经由该接口可信模块可与主机系统通信。可信模块可包括与总线 800 耦合以便为密码操作生成随机数的随机数生成器 810，以及与总线 800 耦合以便存储数据和/或指令以供可信模块的操作中使用的非易失性存储 815。

可信模块还可包括平台配置寄存器 820，它可被用来存储与主机系统完整性相关的受保护信息。在一个实施例中，可信模块也可包括与总线 800 耦合以便存储证明标识密钥（AIK）825 的存储组件。在一个实施例中，AIK 825 可以是可用于数字签署信息的由可信模块和/或主机系统生成的 2048 位 RSA 密钥。也可使用其它 AIK 配置。

程序代码 830 可以被存储在与总线 800 耦合的易失性或非易失性的存储器中。程序代码 830 包括使得可信模块操作来提供安全性操作的指令。在一个实施例中，执行引擎 835 与总线 800 耦合来执行程序代码 830。可信模块还可包括允许主机系统的用于启动或禁用可信模块的操作的选择（opt-in）模块 840。选择模块 840 可以是例如主机系统上的物理开关。

在一个实施例中，可信模块可包括与总线 800 耦合执行密码操作的密码引擎 845。密码引擎 845 可以是例如执行 RSA 密码操作的 RSA 引擎。例如不对称密码协议的其它密码协议也可由密码引擎 845 支持。可信模块还可包括与总线 800 耦合可为密码操作生成一个或多个密钥的密钥生成器 850。

散列引擎 855 也可与总线 800 耦合，且可提供支持密码操作的散列功能。在一个实施例中，散列引擎 855 可以是 SHA-1 引擎，且可执行安全散列算法操作以供在由可信模块提供的安全性功能中使用。在替换实施例中，散列引擎 855 可以是 DSA 引擎，或者散列引擎 855 可支持任何其它密码协议。

说明书中对“一个实施例”或“实施例”的引用指的是，结合实施例描述的特定特征、结构或特性被包含在本发明的至少一个实施例中。短语“在一个实施例中”在说明书中不同位置的出现不必指的是相同的实施例。

尽管按照若干实施例描述了本发明，但本领域的技术人员可以认识，本发明不限于所述的实施例，而是能以所附权利要求书的精神和范围内的修改和变更实践。因此描述可被认为是说明性而非限制性的。

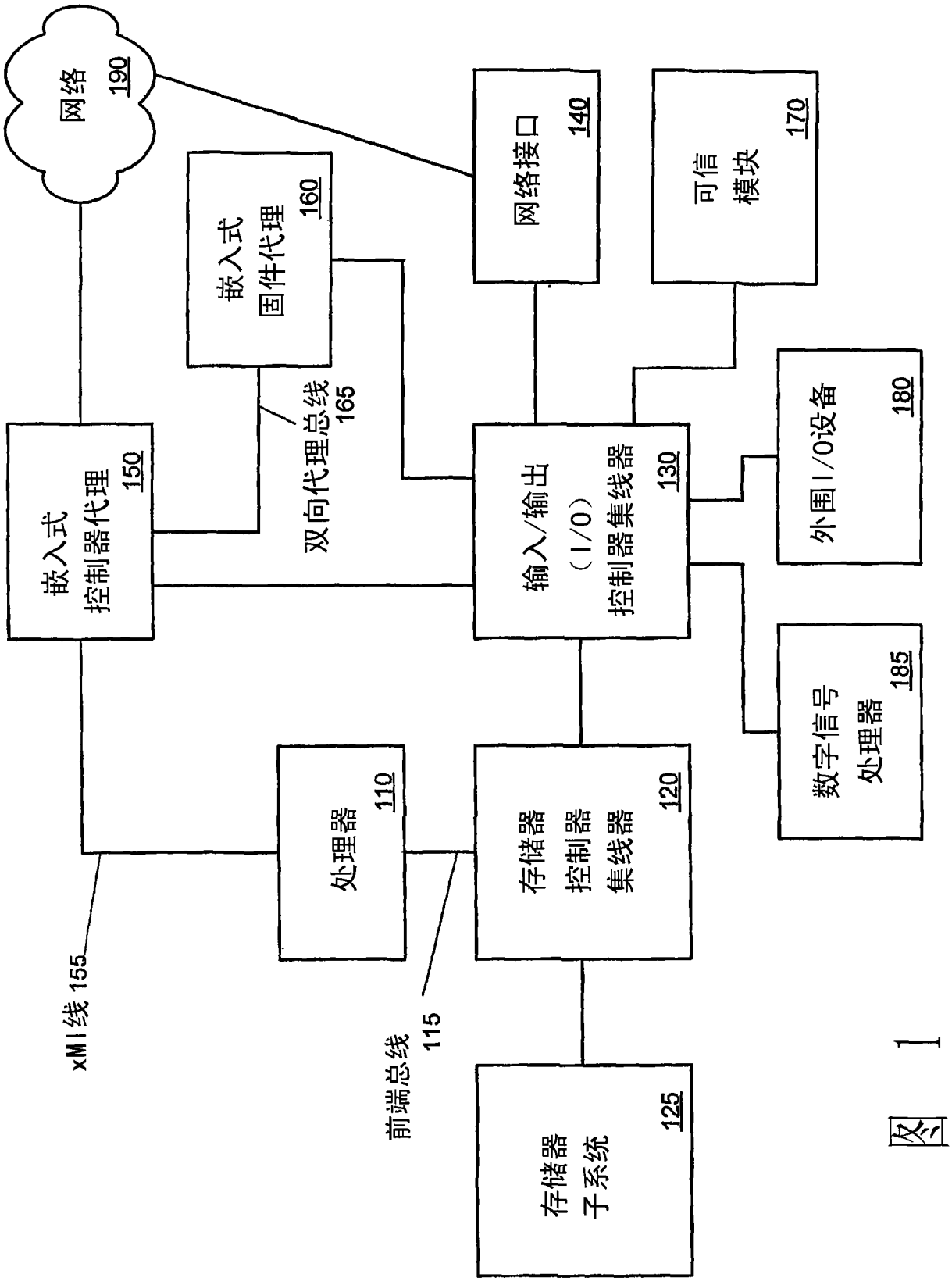

网络 190
网络接口 140
可信模块 170
嵌入式固件代理 160
双向代理总线 165
嵌入式控制器代理 150
输入/输出（I/O）控制器集线器 130
外围I/O设备 180
数字信号处理器 185
处理器 110
存储器控制器集线器 120
xMI线 155
前端总线 115
存储器子系统 125

图 1

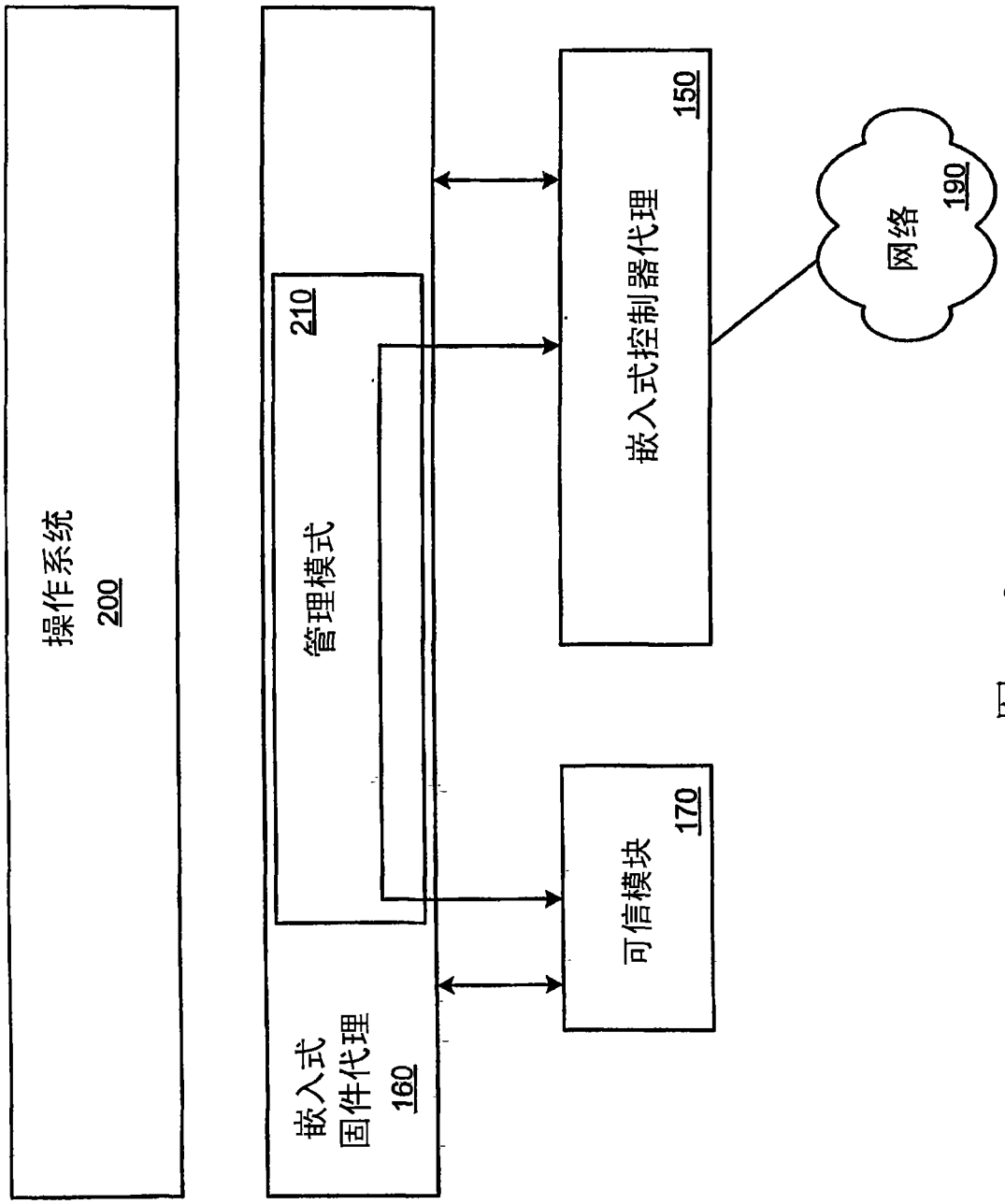


图 2

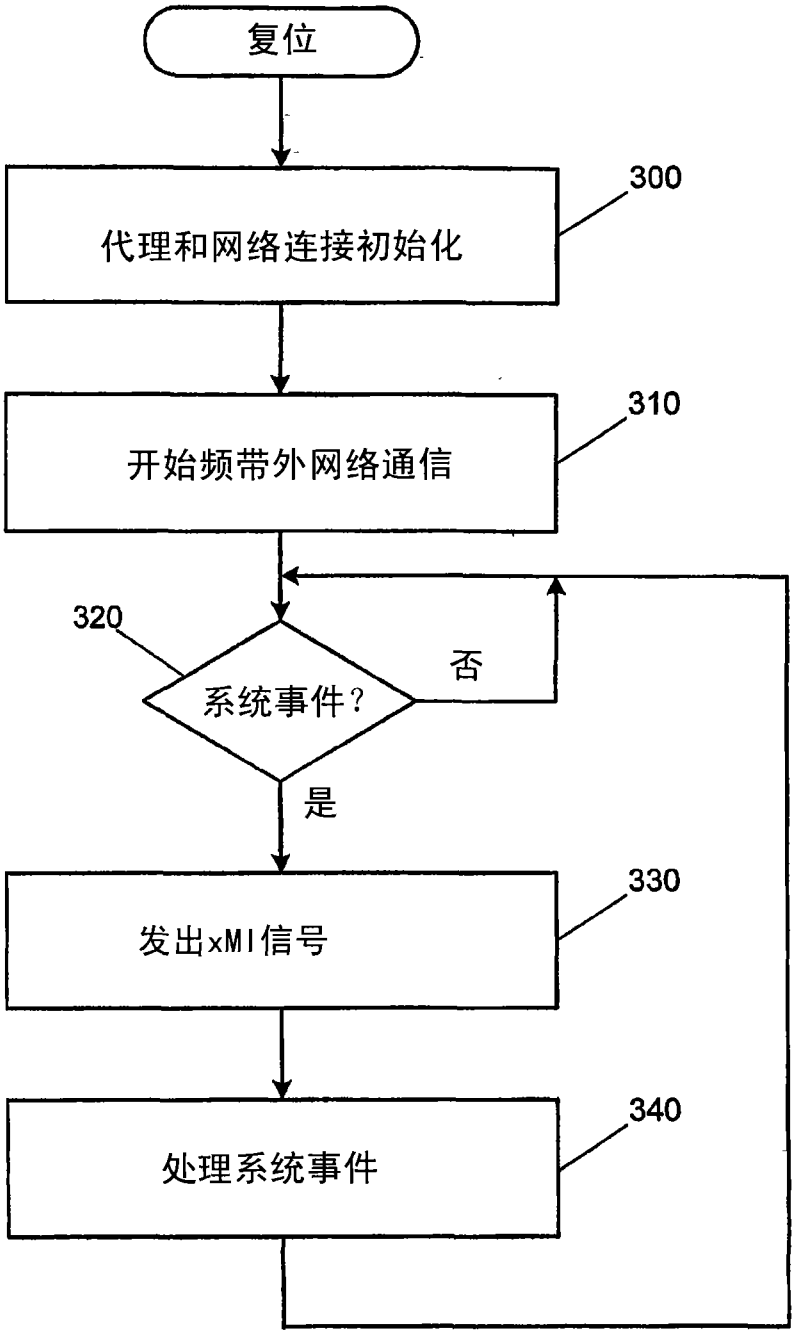

复位
300
代理和网络连接初始化
310
开始频带外网络通信
320
系统事件？
否
是
330
发出xMI信号
340
处理系统事件

图 3

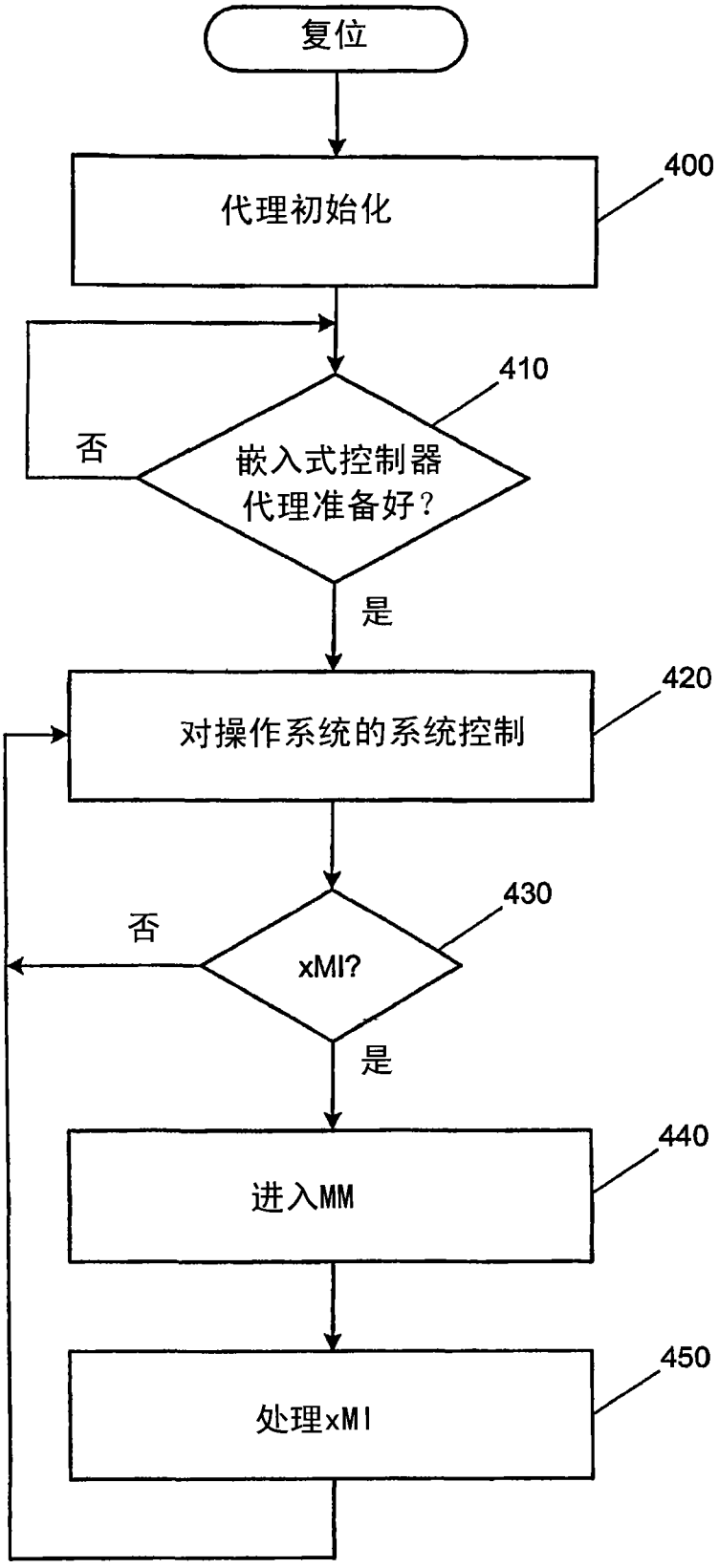

复位
代理初始化
400
410
否
嵌入式控制器
代理准备好？
是
420
对操作系统的系统控制
430
否
xMI?
是
440
进入MM
450
处理xMI

FIG. 4

图 4

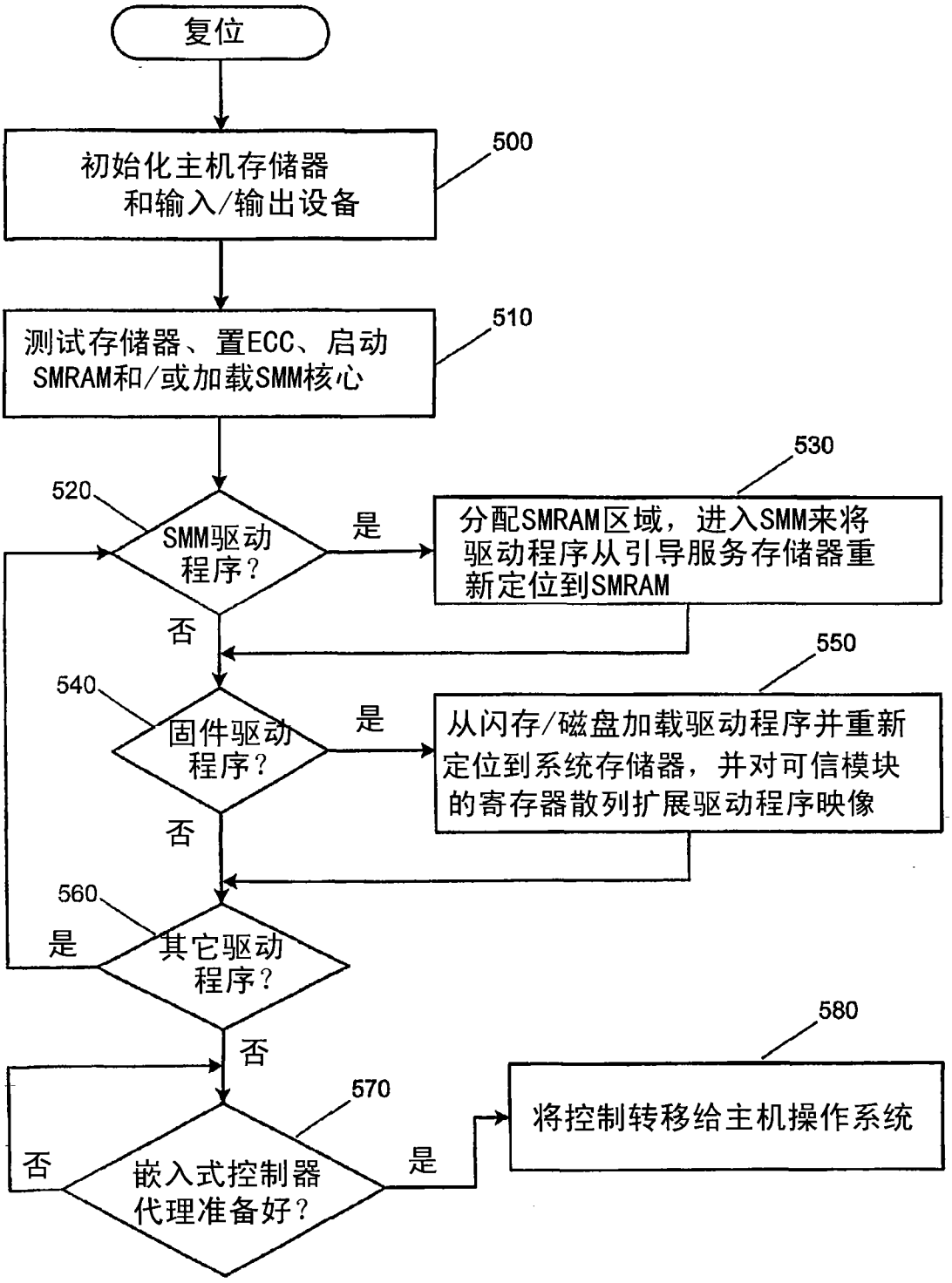

复位
初始化主机存储器
和输入/输出设备
500
测试存储器、置ECC、启动
SMRAM和/或加载SMM核心
510
520
SMM驱动
程序？
是
530
分配SMRAM区域，进入SMM来将
驱动程序从引导服务存储器重
新定位到SMRAM
否
540
固件驱动
程序？
是
550
从闪存/磁盘加载驱动程序并重新
定位到系统存储器，并对可信模块
的寄存器散列扩展驱动程序映像
否
560
是
其它驱动
程序？
否
570
否
嵌入式控制器
代理准备好？
是
580
将控制转移给主机操作系统

图 5

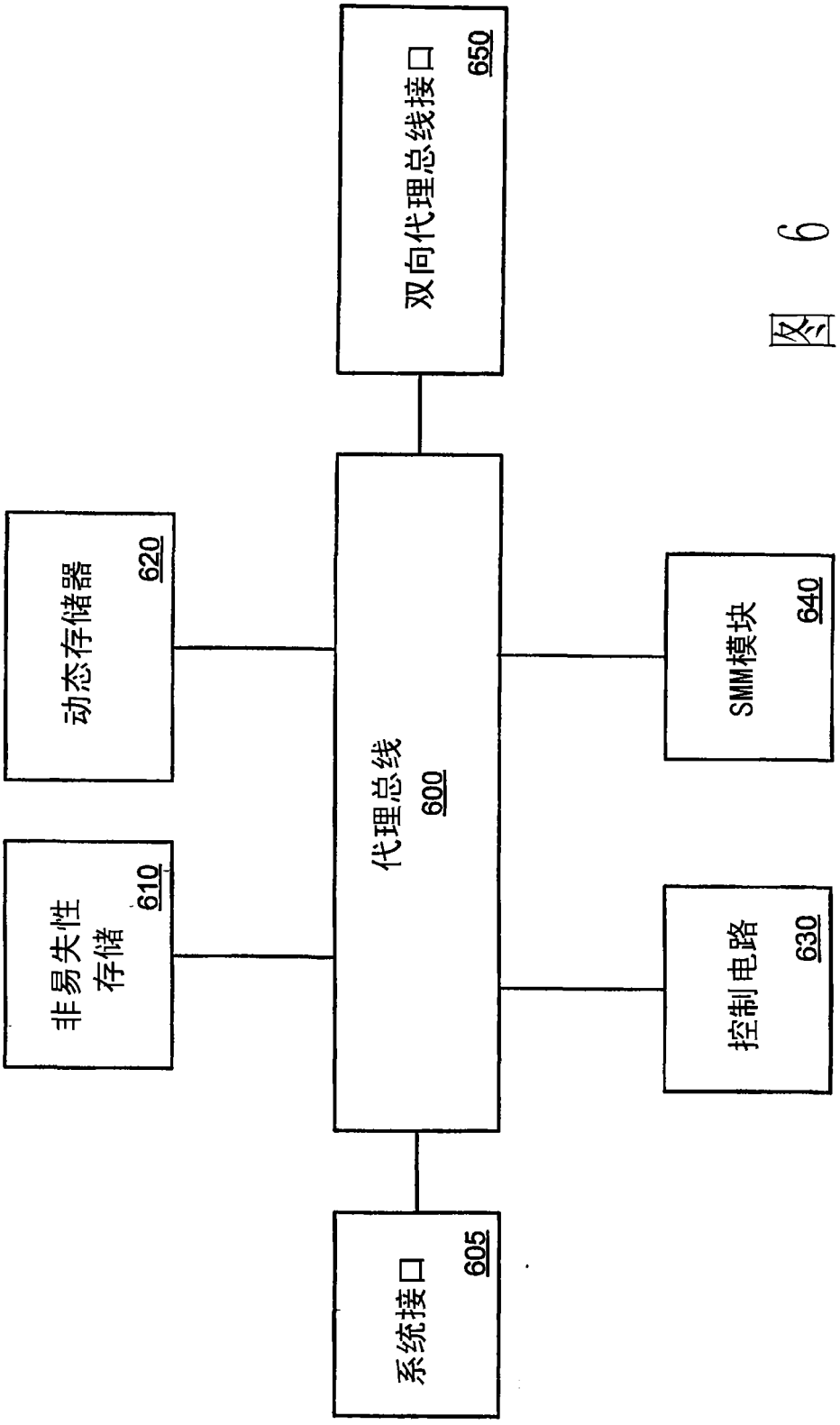

双向代理总线接口
650
动态存储器
620
非易失性存储
610
代理总线
600
SMM模块
640
控制电路
630
系统接口
605

图 6

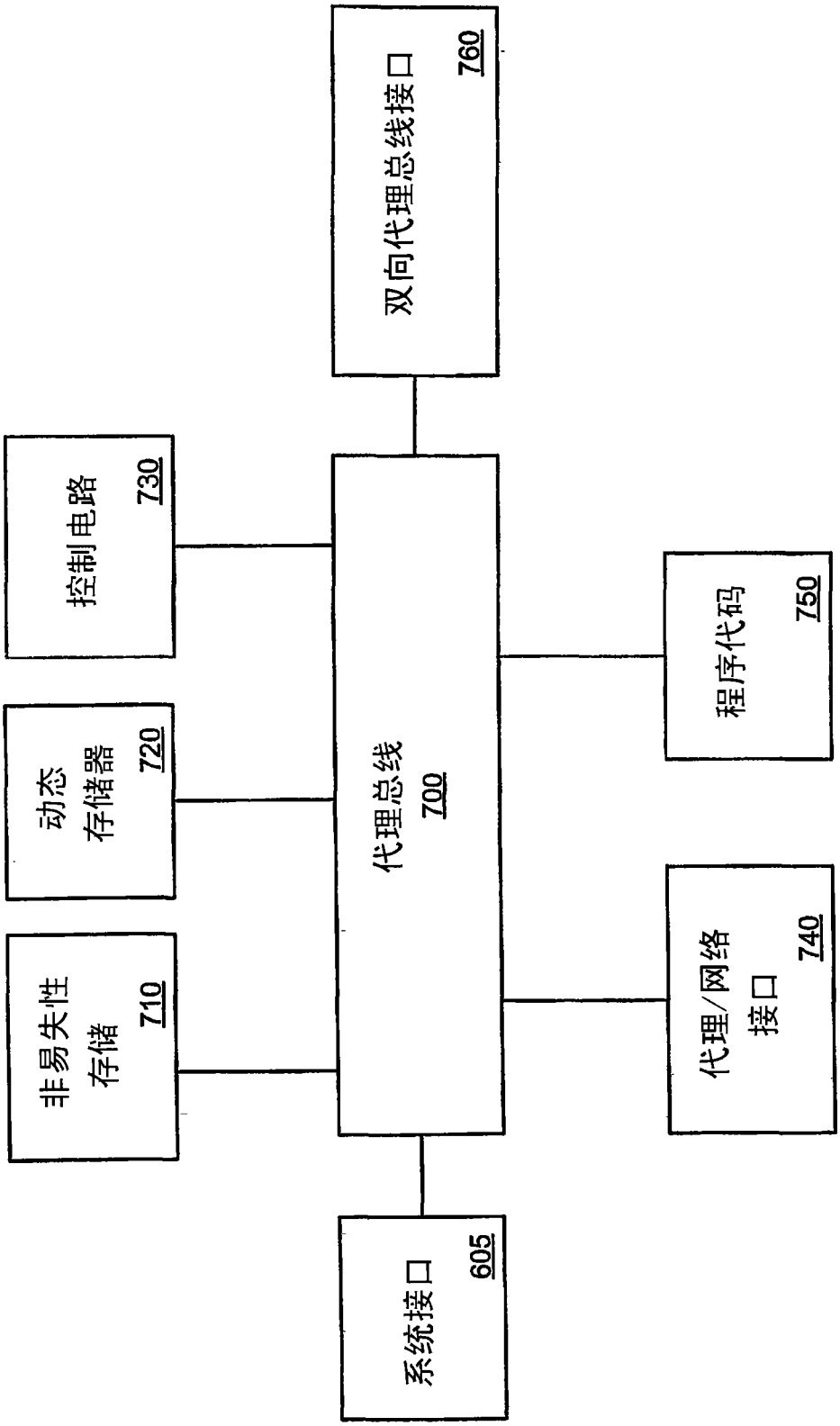

双向代理总线接口
760
控制电路
730
动态
存储器
720
非易失性
存储
710
代理总线
700
程序代码
750
代理/网络
接口
740
系统接口
605

图 7

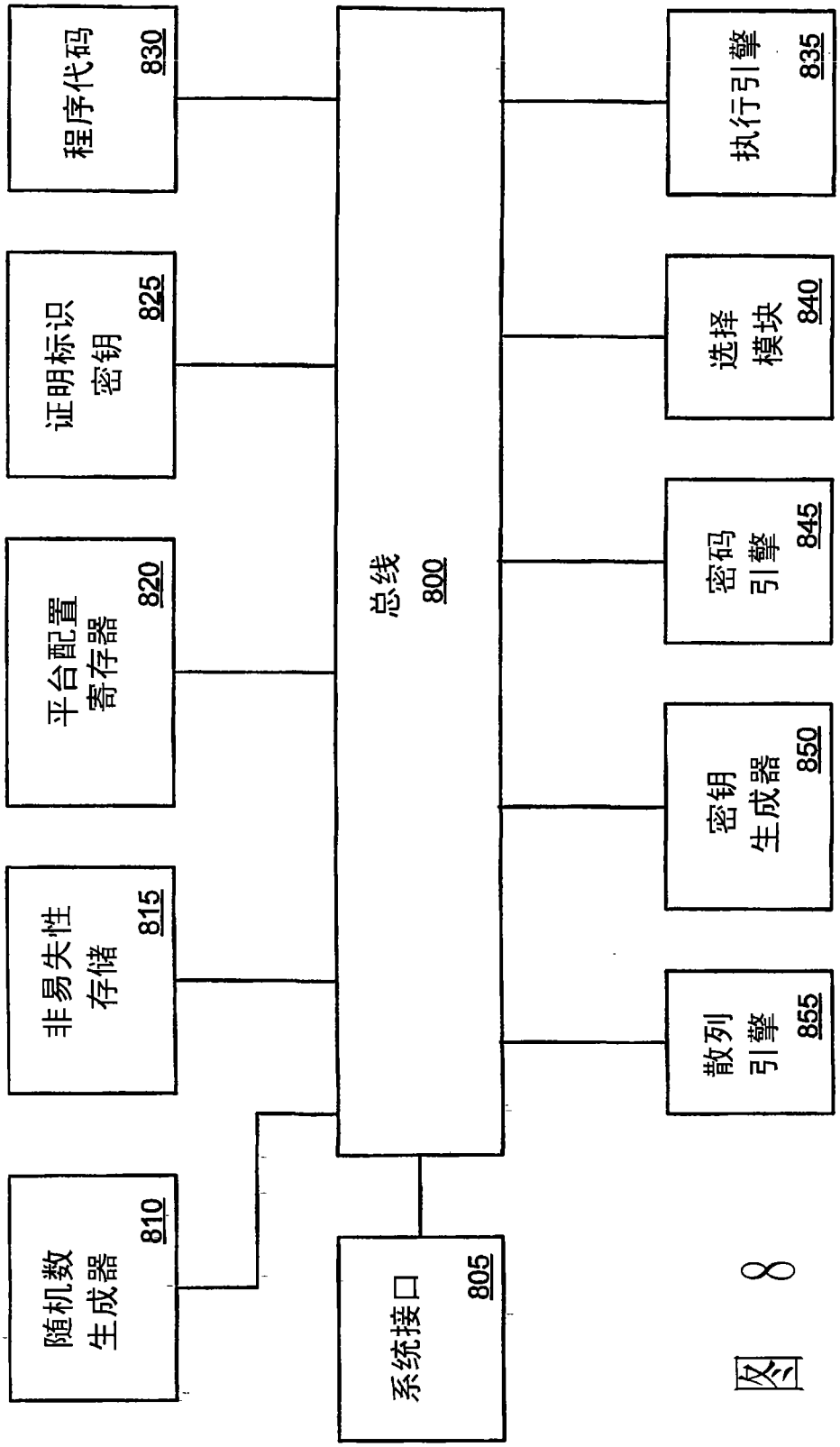

程序代码 830
证明标识 密钥 825
平台配置 寄存器 820
非易失性 存储 815
随机数 生成器 810
总线 800
系统接口 805
执行引擎 835
选择 模块 840
密码 引擎 845
密钥 生成器 850
散列 引擎 855

图 8