理器。

13．如权利要求 11 所述的系统，其中所述基板管理控制器通过隧道传送英特尔平台管理接口协议中的 TCPA 命令集来与所述主处理器通信。

14．如权利要求 11 所述的系统，其中所述基板管理控制器通过预留专用于 TCPA 消息传递的额外的命令－数据端口来与所述主处理器通信。

15．如权利要求 11 所述的系统，还包括连接到所述基板管理控制器的多个主处理器。

16．如权利要求 11 所述的系统，其中多个 BIOS 映像的完整性被验证。

17．如权利要求 11 所述的系统，其中熵相关数据由所述基板管理控制器收集以提供安全性度量。

18．如权利要求 11 所述的系统，其中功率损耗数据由所述基板管理控制器收集以提供可信平台模块功能。

19．如权利要求 11 所述的系统，其中所述基板管理控制器计算引导块的加密哈希值，以检测 BIOS 映像是否可信任。

20．如权利要求 11 所述的系统，其中所述基板管理控制器将密钥保留在隔离存储器中。