

(12) 发明专利申请

(10) 申请公布号 CN 103477343 A

(43) 申请公布日 2013. 12. 25

(21) 申请号 201280010063. 4

代理人 李晓冬

(22) 申请日 2012. 02. 22

(51) Int. Cl.

(30) 优先权数据

G06F 21/57(2013. 01)

102011012226. 5 2011. 02. 24 DE

(85) PCT申请进入国家阶段日

2013. 08. 22

(86) PCT申请的申请数据

PCT/EP2012/000765 2012. 02. 22

(87) PCT申请的公布数据

W02012/113547 DE 2012. 08. 30

(71) 申请人 信特尼有限公司

地址 英国剑桥

(72) 发明人 斯蒂芬·斯匹兹

(74) 专利代理机构 北京东方亿思知识产权代理

有限责任公司 11258

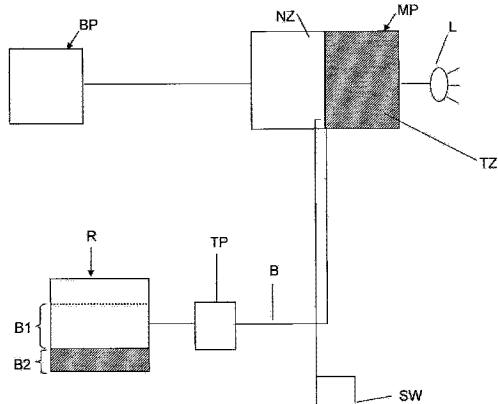
权利要求书1页 说明书5页 附图2页

(54) 发明名称

操作特别是在移动终端中的微处理器单元的方法

(57) 摘要

本发明涉及一种特别是在移动终端中的用于操作微处理器单元的方法，其中微处理器单元包括微处理器(MP)，在微处理器上以第一操作系统(B1)实施标准运行时间环境(NZ)并以第二安全操作系统(B2)实施安全运行时间环境。该微处理器单元还包括安全运行时间环境(TZ)外部的RAM存储器(R)，当执行标准运行时间环境(NZ)时，第一操作系统(B1)被载入到该RAM存储器中。本发明的特点是第二操作系统(B2)是第一操作系统(B1)的安全版本，在执行安全运行时间环境(TZ)期间，该安全版本被载入到RAM存储器的拟用于安全运行时间环境的部分中。



1. 一种用于操作特别是移动终端中的微处理器单元的方法，其中所述微处理器单元包括微处理器 (MP)，在所述微处理器 (MP) 上实施具有第一操作系统 (B1) 的标准运行时间环境 (NZ) 和具有第二操作系统 (B2) 的受保护的运行时间环境 (TZ)，所述微处理器单元还包括所述受保护的运行时间环境 (TZ) 外部的 RAM 存储器 (R)，当所述标准运行时间环境 (NZ) 被执行时，所述第一操作系统 (B1) 被载入到所述 RAM 存储器 (R) 中，所述方法的特征在于：

所述第二操作系统 (B2) 是所述第一操作系统 (B1) 的受保护的版本，在执行所述受保护的运行时间环境 (TZ) 的过程中，所述受保护的版本被载入到所述 RAM 存储器的为所述受保护的运行时间环境提供的部分中。

2. 如权利要求 1 所述的方法，其特征在于所述第二操作系统 (B2) 以 OnSoC RAM 的形式被载入到所述 RAM 存储器 (R) 中，其中所述 OnSoC RAM 特别地通过 AMBA 总线 (B) 被耦合到所述微处理器 (MP)。

3. 如权利要求 1 或权利要求 2 所述的方法，其特征在于所述微处理器单元是通过开关 (SW) 控制的，用户能够使用所述开关 (SW) 控制在所述标准运行时间环境 (NZ) 和所述受保护的运行时间环境 (TZ) 之间转换。

4. 如前述权利要求中的任何一个所述的方法，其特征在于使用指示器单元 (L) 来指示给用户何时所述受保护的运行时间环境 (TZ) 被执行。

5. 如前述权利要求中的任何一个所述的方法，其特征在于所述微处理器单元是为手机提供的并包含用于处理通信功能的基带处理器 (BP)，其中所述基带处理器 (BP) 的通信功能的一部分是在所述第二操作系统中实施的。

6. 如权利要求 5 所述的方法，其特征在于语音呼叫功能和 / 或 SMS 功能是在所述第二操作系统中作为所述基带处理器 (BP) 的通信功能被实施的。

7. 如前述权利要求中的任何一个所述的方法，其特征在于所述受保护的运行时间环境 (TZ) 是 ARM TrustZone<sup>®</sup>。

8. 一种特别是用于移动终端的微处理器单元，所述微处理器单元包括微处理器 (MP)，在所述微处理器 (MP) 上实施具有第一操作系统 (B1) 的标准运行时间环境 (NZ) 和具有第二操作系统 (B2) 的受保护的运行时间环境 (TZ)，所述微处理器单元还包括所述受保护的运行时间环境 (TZ) 外部的 RAM 存储器 (R)，当所述标准运行时间环境 (NZ) 被执行时，所述第一操作系统 (B1) 被载入到所述 RAM 存储器 (R) 中，

其特征在于：

所述第二操作系统 (B2) 是所述第一操作系统 (B1) 的受保护的版本，并且所述 RAM 存储器 (R) 的一部分是为所述第二操作系统 (B2) 提供的，在执行所述受保护的运行时间环境 (TZ) 的过程中，所述第二操作系统 (B2) 被载入到所述一部分中。

9. 如权利要求 8 所述的微处理器单元，其特征在于所述微处理器单元被设计以便使权利要求 2 到权利要求 7 之一所要求的方法能够在所述微处理器单元上被实现。

10. 一种移动终端，特别是手机，其特征在于所述移动终端包括根据权利要求 8 或权利要求 9 所述的微处理器单元。

## 操作特别是移动终端中的微处理器单元的方法

### 技术领域

[0001] 本发明涉及操作特别是移动终端中的微处理器单元的方法，并涉及合适的微处理器单元和合适的移动终端。

### 背景技术

[0002] 现有技术公开了在微处理器单元中实施所谓的受保护的运行时间环境，以便在隔离的环境中执行安全关键性应用。在这种情况下，微处理器单元意在被理解为指的是用于执行应用的所有硬件，特别是实际的微处理器和用于存储数据的恰当的存储器。

[0003] 常规的受保护的运行时间环境通常使用对存储要求低的操作系统，如现有技术中已知的 MobiCore<sup>®</sup> 操作系统，该操作系统被与所谓的 ARM TrustZone<sup>®</sup> 形式的受保护的运行时间环境相结合使用。在这种情况下，用于受保护的运行时间环境中的操作系统被加载到受保护的运行时间环境中的内部 RAM 存储器中。由于内部 RAM 存储器的大小有限，受保护的运行时间环境中使用的操作系统必须是小型的，这意味着当受保护的运行时间环境被执行时，由微处理器单元提供的功能的范围很小。只要仅有安全关键性任务被发送到受保护的运行时间环境，这就不是问题。然而，在特定的应用实例中，具有较大功能范围的受保护的运行时间环境也有必要由微处理器单元提供。如果微处理器单元被用于手机中，例如，防止窃听攻击的保护优先地要求提供能够用于手机的语音通话功能的受保护的运行时间环境。这不能通过目前的用于受保护的运行时间环境中的操作系统实现。

[0004] 因此，本发明的目的是操作微处理器单元，从而提供与现有技术相比具有更大的范围的功能的受保护的运行时间环境。

[0005] 该目的是通过根据专利权利要求 1 的方法、根据专利权利要求 8 的微处理器单元以及根据权利要求 10 的移动终端实现的。本发明的发展在从属权利要求中做出了限定。

### 具体实施例

[0006] 根据本发明的方法用于操作微处理器单元，所述微处理器单元包括微处理器，在微处理器上实施具有第一操作系统的标准运行时间环境及具有第二受保护的操作系统的受保护的运行时间环境。在这种情况下，微处理器单元还包括受保护的运行时间环境外部的 RAM 存储器，当执行标准运行时间环境时，第一操作系统被载入到 RAM 存储器中。第一操作系统特别是固有的用于微处理器单元的已知操作系统，例如，如果微处理器单元用于手机时的手机操作系统。这种手机操作系统的例子是用于智能手机并提供大范围的功能的 Android 或 Symbian。

[0007] 根据本发明的方法的特点在于第二操作系统是第一操作系统的受保护的版本，在受保护的运行时间环境的执行过程中，该受保护的版本被载入到 RAM 存储器的为受保护的运行时间环境提供的部分中。在这种情况下，第一操作系统的受保护的版本特别是所谓的加固的操作系统。术语“加固”众所周知是来自计算机工程并表示通过只使用操作诸如程序或操作系统之类的系统所必需的并在考虑到安全方面时保证正确运行的特定软件来加

强该系统的安全。

[0008] 根据本发明，因此不仅原始的第一操作系统而且满足更高安全需求的第二操作系统也被使用了。通常，与这种情形下的原始操作系统相比在受保护或加固的操作系统上功能的范围是缩小的，但明显大于为受保护的运行时间环境提供的常规的操作系统(如 MobiCore<sup>®</sup>)上的功能范围，这意味着还需要更多的存储器。本发明凭借将第二受保护的操作系统载入到受保护的运行时间环境外部的 RAM 存储器中来考虑到这点，因为该外部的存储器比受保护的运行时间环境中的内部 RAM 存储器具有更大的设计。

[0009] 在根据本发明的方法的一个特别优选的实施例中，第二操作系统以 OnSoC (SoC=System on a Chip，芯片上的系统) RAM 的形式被载入到 RAM 存储器中。在这种情况下，OnSoC RAM 与微处理器单元的其它组成部分一起整体地集成在芯片上。在一个优选的实施例中，OnSoC RAM 通过固有的公知的 AMBA (AMBA=Advanced Microcontroller Bus Architecture，高级微控制器总线架构) 总线被耦合到微处理器单元的微处理器。

[0010] 在根据本发明的方法的进一步特别优选的实施例中，微处理器单元通过用户能够用来在执行标准和受保护的运行时间环境间转换的开关而被控制。如此，用户能够规定他能够用来操作微处理器单元的模式。如果用户例如在保护关键性环境中使用微处理器单元，则他能够从第一非保护操作系统转换到第二受保护的操作系统。在这种情况下，第二操作系统提供比常规的受保护的运行时间环境大的功能范围，在常规的受保护的运行时间环境中操作系统被载入到受保护的运行时间环境内部的 RAM 存储器中。

[0011] 在进一步优选的实施例中，指示器单元被用来指示用户何时受保护的运行时间环境被执行，其结果是用户总是被通知他目前操作微处理器单元所处的模式。

[0012] 在根据本发明的方法的进一步特别优选的实施例中，微处理器单元被提供给手机，并包含用于处理通信功能的基带处理器。在该实施例中，为确保即使当受保护的运行时间环境被执行时特定的通信功能也被提供，基带处理器的通信功能的一部分也在第二操作系统被实施。优选地，这种情况下，语音呼叫功能或短消息服务 (SMS) 功能或两者都是作为基带处理器的通信功能被实施的，其结果是用户至少能够使用手机的基本功能。

[0013] 在根据本发明的方法的进一步特别优选的实施例中，受保护的运行时间环境是在固有公知硬件的基础上以所谓的 ARM TrustZone<sup>®</sup> 形式被实施的。与常规方法相比，源自为标准的运行时间环境提供的操作系统的受保护的或加固的操作系统现在被用在信任区 (TrustZone) 中以取代通常使用的 MobiCore<sup>®</sup> 操作系统。

[0014] 除上述方法外，本发明还涉及特别是用于移动终端的微处理器单元，该微处理器单元包括微处理器，在微处理器上实施具有第一操作系统的标准运行时间环境和具有第二操作系统的受保护的运行时间环境，还包括受保护的运行时间环境外部的 RAM 存储器，当执行标准运行时间环境时向该 RAM 存储器载入第一操作系统。该微处理器单元的不同之处在于第二操作系统是第一操作系统的受保护的或加固的版本，并且 RAM 存储器的一部分是为第二操作系统提供的，在执行受保护的运行时间环境的过程中，第二操作系统被载入到该部分中。

[0015] 优选地，微处理器单元被设计从而上述的根据本发明的方法的一个或多个优选的变体能够在该微处理器单元上实施。

[0016] 此外,本发明涉及到移动终端,特别是手机,该移动终端包括根据本发明的微处理器单元或根据本发明的微处理器单元的一个或多个变体。

[0017] 本发明的示例性实施例参照附图详述如下,其中:

[0018] 图1示出了基于现有技术在微处理器单元中实施受保护的运行时间环境;以及

[0019] 图2示出了基于本发明的实施例实施受保护的运行时间环境。

[0020] 下面对于根据本发明的方法的描述是基于为手机提供的微处理器单元的,然而,该方法也能用于其它移动设备中的微处理器单元。在这种情况下,微处理器单元以所谓的SoC (SoC=System on a Chip, 芯片上的系统)或信号芯片系统的形式被实施,即基本上微处理器单元所有的组件都集成在单个 IC 芯片上。

[0021] 图1示出了单个芯片系统的设计,其中受保护的运行时间环境是以常规形式实施的。在这种情况下,该芯片包含实际的微处理器 MP,它是 ARM 型微处理器,在该 ARM 型微处理器上以 TZ 表示的信任区 (TrustZone) 形式的受保护的运行时间环境以公知的方式被实施。在下面进一步描述的图1以及图2中,具有受保护的运行时间环境的区域在本例中总是以阴影形式示出。为了操作受保护的运行时间环境 TZ,图1中使用固有公知的 MobiCore® 操作系统。如移动支付应用或其它需要访问个人用户特定数据的应用之类的安全关键性功能被重新安置到受保护的运行时间环境。在操作信任区 TZ 期间, MobiCore® 操作系统被载入到信任区内的内部 RAM 存储器中,所述 RAM 存储器在图1中以 IR 表示。在本例中, RAM 存储器的包含 MobiCore® 操作系统的部分以 MC 表示。参考符号 MC 随后也被用来表示 MobiCore® 操作系统。

[0022] 除受保护的运行时间环境 TZ 外,微处理器 MP 还包含标准运行时间环境,在图1中以 NZ 表示。这存储了微处理器单元的常规操作系统,该操作系统比 MobiCore® 操作系统有更大的存储需求。在所述实施例中,该操作系统是如用于智能手机中的所谓的具有大范围功能的富 OS (richOS)。这种操作系统的一个例子是手机操作系统 Android。

[0023] 在执行标准运行时间环境期间, RAM 存储器 R 被用于图1的微处理器单元中,所述 RAM 存储器具有芯片上 OnSoC RAM 形式并通过固有公知的 AMBA 总线 B 链接到微处理器 MP。这种情况下,常规的 richOS 操作系统被载入到该 RAM 存储器中。在图1中, RAM 存储器的包含 richOS 操作系统的部分以 B1 表示。这一参考符号随后也被用来表示 richOS 操作系统。

[0024] 除微处理器 MP 外,图1的微处理器单元还包含被用来实施手机的通信功能的所谓的基带处理器 BP。因此,基带处理器 BP 与手机的 SIM/USIM 卡及移动无线网络通信,还可能与麦克风进行通信。

[0025] 为了在信任区 TZ 内以安全模式操作图1中的微处理器,在标准区 NZ 内提供启动到受保护的运行时间环境的转换的 MobiCore® 驱动器 D。如图1所示,在执行受保护的运行时间环境的过程中,仅使用只有有限存储量(大约 128kB) 的内部 RAM 存储器 IR。因此, MobiCore® 操作系统 MC 的功能范围比被载入到 OnSoC RAM 存储器 R 中的 richOS 的功能范围小很多,OnSoC RAM 存储器 R 具有明显更大的设计并且通常有几个兆字节的存储量。

[0026] 考虑到 MobiCore® 的小的功能范围,只有安全关键性任务能够被委派给受保护的安全时间环境。因此,在执行受保护的安全时间环境期间,微处理器单元的更多功能不能被使用。这是不利的,因为在特定的情形下,希望常规的操作系统的有如语音呼叫功能等的更多功能在执行受保护的运行时间环境的过程中也被控制。特别地,在公共领域环境内的攻击事件的情况下,比如电话窃听的情况下,基于受保护的运行时间环境的操作应该是可能的。由于当执行 MobiCore® 操作系统时不提供语音呼叫功能,所以 MobiCore® 不能确保针对这种袭击事件的保护。

[0027] 图 2 示出了根据本发明的微处理器单元的实施例,它用来解决上面提出的问题。在这种情况下,为与图 1 的组件对应的组件使用相同的参考符号。以与图 1 类似的方式,图 2 中的微处理器单元包括具有信任区 TZ 和标准区 NZ 的微处理器 MP。类似地,也提供基带处理器 BP 和 OnSoC RAM 存储器 R。与图 1 的实施例相比,现在不再基于 MobiCore® 操作系统执行信任区,而是使用常规的 richOS 操作系统 B1 的加固的变体。在这种情况下,在图 2 中以 B2 表示的加固的操作系统比操作系统 B1 有更小的功能范围,但现在明显比纯 MobiCore® 操作系统包含更多的功能。术语“加固”已经在上面进一步描述并涉及到操作系统功能范围的减小,从而增加其对来自未授权的第三方的攻击的安全性。因此,与原始操作系统相比,该加固的操作系统是受保护的具有减小的功能范围的操作系统是。

[0028] 根据图 2 的实施例,该加固的操作系统 B2 现在在信任区 TZ 的操作过程中被使用,但为此不再被载入到内部 RAM 存储器 IR,而是载入到 OnSoC RAM 存储器 R,这是因为内部 RAM 存储器对于加固的操作系统 B2 而言已不再足够。在图 2 所示的实施例中,加固的操作系统也包含基带处理器 BP 的特定的通信功能,特别是基带处理器 BP 的语音呼叫功能。这由基带处理器 BP 内的阴影区域表示。在这种情况下,加固的操作系统包含用于通过基带处理器 BP 通信的相关驱动器。

[0029] 根据应用实例,图 2 所示的微处理器单元允许使用标准操作系统 B1 和加固的操作系统 B2 二者。当微处理器单元被开启或启动时,通过 AMBA 总线访问 RAM 存储器 R 的所谓的信任区保护控制器 TP 随后被使用并被配置以使得 OnSoC RAM 存储器 R 的一部分是专用于信任区 TZ 的执行。尽管通过该信任区保护控制器分区的 OnSoC RAM 存储器的安全性不如内部 RAM 存储器 IR 高,但是该安全性对于保护整个加固的操作系统是足够的。合适的开关 SW 也允许使用手机在常规的操作系统 B1 和加固的操作系统 B2 间转换。在这种情况下,图 2 中的微处理器单元也包含 LED 形式的指示器单元 L,LED 的点亮发信号告知用户他所使用的手机处于受保护模式,其中在受保护模式中执行加固的操作系统。

[0030] 上述本发明的实施例有一系列优点。特别地,微处理器单元或相关手机的用户能够在设备中的手机的两种操作模式间选择或切换。首先,他能够基于操作系统 B1 在非保护模式下使用手机,在这种情况下他有机会利用已建立的 richOS 操作系统的优点,比如下载应用、使用 GPS 导航之类的。如果,相反地,手机的受保护的操作是必需的,则用户能够转换到安全模式,在安全模式下手机使用加固的操作系统 B2 操作。在这种情况下,用户不再拥有手机可用的所有功能,但是手机能够针对来自第三方的攻击被保护。然而,不像当图 1 所示的 MobiCore® 操作系统被使用时那样,在安全模式下电话的功能范围是更大的。特别

地,语音呼叫功能继续由手机确保。根据本发明,在受保护的运行时间环境中使用加固的操作系统允许如前面提到的操作系统 Android 之类的完整的手机操作系统被保护。在这种情况下,本发明特别适用于需要比基于 MobiCore<sup>®</sup> 的软件虚拟化更高级别的安全性而不一定为了安全性必须使用内部 RAM 存储器的应用(例如,在公共区域环境中,在窃听攻击的情况下)。

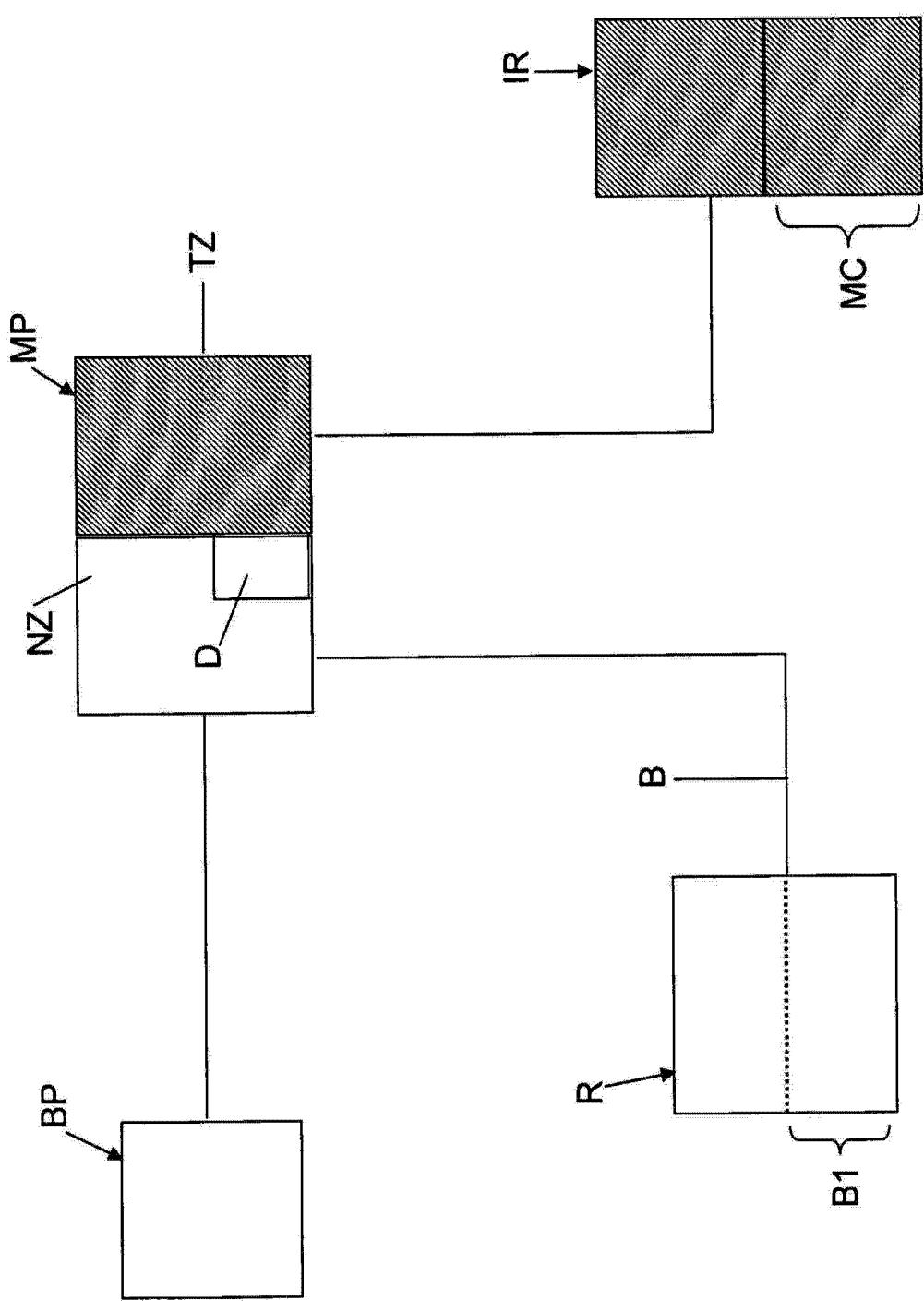


图 1

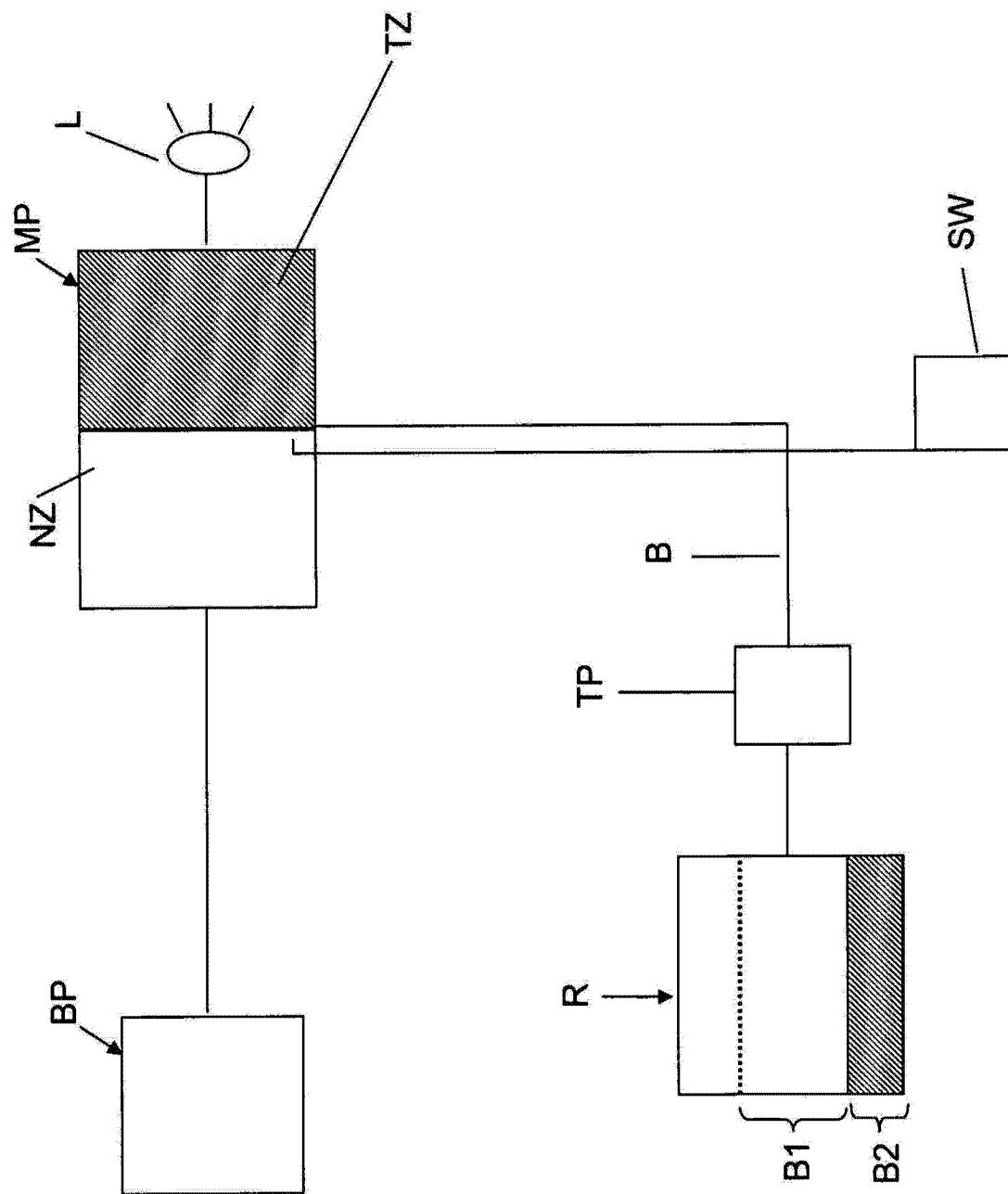


图 2