



(12) 发明专利

(10) 授权公告号 CN 102844815 B

(45) 授权公告日 2015. 11. 25

(21) 申请号 201080066463. 8

G11C 11/00(2006. 01)

(22) 申请日 2010. 10. 21

G11C 16/22(2006. 01)

(30) 优先权数据

102010028231. 6 2010. 04. 27 DE

(56) 对比文件

EP 1067557 A1 , 2001. 01. 10, 全文.

US 2007/0150754 A1 , 2007. 06. 28, 全文.

(85) PCT国际申请进入国家阶段日

2012. 10. 26

US 2007/0199046 A1 , 2007. 08. 23, 全文.

US 2009/0296479 A1 , 2009. 12. 03, 全文.

(86) PCT国际申请的申请数据

PCT/EP2010/065858 2010. 10. 21

US 5732017 A , 1998. 03. 24, 说明书第 3

栏第 37 行 - 第 7 栏第 45 行, 附图 1.

(87) PCT国际申请的公布数据

W02011/134541 DE 2011. 11. 03

US 6094724 A , 2000. 07. 25, 全文.

US 6421279 B1 , 2002. 07. 16, 说明书第 10

栏第 7-22 行、第 18 栏第 16 行 - 第 19 栏第 33 行, 附图 1-6.

(73) 专利权人 罗伯特·博世有限公司

地址 德国斯图加特

WO 02/01368 A2 , 2002. 01. 03, 说明书第 4

页第 16 行 - 第 10 页第 2 行, 附图 2-3.

(72) 发明人 M. 伊勒 A. 奥厄 R. 塞尔温斯基

O. 布贝克 J. 海克 J. 肖克罗拉希

审查员 房琦

(74) 专利代理机构 中国专利代理(香港)有限公

司 72001

代理人 李少丹 刘春元

(51) Int. Cl.

G06F 21/79(2013. 01)

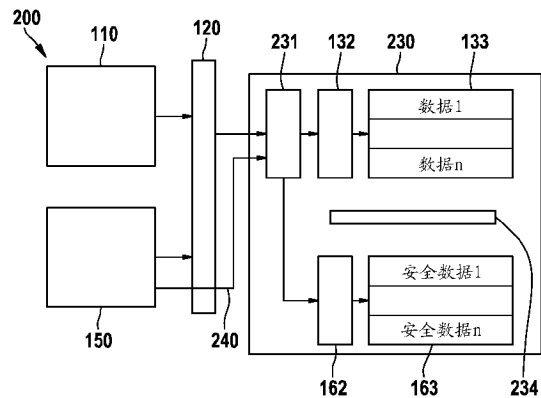
权利要求书1页 说明书3页 附图2页

(54) 发明名称

用于同时提供至少一个安全存储区域和至少一个非安全存储区域的存储模块

(57) 摘要

本发明涉及一种用于同时提供至少一个安全存储区域(163)和至少一个非安全存储区域(133)的存储模块(230),其中所述存储模块(230)包含有用于每个存储区域(133,163)的自身的写/读电子单元(132,162)以及至少一个共同的模拟电路部分(234),比如供电电路,以用于多个写/读电子单元(132,162)和/或多个存储区域(133,163)的供电。本发明还涉及具有这种存储模块(230)的微控制器(200)。尤其在闪存存储器中从而比如可以节省充电泵和/或写/读放大器工作台。



1. 一种包含存储模块(230)的微控制器(200),该存储模块用于同时提供至少一个安全存储区域(163)和至少一个非安全存储区域(133),其中所述存储模块(230)包含有用于每个存储区域(133,163)的自身的写/读电子单元(132,162)以及用于多个写/读电子单元(132,162)和/或多个存储区域(133,163)的至少一个共同的模拟电路部分(234),其中所述微控制器(200)包含有至少一个主 CPU (110)以及至少一个安全 CPU (150),其分别与所述存储模块(230)相连接,并对所述存储模块(230)进行存取以写和/或读非安全的或安全的数据。

2. 根据权利要求1所述的微控制器(200),其中所述存储模块(230)包含有用于所有写/读电子单元(132,162)和/或所有存储区域(133,163)的正好一个模拟电路部分(234)。

3. 根据权利要求1或2所述的微控制器(200),其中所述模拟电路部分(234)包含有供电电路,以给所述写/读电子单元(132,162)和/或存储区域(133,163)供电。

4. 根据权利要求1或2所述的微控制器(200),其中所述存储模块(230)包含有至少一个共同的接口单元(231),以连接至少两个写/读电子单元(132,162)。

5. 根据权利要求4所述的微控制器(200),其中所述存储模块(230)包含有正好一个接口单元(231),以连接所有的写/读电子单元(132,162)。

6. 根据权利要求1或2所述的微控制器(200),其中所述存储区域(133,163)作为闪存存储区域来构造,并且所述模拟电路部分(234)包含有充电泵和/或写/读放大器工作台。

7. 根据权利要求1所述的微控制器(200),其中所述至少一个主 CPU (110)以及所述至少一个安全 CPU (150)分别通过微控制器内部总线连接(120)与所述存储模块(230)的接口单元(231)相连接。

8. 根据权利要求1或7所述的微控制器(200),其中所述至少一个安全 CPU (150)附加地通过附加的识别连接(240)与所述存储模块(230)相连接。

9. 根据权利要求8所述的微控制器(200),其中所述至少一个安全 CPU (150)通过所述识别连接(240)与所述存储模块(230)的接口单元(231)相连接。

用于同时提供至少一个安全存储区域和至少一个非安全存储区域的存储模块

[0001] 本发明涉及一种用于同时提供至少一个安全存储区域和至少一个非安全存储区域的存储模块、以及一种具有这种存储模块的微控制器。

现有技术

[0002] 本发明涉及所谓的安全微控制器(secure microcontroller)领域、尤其汽车领域。在安全性重要的领域中的大多应用中,不可操纵的或不可见的数据存储是重要的基本要求。对称方法的密钥或者不对称方法的私有密钥是保密的,并从而必须在存取之前被保密。其他的应用情况需要至少防止更改,比如序列号或里程的存储、刷程序的禁止等。

[0003] 从而通常应所述为必须看到和/或改变所述秘密的一些功能的实施来提供安全的环境。所述环境通常包含一种“secure CPU”(安全 CPU)以及用于安全非易失地存储数据的分立存储模块,也称作“Secure NVM(安全 NVM)”(NVM=Non Volatile Memory,非易失存储器),所述存储模块仅能够通过所述“secure CPU”而被响应。

[0004] 要注意的是,为了提供安全的功能而使用了微控制器,其中所述微控制器除了通常的微控制器部件、诸如 CPU、存储模块、总线、I/O 接口等,还包含安全 CPU 以及安全存储模块。但是在微控制器中提供安全的环境是相对耗费的,这尤其归因于当今通常使用的非易失存储器技术。安全的存储模块一般作为闪存模块来构造,并如同所有的闪存存储模块一样包含有真正的存储器单元(晶体管)、用于运行所述存储器的写/读电子装置(比如状态机、地址缓冲器、数据缓冲器、行解码器、列解码器等)、用于把所述写/读电子装置连接到内部微控制器总线的接口单元以及用于供电和/或放大等的模拟电路部分。所述模拟电路部分通常(比如闪存、EEPROM)包含有充电泵(charge pump)和放大器工作台(Verstaerkerbank),所述模拟电路部分尤其需要非常多的芯片面积并导致所述模块显著的成本。

[0005] 从而希望在安全的微控制器中尽可能仅需要采用一个存储模块来记录安全的以及非安全的数据。但是,在现有技术所采用的存储模块中,对这种存储器进行存取的用户(通常是 CPU)可能看到并更改整个数据区域,使得采用相应一个存储模块来用于安全数据和非安全的数据。

[0006] 本发明的公开

[0007] 根据本发明推荐了具有权利要求 1 所述特征的一种存储模块。有利的扩展是从属权利要求以及下文说明的主题。

[0008] 本发明的优点

[0009] 本发明所基于的想法是,如果在此仅多重地构造对于提供安全功能必要的元件并仅尽可能简单地构造其他所有元件,那么就尤其简单地在一个存储模块中同时提供安全的和不安全或者说非安全的存储区域。如果为每个存储区域设置一个自身的写/读电子单元,但其中在所述存储模块中为所有的写/读电子单元仅设置一个模拟电路部分比如供电电路,那么一个存储模块就尤其能够同时提供安全的存储区域和非安全的存储区域。本发

明描述了一种扩展的存储模块,所述存储模块实现了针对多个用户对一个大存储器的共同利用。其允许用户分别使用自身专用的部分,由此保证了保密数据和 / 或不可操纵数据的安全性。根据本发明的存储模块可以有利地作为一个单独的所谓 Hard Macro (硬件宏) 在所述芯片上来定义。

[0010] 有利地仅设置一个接口单元以连接所述写 / 读电子单元。结果从而在一个唯一的存储模块中提供了具有自身的写 / 读电子单元的多个存储区域,但其中尤其有利地省略了多余的接口单元。

[0011] 根据本发明的一个有利的扩展,所述存储模块作为闪存存储模块来构造,然后其中为了给所设置数量的存储区域和写 / 读单元供电而仅设置了一个充电泵和 / 或一个放大器工作台(写 / 读放大器工作台)。尤其在闪存存储器中本发明具有特殊的优点,因为在此所述供电电路作为所述模拟电路部分的组成部分是特别费事的。

[0012] 本发明的其他优点和扩展参见本说明以及附图。

[0013] 应理解,前述的以及在下文中还要解释的特征不仅可以以相应所述的组合、而且还可以以其他的组合或单独地应用,而不脱离本发明的范畴。

[0014] 本发明借助一个实施例在附图中示意地示出,并在下文中参照附图来详细解释。

[0015] 附图的简述

[0016] 图 1 示意性示出了不包含在本发明保护范围中的一种安全微控制器的构造,

[0017] 图 2 示意性示出了一个微控制器的构造,其包含有根据本发明优选实施方式的存储模块。

[0018] 本发明的实施方式

[0019] 在图 1 和图 2 中分别仅示出了微控制器的对于本发明重要的部件,其中相同的元件设置有相同的参考符号。

[0020] 在图 1 中示意示出了安全微控制器,并整体用 100 来表示。所述微控制器 100 包含有主计算单元或主 CPU 110,其连接到微控制器内部的总线 120 上。在所述总线 120 上同样连接了一个第一存储模块 130,所述存储模块设置用于非安全地记录数据。

[0021] 在所述微控制器 100 中另外还通过一个安全 CPU 150 以及一个安全存储模块 160 提供了一个安全环境 140。为了实施安全的功能,所述安全 CPU 150 通过所述总线 120 被响应,并在需要时就存取所述安全存储模块 160。

[0022] 所述存储模块 130 和 160 基本相同地构造,并分别支配有接口单元 131 及 161 以把所述存储模块连接到所述微控制器内部总线 120,并支配有写 / 读电子单元 132 及 162 以及自身的存储区域 133 及 163。所述存储模块 130 和 160 符合目的地包含有闪存存储器,使得所述存储区域 133 和 163 包含有许多浮栅晶体管来作为存储器单元。另外所述存储模块 130 和 160 还分别包含有一个模拟电路部分 134 及 164,其在所述的闪存存储器的例子中至少包含有具有充电泵的一个供电电路以及一个写 / 读放大器工作台。所述写 / 读电子单元 132 和 162 分别包含有比如状态机、地址缓冲器、数据缓冲器、行解码器、列解码器等。所述存储模块 130 和 160 是分立的模块,并从而分别作为硬件宏在所述芯片面上来定义。

[0023] 在图 2 中示意示出了根据本发明优选实施方式的微控制器 200。所述微控制器 200 同样包含有多个部件,其中再次仅描绘了对于本发明重要的部分。在此已经在图 1 中示出的部件设置有相同的参考符号。

[0024] 所述微控制器 200 包含有根据本发明优选实施方式的存储模块 230。所述存储模块 230 构造用于同时提供一个非安全的存储区域 133 以及一个安全的存储区域 163。所述存储区域 133 和 163 分别设置有所属的写 / 读电子单元 132 及 162。所述写 / 读电子单元 132 和 162 分别包含有比如状态机、地址缓冲器、数据缓冲器、行解码器、列解码器等,也即主要是为了提供安全分离的存储区域所需的元件。

[0025] 但所述存储模块 230 有利地仅支配有一个唯一的模拟电路部分 234,其在闪存存储器的情况下尤其包含有一个具有充电泵的供电电路和 / 或一个写 / 读放大器工作台,并且其用于给所述存储模块 230 的所有元件供电。

[0026] 根据所示的优选实施方式,所述写 / 读电子单元 132 和 162 通过一个唯一的接口单元 231 而对外连接,在本情况中连接到所述微控制器内部总线 120。

[0027] 有利地所述存储模块 230 可以为了同时提供安全的和非安全的存储区域而作为硬件宏在芯片面上来定义。

[0028] 根据在此所示的本发明的实施方式,所述安全 CPU 150 通过一个识别连接 240 而与所述安全存储模块 230 或其接口单元 231 相连接。通过在所述接口单元 231 中增加一个相应的电路逻辑,如果行使存取的用户是明确可识别的,那么就可以限制用户对不同存储区域 133 和 163 的存取。所述明确的识别比如可以通过所述识别连接 240 来进行。但所述识别也可以通过所述总线 120 来进行,为此比如可以采用已公开的信号,如主机接口识别码。

[0029] 虽然在本例子中仅有两个用户、也即所述 CPU 110 和 150 来存取在所述安全存储模块 230 中的仅两个存储区域、也即所述存储区域 133 和 163,但本发明并不局限于所述实施方式。相反可以相互独立地提供任意多的用户和任意多的存储区域。

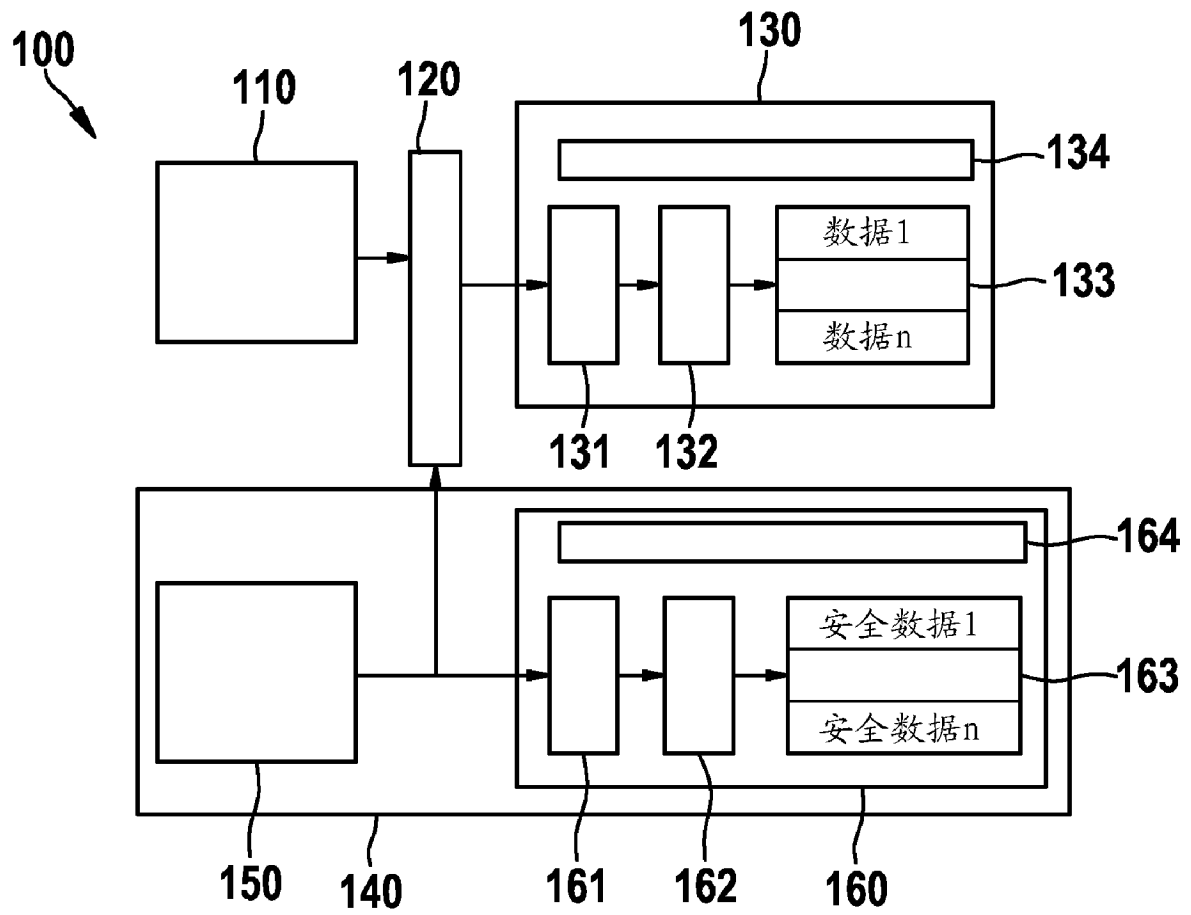


图 1

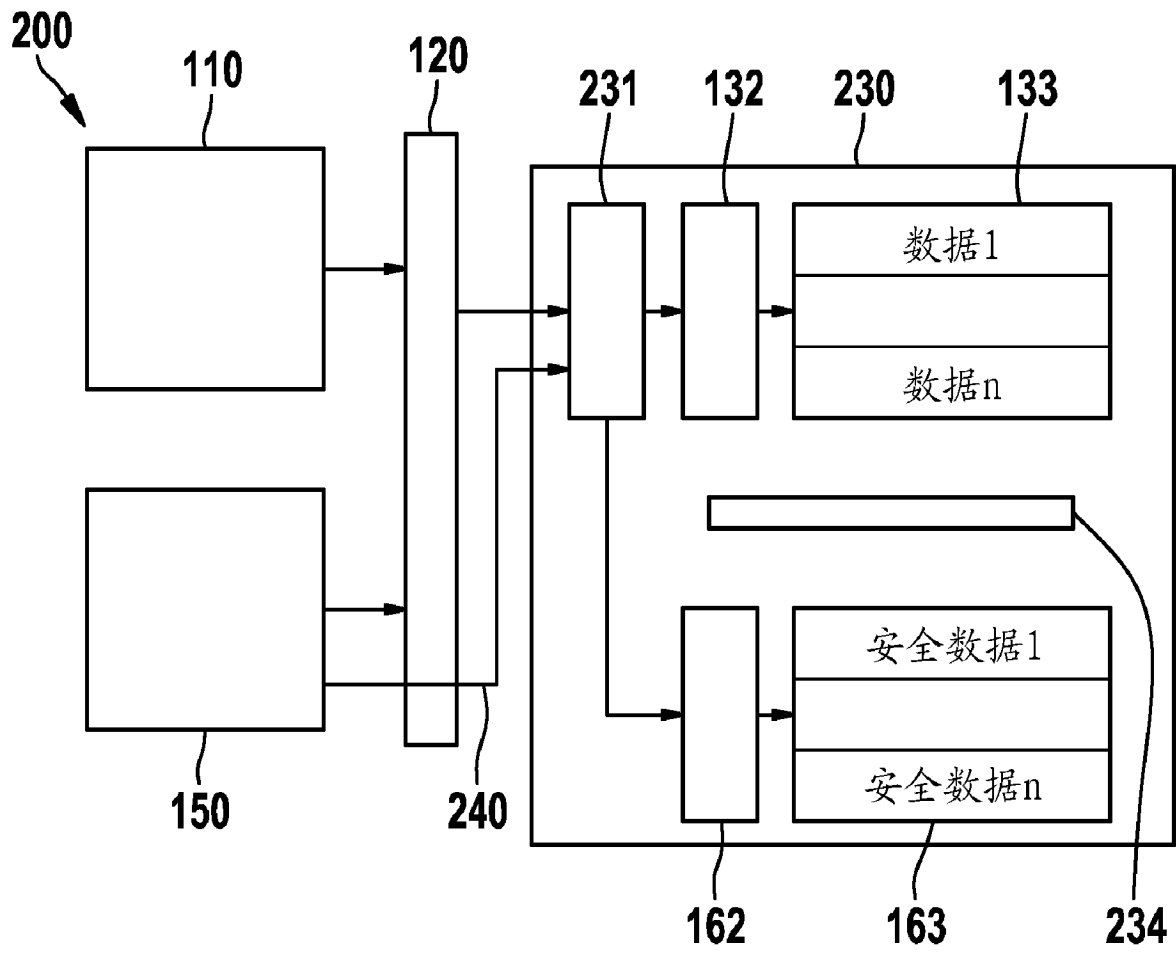


图 2