



(12) 发明专利申请

(10) 申请公布号 CN 105573159 A

(43) 申请公布日 2016. 05. 11

(21) 申请号 201510716005. 9

(22) 申请日 2015. 10. 29

(30) 优先权数据

102014222181. 1 2014. 10. 30 DE

(71) 申请人 罗伯特·博世有限公司

地址 德国斯图加特

(72) 发明人 C. 波尔 H. 哈乔格卢 F. 施通普夫

(74) 专利代理机构 中国专利代理(香港)有限公司
72001

代理人 卢江 胡莉莉

(51) Int. Cl.

G05B 19/04(2006. 01)

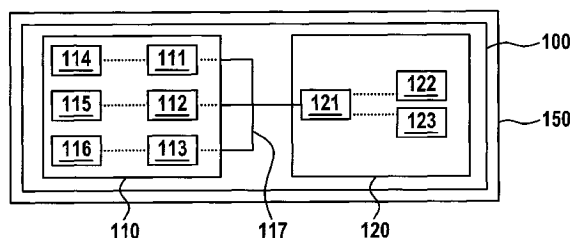
权利要求书1页 说明书6页 附图2页

(54) 发明名称

用于运行控制设备的方法

(57) 摘要

本发明提出用于运行控制设备的方法。本发明涉及用于运行具有拥有处理器单元(110)和安全处理器单元(120)的片上系统(100)的控制设备(150)的方法,其中处理器单元(110)和安全处理器单元(120)分别包括至少一个处理器内核(111、112、113;121),其中处理器单元(110)指示安全处理器单元(120)实施安全关键过程,其中由处理器单元(110)或安全处理器单元(120)给要在安全处理器单元(120)中实施的安全关键过程(210、220、230、240)分别分配优先级并且其中安全关键过程(210、220、230、240)在安全处理器单元(120)中根据相应的优先级来实施。



1. 用于运行具有拥有处理器单元(110)和安全处理器单元(120)的片上系统(100)的控制设备(150)的方法,

- 其中所述处理器单元(110)和所述安全处理器单元(120)分别包括至少一个处理器内核(111、112、113 ;121),

- 其中所述处理器单元(110)指示所述安全处理器单元(120)实施安全关键过程(210、220、230、240),

- 其中由所述处理器单元(110)或所述安全处理器单元(120)给要在所述安全处理器单元(120)中实施的安全关键过程(210、220、230、240)分别分配优先级,以及

- 其中在所述安全处理器单元(120)中根据相应的优先级来实施所述安全关键过程(210、220、230、240)。

2. 根据权利要求1所述的方法,其中,

- 如果在所述安全处理器单元(120)中实施具有第一优先级的第一安全关键过程(210)并且如果所述处理器单元(110)指示所述安全处理器单元(120)实施具有比所述第一优先级更高的第二优先级的第二安全关键过程(220),

- 所述第一安全关键过程(210)的实施在所述安全处理器单元中被中断,

- 所述第二安全关键过程(120)在所述安全处理器单元(120)中被实施,以及

- 在所述第二安全关键过程(220)的实施之后,所述第一安全关键过程(210)的实施在所述安全处理器单元(120)中被继续。

3. 根据权利要求2所述的方法,其中,如果所述第一安全关键过程(210)的实施在所述安全处理器单元(120)中被中断,则存放所述实施的当前进展,并且其中在所述第二安全关键过程(220)的实施之后,所述第一安全关键过程(210)的实施在所述安全处理器单元(120)中在该所存放的当前进展的情况下被继续。

4. 根据权利要求3所述的方法,其中,所述第一安全关键过程(210)的实施在所述安全处理器单元(120)中在该所存放的当前进展的情况下自主地没有所述处理器单元的介入地被继续。

5. 根据前述权利要求之一所述的方法,其中,在所述安全处理器单元(120)中实施要实时地实施的安全关键过程(210、220、240),使得实时条件被满足。

6. 根据权利要求5所述的方法,其中,给要实时地实施的安全关键过程(210、220、240)分配比不要实时地实施的安全关键过程(230)更高的优先级。

7. 根据前述权利要求之一所述的方法,其中,在所述安全处理器单元(120)中实施有实时能力的操作系统。

8. 计算单元(150),该计算单元被设置用于执行根据前述权利要求之一所述的方法。

9. 计算机程序,当所述计算机程序在计算单元(150)上被实施时促使所述计算单元(150)执行根据权利要求1至7之一所述的方法。

10. 机器可读的存储介质,该存储介质具有存储在其上的根据权利要求9所述的计算机程序。

用于运行控制设备的方法

技术领域

[0001] 本发明涉及用于运行具有拥有处理器单元和安全处理器单元的片上系统的控制设备的方法以及用于执行该方法的计算单元和计算机程序。

背景技术

[0002] 片上系统(System-on-a-Chip, SoC)是一种集成电路(IC),在该集成电路中相应系统的多种功能被集成在唯一的芯片(裸片(Die))上。这种 Soc 可以包括处理器单元(处理器系统部分, PS)。这种处理器单元可以包括适宜的处理器或处理器内核或者多核处理器。多核处理器包括多个(至少两个)处理器内核。处理器内核大多包括算术逻辑单元(ALU)以及此外包括本地存储器,该算术逻辑单元是用于实施任务、程序、计算命令等的实际的电子运算器。

[0003] 除了处理器单元之外, SoC 也可以包括所谓的硬件安全模块(Hardware Security Module, HSM)。与常规的处理器单元类似,该 HSM 也可以包括一个或多个处理器内核以及本地存储器(ROM、RAM、闪存、EEPROM)。HSM 因此具有不依赖于处理器单元的自己的物理资源((多个)处理器内核、本地存储器等等)。HSM 的资源尤其可以相对于处理器单元的资源在硬件层面上被屏蔽。

[0004] HSM 是被保护免于尤其对处理器单元的操纵和攻击的被隔离的安全环境并且因此尤其可以被用于安全关键过程或操作。在这种安全关键或密码过程期间可以处理和 / 或创建例如签名、加密等的安全关键数据。

[0005] 可以被证明为适宜的是,将具有处理器单元和 HSM 的这种 SoC 集成到控制设备中、尤其是机动车的控制设备、譬如发动机控制设备中。但是,常规的 HSM 大多不适于在这种控制设备中应用并且不能保证遵守适用于机动车领域的(安全)要求和(安全)规范。

[0006] 例如可以在控制设备中要求确定的过程、尤其是安全关键过程满足实时条件,即这些过程的结果在所定义的时间间隔之内被有保证计算出,也即在确定的时间块之前存在。但是利用常规的 HSM 大多不能保证安全关键过程满足实时条件。

[0007] 因此值得期望的是,提供将具有处理器单元和硬件安全单元的片上系统实现到控制设备中、尤其是实现到机动车的控制设备中的可能性。

发明内容

[0008] 根据本发明提出具有权利要求 1 的特征的用于运行控制设备的方法。有利的构型是从属权利要求以及随后的描述的主题。

[0009] 所述控制设备尤其被构造为机动车的控制设备,尤其是被构造为发动机控制设备。该控制设备包括具有处理器单元和安全处理器单元的片上系统(SoC),所述处理器单元和所述安全处理器单元分别包括至少一个处理器内核。所述处理器单元和所述安全处理器单元分别尤其包括相对于电压变化、时钟变化和温度变化的保护机构。

[0010] 此外,所述处理器单元和所述安全处理器单元分别尤其包括本地存储器、例如闪

速存储器、ROM 存储器、RAM 存储器和 / 或 EEPROM 存储器。替代地或附加地,尤其也可以针对处理器单元和安全处理器单元设置共同的本地存储器。在这种情况下尤其设置有存储器安全机构,例如存储器保护单元(Memory Protection Unit, MPU)。这种存储器安全机构管理对该共同的存储器的访问并且保护该共同的存储器免于操纵和攻击。尤其通过这种存储器安全机构针对处理器单元和安全处理器单元在共同的存储器中实现存储区的隔离。

[0011] 所述安全处理器单元尤其被构造为硬件安全模块(Hardware Security Module, HSM)。处理器单元和安全处理器单元尤其相互不相关并且分别具有自己的物理资源(处理器内核、本地存储器等等)。所述安全处理器单元尤其在硬件层面上被屏蔽并且是安全的环境,所述环境被保护免于操纵和攻击或者至少应当使操纵或攻击变得困难。

[0012] 处理器单元可以指示安全处理器单元实施安全关键过程。处理器单元和安全处理器单元尤其可以通过通信系统、例如适宜的总线或被共同利用的存储器或通信寄存器或其组合处于通信连接中。

[0013] 安全关键过程或密码过程尤其应被理解为如下过程,在这些过程中处理和 / 或产生安全关键数据、例如对于某些操作来说所需的秘密密钥,所述数据作为整体或部分地不应离开 SoC 或不应到达第三方。例如,如下过程或操作中的一个或多个可以被视为这种安全关键过程:产生和 / 或检验签名;加密和 / 或解密数据;应用哈希算法;产生编码和 / 或密码;认证和 / 或验证消息、控制命令和 / 或操控值,存储安全关键数据。

[0014] 根据本发明,给要在安全处理器单元中实施的安全关键过程分别分配优先级并且所述安全关键过程在安全处理器单元中根据相应的优先级来实施。尤其是,如果处理器单元指示安全处理器单元实施相应的安全关键过程,则处理器单元本身给该安全关键过程分配相应的优先级。也可以设想,安全处理器单元给要实施的安全关键过程分配相应优先级。

[0015] 尤其是处理器单元的各个处理器内核指示安全处理器单元实施相应的安全关键过程。例如在处理器单元的相应处理器内核中实施的操作系统可以相应地指示安全处理器单元。在处理器单元的各个处理器内核中也可以实施(特别是非安全关键)过程或操作或应用。也可以设想这些过程相应地直接指示安全处理器单元。

[0016] 尤其可以在安全处理器单元中创建流程图或顺序(“调度(scheduling)”),根据所述流程图或顺序来实施不同的安全关键过程。尤其根据相应的优先级递减地实施安全关键过程。具有高优先级的安全关键过程尤其首先被实施,具有低优先级的安全关键过程尤其最后被实施。

[0017] 本发明的优点

通过本发明使得能够灵活地规划要完成的安全关键过程。通过本发明可以区分其完成非常重要并且应当尽可能快地进行的相关的安全关键过程与其完成不迫切并且不应尽快地进行的具有次要重要性的安全关键过程。

[0018] 尤其通过本发明不必要的是,安全处理器单元按其被指示的顺序实施安全关键过程。具有高优先级的相关的安全关键过程可以在具有次要重要性以及低优先级的安全关键过程之前被实施。安全处理器单元尤其分别仅实施一个唯一的安全关键过程并且不同时实施多个安全关键过程。通过本发明使得能够合理地利用安全处理器单元的资源并且根据安全关键过程的重要性和相关性来完成安全关键过程。

[0019] 常规硬件安全模块也不能同时实施多个过程。在常规硬件安全模块中必要时可能

必需的是,在可以启动新的过程之前,等待直到当前在HSM中实施的过程结束。根据当前实施的过程,可能必要时持续比较长的时间、例如多达数秒,直到可以启动新过程。据此,在可以实施重要的安全关键过程之前,必要时首先必须等候多达数秒。

[0020] 通过本发明来消除常规硬件安全模块的这种问题。给其实施非常重要并且应当尽可能快地被执行的相关的安全关键过程分别分配高或最高的优先级。这些安全关键过程在安全处理器单元中作为第一个并且尽可能快地被实施。因此可以保证尽可能快地创建或处理迫切需要的安全关键数据。

[0021] 可以设想适宜地大的数目的不同优先级或不同优先级等级。越多不同的优先级可以被分派给安全关键过程,就可以越好地区分不同安全关键过程的相关性。

[0022] 通过本发明尤其可以保证遵守适用于机动车领域的(安全)要求和(安全)规范。尤其通过本发明实现安全处理器单元的实时能力。本发明因此尤其适于机动车的控制设备,例如适于发动机控制设备。通过本发明可以阻止对控制设备的攻击和操纵。在机动车的控制设备的情况下尤其可以保证“专有技术(Know-How)保护”并且诸如在“芯片调谐(Chiptuning)”的情况下禁止对控制设备软件的操纵。

[0023] 尤其在安全关键过程期间处理和/或创建对于机动车的操控和运行而言所需的数据、例如专门的操控命令、技术数据、控制值或特征值。这些命令或值由制造商常常在多年的开发过程中以高的研究耗费通过长时间持续的并且昂贵的测试系列所确定并且最优化。因此在制造商的意义上,这些数据不能被第三方、攻击者读出,以便保障“专有技术保护”。

[0024] 在“芯片调谐”期间攻击者尝试操纵所实施的安全关键过程并且在此改变控制设备的控制参数,以便造成功率提高。这可能导致构件损坏和环境污染,甚至导致人员伤害,因为可能损害总的车辆设计(驱动装置、制动装置)。

[0025] 有利地,具有低优先级的安全关键过程的实施可以为了具有高优先级的安全关键过程而被中断并且稍后再次被继续。安全处理器单元并不严格地并且强制性地受要完成的安全关键过程的所创建的流程图或所创建的顺序的约束。所述流程图或所述顺序尤其可以随时被改变,各个安全关键过程可以可以在流程图或顺序方面在需要时灵活地重新被分配。

[0026] 如果在安全处理器单元中实施具有第一优先级的第一安全关键过程并且如果处理器单元指示安全处理器单元实施具有比第一优先级更高的第二优先级的第二安全关键过程,则在安全处理器单元中第一安全关键过程的实施优选地被中断或暂停并且第二安全关键过程在安全处理器单元中被实施。

[0027] 一旦安全处理器单元获得呼叫具有更高优先级的安全关键过程的相应的指示,这尤其可以自动地进行。有利地,例如在安全处理器单元的本地存储器(RAM、闪速、EEPROM)中,存放并且(完整地)存储第一安全关键过程的实施的当前进展。

[0028] 在第二安全关键过程的实施之后,第一安全关键过程的实施优选地在安全处理器单元中被继续。该实施有利地直接在所存放的当前进展的情况下被继续。因此第一安全关键过程的数据没有丢失,该实施不必重新被启动。优选地,第一安全关键过程的实施自主地被继续,而不需要处理器单元的另外的交互。

[0029] 如果在第二安全关键过程的实施期间一个或多个另外的分别被分配比第一安全

关键过程更高的优先级但比第二安全关键过程更低的优先级的安全关键过程的实施被指示,则在第二安全关键过程的实施之后优选地首先实施这些另外的安全关键过程并且此外第一安全关键过程保持中断或暂停。

[0030] 有利地,安全处理器单元具有实时能力。要实时地实施的安全关键过程在安全处理器单元中被实施,使得实时条件被满足。该实时条件尤其在规范 DIN 44300 中定义。这些安全关键过程由安全处理器单元有保证地在预先给定的、所定义的时间间隔之内完整地实施。这些安全关键过程的结果在该所定义的时间间隔之内被有保证地计算并且据此在确定的时间块之前存在。此外提供这些安全关键过程的决定论或可预测性。

[0031] 在安全处理器单元中可以除了这种要实时地实施的安全关键过程之外也实施不应满足实时条件的安全关键过程。优选地给要实时地实施的安全关键过程分配比不要实时地实施的安全关键过程更高的优先级。

[0032] 安全处理器单元的实时能力尤其可以通过以下可能性来保证:为了具有高优先级的安全关键过程中断并且稍后又继续具有低优先级的安全关键过程的实施。当前所实施的次要的安全关键过程因此可以为了必须满足实时条件的安全关键过程被中断。尤其给要实时地实施的安全关键过程根据相应时间间隔分配优先级,在所述时间间隔之内必须实施该安全关键过程。

[0033] 优选地,在安全处理器单元中实施有实时能力的操作系统。可以由这种有实时能力的操作系统实施计算操作(例如过程、任务、应用等等),使得相应的实时条件被满足。有实时能力的操作系统尤其满足根据规范 DIN 44300 定义的实时条件。据此,用于处理出现的数据或要实施的安全关键过程的程序持续地是操作准备就绪的,使得这些处理的结果在预先给定的时间段之内是可用的。所述数据可以根据应用情况在时间上随机地分配之后或在预先确定的时间点出现。

[0034] 根据本发明的计算单元、例如片上系统或机动车的控制设备尤其在程序技术上被设置用于执行根据本发明的方法。

[0035] 以软件的形式实现所述方法也是有利的,因为这尤其是在实施的控制设备还被用于另外的任务并且因此总归存在时引起特别低的成本。用于提供计算机程序的合适的数据载体尤其是磁盘、硬盘、闪速存储器、EEPROM、CD-ROM、DVD 等等。通过计算机网络(互联网、内联网等等)下载程序也是可能的。

[0036] 本发明的另外的优点和构型从说明书和附图中得出。

[0037] 应理解,前面提到以及随后还要阐述的特征不仅能够以分别说明的组合而且能够以其它组合或单独地被使用,而不离开本发明的范围。

[0038] 在附图中根据实施例示意性地示出了本发明并且下面参照附图详细地描述本发明。

附图说明

[0039] 图 1 示意性地示出根据本发明的控制设备的优选构型。

[0040] 图 2 作为时间-优先级图示意性地示出根据本发明的方法的优选实施方式。

[0041] 图 3 作为时间-优先级图示意性地示出根据本发明的方法的优选实施方式。

具体实施方式

[0042] 在图 1 中示意性地示出根据本发明的控制设备的优选构型并且用 150 标记。该控制设备 150 例如被构造为机动车的发动机控制设备,该发动机控制设备被设置用于执行机动车的内燃机的发动机控制。

[0043] 控制设备 150 具有片上系统(SoC) 100。该 SoC 100 包括处理器单元 110 和安全处理器单元 120。

[0044] 处理器单元 110 包括具有三个处理器内核 111、112 和 113 的多核处理器。给每个处理器内核 111、112 或 113 分别分配例如闪速存储器的本地存储器 114、115 或 116。安全处理器单元 120 包括处理器内核 121 和具有 RAM 存储器 122 和 ROM 存储器 123 的本地存储器。

[0045] 替代地,也可以设置安全处理器单元 120 和处理器单元 110 的共同的本地存储器(例如 RAM、EEPROM、闪速)以及管理对该共同的存储器的访问的存储器安全机构(例如存储器保护单元(Memory Protection Unit))。

[0046] 处理器单元 110 和安全处理器单元 120 是两个不相关的单独的处理器单元。安全处理器单元 120 在硬件层面上被屏蔽并且被保护免于操纵和攻击。在安全处理器单元 120 中实施有实时能力的操作系统。处理器单元 110 和安全处理器单元 120 通过总线 117 相互处于通信连接中。

[0047] 在处理器单元 110 的处理器内核 111、112、113 中可以实施不同的应用。在这些应用期间必要时必须创建和 / 或处理用于机动车的操控和运行所需要的安全关键数据、例如专门的操控命令、技术数据、控制或特征值。

[0048] 这些安全关键数据不允许离开控制设备 150 并且不应到达第三方。此外,必须确保实时创建这些安全关键数据中的专门的数据。为了该目的,控制设备 150 被设置用于执行根据本发明的方法的优选实施方式。

[0049] 在此期间,在处理器单元 110 的处理器内核 111、112、113 中实施的并且应当创建或处理安全关键数据的相应应用指示安全处理器单元 120 实施确定的安全关键过程。所述应用在此给安全关键过程分别分配优先级。安全处理器单元 120 根据相应优先级实施不同的安全关键过程。在这些安全关键过程期间在安全处理器单元 120 中创建或处理相应的安全关键的数据。

[0050] 下面根据图 2 和 3 描述根据本发明的方法的一种优选实施方式。在图 2 和 3 中分别示意性地示出了时间 - 优先级图。在纵坐标上分别绘出了可以被分配给不同的安全关键过程的优先级“P”。在横坐标上分别绘出了时间“t”。具有所分配的优先级的在安全处理器单元 120 中在确定的时间点之间实施的安全关键过程在时间 - 优先级图中作为条示出。

[0051] 下面根据图 2 描述根据本发明的方法的优选实施方式的第一示例。

[0052] 在第一时间点 t₁,在处理器内核 111 中实施的第一应用指示安全处理器单元 120 实施第一安全关键过程 210。在该第一安全关键过程 210 期间应当执行对消息的验证或对消息的认证码的检验,所述消息由机动车的另一控制设备发送到发动机控制设备 150。该第一过程 210 不应被实时地执行。所述第一应用给该第一过程 210 分配例如“5”的中间的第一优先级。

[0053] 安全处理器单元 120 在第一时间点 t₁ 开始实施该第一过程 210。在第二时间点

t2——在该时间点第一过程 210 的实施还未结束——在处理器内核 112 中实施的第二应用指示安全处理器单元 120 实施第二安全关键过程 220。

[0054] 在该第二安全关键过程 220 期间,应当针对内燃机确定燃料喷射量和燃料-空气混合物的组成。该第二过程 220 是对于机动车的无错误运行来说非常重要的相关过程。该第二过程 220 应当实时地实施。第二应用给该第二过程 220 分配比较高的第二优先级,例如“10”。

[0055] 由于该第二优先级比第一优先级更高,安全处理器单元 120 在时间点 t2 中断第一过程 210 的实施并且取而代之实施第二过程 220。第一过程 210 的进展由安全处理器单元 120 存储。

[0056] 在第三时间点 t3,第二过程 220 的实施结束。在该第三时间点 t3,安全处理器单元 120 在时间点 t2 的进展的情况下继续第一过程 210 的实施。在第四时间点 t4,第一过程 210 的实施结束。

[0057] 下面根据图 3 描述根据本发明的方法的优选实施方式的第二示例。

[0058] 在第五时间点 t5,在处理器内核 111 中实施的第三应用指示安全处理器单元 120 执行第三安全关键过程 230。在该第三安全关键过程 230 期间应当执行对芯片调谐的检验,即检验控制设备 150 的控制参数是否被改变了以便造成功率提高。该检验不应实时地被执行。所述第三应用给该第三过程 230 分配比较低的第三优先级,例如优先级“1”。

[0059] 安全处理器单元 120 在第五时间点 t5 开始实施第三过程 230。在第六时间点 t6——在该时间点第三过程 230 的实施还未结束——第二应用重新指示安全处理器单元 120 实施第二安全关键过程 220,以便重新针对内燃机确定燃料喷射量和燃料-空气混合物的组成。第二应用给第二过程 220 重新分配例如“10”的高的第二优先级。

[0060] 由于第二优先级比第三优先级更高,安全处理器单元 120 在所述第六时间点 t6 中断第三过程 230 的实施并且取而代之实施第二过程 220。第三过程 230 的进展由安全处理器单元 120 存储。

[0061] 在第七时间点 t7,第一应用指示安全处理器单元 120 实施第四安全关键过程 240。在该第四安全关键过程 240 期间数据应当被加密并且配备认证码,所述数据应当被传送到机动车的另一控制设备。该第四过程 240 不应实时地被执行。第一应用给该第四过程 240 分配例如“5”的第四优先级。

[0062] 由于该第四优先级比第二优先级更低,安全处理器单元 120 在所述时间点 t7 不中断第二过程 220 的实施。

[0063] 在第八时间点 t8,第二过程 220 的实施结束。由于第四优先级比第三过程 230 的第三优先级更高,安全处理器单元 120 在时间点 t8 不继续第三过程 230 的实施,而是取而代之开始第四过程 240 的实施。

[0064] 在第九时间点 t9,第四过程 240 的实施结束。在所述第九时间点 t9 安全处理器单元 120 在时间点 t6 的进展的情况下继续第三过程 230 的实施。在第十时间点 t10,第三过程 230 的实施结束。

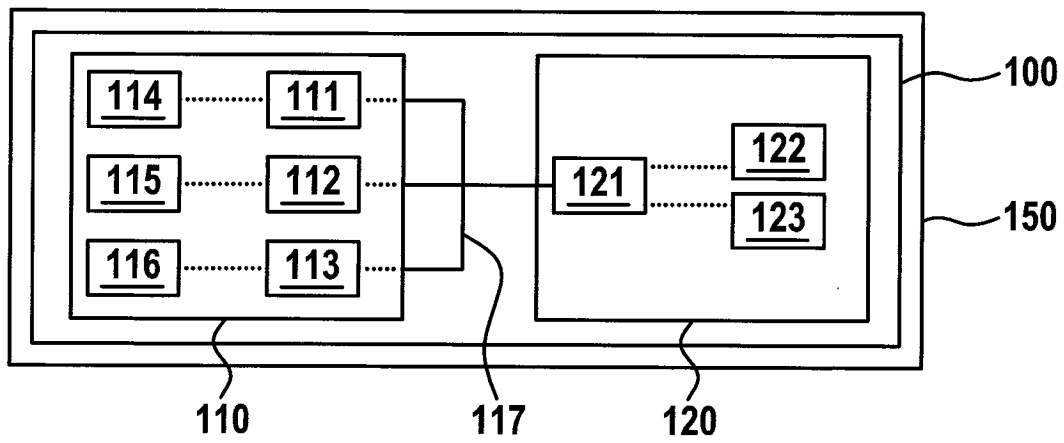


图 1

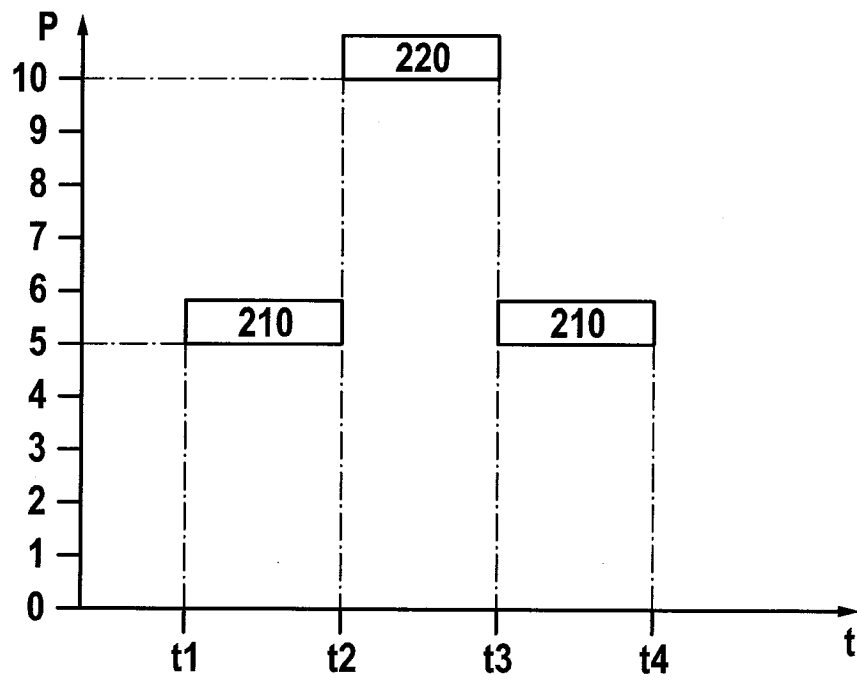


图 2

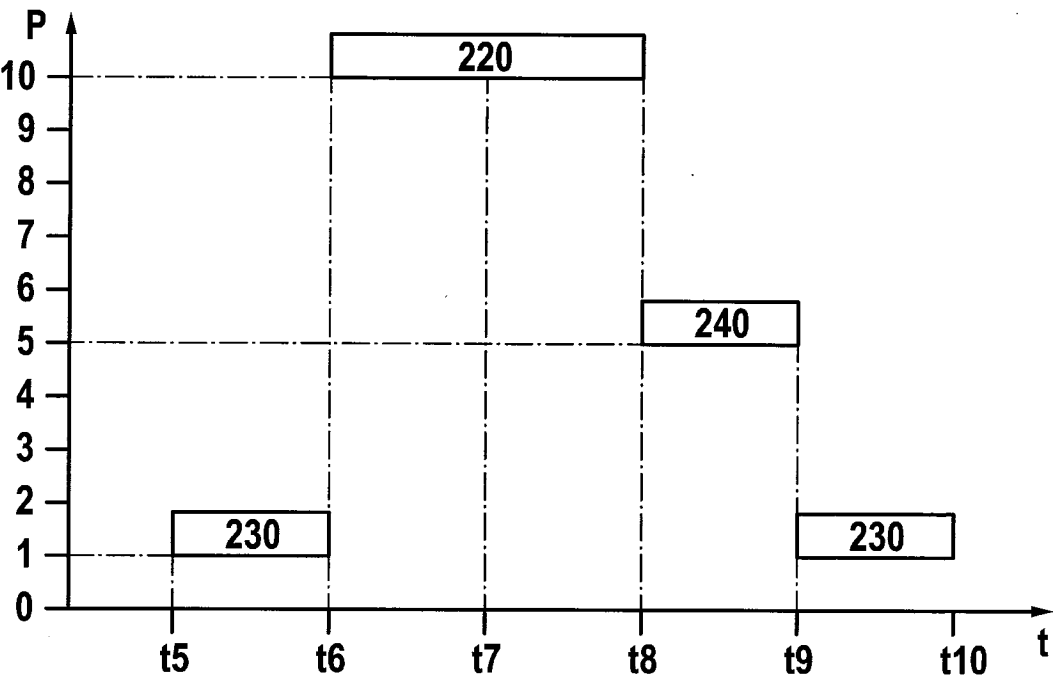


图 3