



(12) 发明专利申请

(10) 申请公布号 CN 115380261 A

(43) 申请公布日 2022. 11. 22

(21) 申请号 202180030037.7

(22) 申请日 2021.04.12

(30) 优先权数据

102020205146.1 2020.04.23 DE

(85) PCT国际申请进入国家阶段日

2022.10.21

(86) PCT国际申请的申请数据

PCT/EP2021/059371 2021.04.12

(87) PCT国际申请的公布数据

W02021/213821 DE 2021.10.28

(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 A·奥厄 F·诺滕斯坦纳

M·施赖伯 A·默克尔

J·帕莱巴斯

(74) 专利代理机构 中国专利代理(香港)有限公司
72001

专利代理师 张涛 刘春元

(51) Int.Cl.

G06F 1/24 (2006.01)

G06F 11/07 (2006.01)

G06F 11/14 (2006.01)

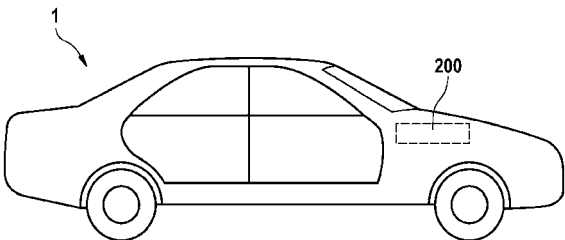
权利要求书2页 说明书21页 附图3页

(54) 发明名称

用于控制技术系统的设备和方法

(57) 摘要

用于控制技术系统、特别是机动车辆的方法。



1. 一种用于控制技术系统(1)的方法,所述技术系统特别是机动车辆或用于机动车辆,所述方法包括:将设备(200)的至少一个硬件组件(202a)复位,其中a)所述设备(200)具有多个计算核心(202a、202b、202c),并且其中所述复位包括将所述多个计算核心(202a、202b、202c)中的单个计算核心(202a)复位(100),特别是按照以下方式,即所述单个计算核心(202a)的复位(100)不影响所述设备(200)的一个或多个另外的计算核心(202b、202c),和/或b)所述设备(200)的模块(202a、202b、202c、206)和/或可能存在的、特别是外部的电路(208)的复位(102)按照以下方式执行,即多个独立的应用(APP1、APP2、APP3)能够运行并且这些应用优选不相互影响。

2. 一种用于控制技术系统(1)、特别是机动车辆的方法,其中所述方法特别是根据权利要求1构造,所述方法包括:将至少一个存储区域(SB1),特别是非易失性存储器(204b)的至少一个存储区域(SB1)分配(110)给一个应用(APP1)或多个应用,特别是将所述非易失性存储器(204b)的第一存储区域(SB1)分配(110)给第一应用或所述第一应用(APP1)并且将所述非易失性存储器(204b)的第二存储区域(SB2)分配(112)给第二应用(APP2)。

3. 一种用于控制技术系统(1)、特别是机动车辆的方法,其中所述方法特别是根据前述权利要求中的至少一项构造,所述方法包括:使用(115)用于收集和管理错误的设备(201),即错误收集和控制单元FCCU(201),其中特别是所述FCCU(201)被构造为保证所述设备(200)或计算装置(202)的应用(APP1、APP2、APP3)的独立(继续)运行,其中特别是所述FCCU(201)收集(116)出现在各个模块(202a、202b、202c、204a、204b、206、208)中的硬件错误并且特别是执行错误反应(117)。

4. 一种用于控制技术系统(1)、特别是机动车辆的方法,其中所述方法特别是根据前述权利要求中的至少一项构造,所述方法包括:将表征应用(APP1)的运行状态的信息(I1-FUSI),特别是表征关于功能安全的运行状态的信息(I1-FUSI)转发(120)到至少一个另外的单元,例如外部单元,特别是布置在所述计算装置(202)或所述设备(200)外部的单元。

5. 一种用于控制技术系统(1)、特别是机动车辆的方法,其中所述方法特别是根据前述权利要求中的至少一项构造,所述方法包括:将至少一个外围模块(208)分配(125)给至少一个、特别是恰好一个应用(APP1)。

6. 一种用于控制技术系统(1)、特别是机动车辆的方法,其中所述方法特别是根据前述权利要求中的至少一项构造,所述方法包括:使用(130)服务质量QoS(Quality of Service)和/或表征所述服务质量的至少一个变量来至少暂时地将分区或应用彼此分开,其中至少一个应用(APP1)为至少一个外围组件(208)设置(132)服务质量,所述服务质量例如能够通过等待时间和/或带宽表征。

7. 一种用于控制技术系统(1)、特别是机动车辆的方法,其中所述方法特别是根据前述权利要求中的至少一项构造,所述方法包括:使用(135)借助于至少一个存储器保护装置MPU(203)的存储区域分配,以特别是保护在一个计算装置或所述计算装置(202)或所述设备(200)上运行的多个应用(APP1、APP2、APP3)之间的确定性数据交换。

8. 一种用于控制技术系统(1)、特别是机动车辆的方法,其中所述方法特别是根据前述权利要求中的至少一项构造,所述方法包括:使用(140)至少一个硬件加速器单元(HSM)来加速所述设备(200)的启动。

9. 一种用于控制技术系统(1)、特别是机动车辆的方法,其中所述方法特别是根据前述

权利要求中的至少一项构造,所述方法包括:使用(150)特别是在至少一个硬件模块或外围组件(208)中实现的机制,借助于所述机制能够由多个分区或应用(APP1、APP2)下达任务,所述任务特别是分别不能被其他分区或应用覆盖或影响。

10.一种用于控制技术系统(1)、特别是机动车辆(1)的设备(200),其中所述设备(200)被构造为执行根据前述权利要求中至少一项所述的方法。

11.一种计算机可读存储介质(SM),包括指令(PRG),所述指令在由计算机(202)执行时促使所述计算机执行根据权利要求1至9中至少一项所述的方法。

12.一种计算机程序(PRG),包括指令,当所述程序(PRG)由计算机(202)执行时,所述指令促使所述计算机执行根据权利要求1至9中至少一项所述的方法。

13.一种数据载体信号(DCS),其传输和/或表征根据权利要求12所述的计算机程序(PRG)。

14.根据权利要求1至9中至少一项所述的方法和/或根据权利要求10所述的设备(200)和/或根据权利要求11所述的计算机可读存储介质(SM)和/或根据权利要求12所述的计算机程序(PRG)和/或根据权利要求13所述的数据载体信号(DCS)用于以下元素中的至少一个的用途:a)实现所述设备(200)的至少一些应用(APP1、APP2、APP3)、优选所有应用的确定性运行时行为,b)避免对第一应用(APP1)的新认证,特别是在改变至少一个另外的应用(APP2)时。

用于控制技术系统的设备和方法

背景技术

[0001] 存在控制技术系统(例如车辆)的子功能的控制设备。这些控制设备分别控制特定的子功能和/或相关联的应用。

发明内容

[0002] 优选实施方式涉及一种用于控制诸如车辆的技术系统的设备。

[0003] 在进一步的优选实施方式中规定,所述设备具有:具有至少一个计算核心的计算装置(“计算机”),分配给所述计算装置的存储装置,所述存储装置用于至少临时存储以下元素中的至少一个:a)数据,b)计算机程序,特别是用于执行根据实施方式的方法。在进一步的优选实施方式中,所述计算机程序还可以表征在所述计算装置上执行的至少一个应用,例如用于控制所述技术系统。

[0004] 在进一步的优选实施方式中,所述设备或所述计算装置具有多个计算核心。

[0005] 在进一步的优选实施方式中,所述存储装置具有易失性存储器(例如工作(RAM))和/或非易失性存储器(例如闪存EEPROM)。

[0006] 在进一步的优选实施方式中,所述计算装置具有以下元件中的至少一个:微处理器(μ R)、微控制器(μ C)、专用集成电路(ASIC)、片上系统(SoC)、可编程逻辑模块(例如FPGA,现场可编程门阵列)、硬件电路或其任意组合。

[0007] 进一步的优选实施方式涉及一种包括指令的计算机可读存储介质,所述指令在由计算机执行时促使所述计算机执行根据实施方式的方法。

[0008] 进一步的优选实施方式涉及一种包括指令的计算机程序,当该程序由计算机执行时,所述指令促使所述计算机执行根据实施方式的方法。

[0009] 进一步的优选实施方式涉及一种数据载体信号,其表征和/或传输根据实施方式的计算机程序。例如可以经由所述设备的可选数据接口接收所述数据载体信号。

[0010] 进一步的优选实施方式涉及至少一个硬件组件的复位(“reset”),特别是针对至少一个应用。

[0011] 在进一步的优选实施方式中,所述设备的模块和/或可能存在的、特别是外部的电路的复位被实施为,使得可以运行多个独立的应用并且这些应用优选地不相互影响。

[0012] 在进一步的优选实施方式中,所述设备被构造为对每个计算核心单独地复位。特别地,因此一个计算核心的复位不会影响所述计算装置中可能存在的另外的计算核心。

[0013] 在进一步的优选实施方式中,可以设置多个区域或集群,所述区域或集群的特征例如在于至少一个计算核心和可选地与所述至少一个计算核心相关联的存储器。在进一步的优选实施方式中,将所述存储器分配给所述至少一个计算核心可以是逻辑的和/或物理的。在进一步的优选实施方式中,至少一个集群可以独立于另外的集群的运行而被复位,特别是不会损害所述另外的集群的运行。由此在进一步的优选实施方式中,例如可以对至少一个集群复位,而可能存在的另外的集群可以独立于所述一个集群的复位而继续运行,以例如执行一个或多个应用。

[0014] 在进一步的优选实施方式中,至少一个集群也可以具有至少一个电路组件或电路部分,例如锁相环(PLL,phased locked loop)。在进一步的优选实施方式中,当至少一个集群复位时,所述至少一个电路组件也可以一起复位。

[0015] 在进一步的优选实施方式中,可能存在的可以例如分配给各个应用的外围模块可以在监督器模式下和/或至少一个应用中复位。

[0016] 在进一步的优选实施方式中,可选地存在的外部组件,例如外部逻辑,可以经由至少一个单独的数据线路,例如单独的GPIO(general purpose input output,通用输入输出)来复位,其中根据进一步的优选实施方式,所述复位例如由监督器模式或由应用执行。在进一步的优选实施方式中,为此可以将GPIO(信号)例如作为复位信号传导至外部组件(例如外部器件或电路)的复位输入端。

[0017] 在进一步的优选实施方式中,可以为可能存在的外部组件或电路提供多个复位连接端(“管脚”),从而例如可以单独复位属于每个应用的外部电路。

[0018] 在进一步的优选实施方式中,所述复位可以通过以下提到的来源中的至少一个来执行,所述来源特别是彼此独立的:a)信号,特别是硬件信号,其例如由监督器和/或监视逻辑触发,b)通过一个比特,所述比特在被写入时执行复位功能,c)通过让软件(特别是应用)设置比特以对应于复位状态。

[0019] 在进一步的优选实施方式中,仍然可以在上述变体c)中以有针对性的方式保持特定功能。作为根据进一步优选实施方式的示例,提到了计时器模块(“计时器”),其例如输出经过脉宽调制(PWM)的信号并且不应当被中断,特别是也不应当通过所述复位被中断。在此情况下,根据进一步的优选实施方式可以将计时器的其他实例或参数特别是在同一模块中经由寄存器设置(写入或设置比特)带入例如对应于复位值(“重新初始化”)的状态,所述模块根据进一步的优选实施方式也可以通过硬件复位。

[0020] 在进一步的优选实施方式中,根据进一步的优选实施方式,利用上述示例性讲述的电路功能既可以由监督器又可以由至少一个应用本身复位所述应用的运行所必需的组件或电路部分,特别是独立于其他应用的状态和/或运行(所述其他应用可以处于复位、启动、减速或正常功能)。

[0021] 进一步的优选实施方式涉及一种用于复位用于控制技术系统、特别是机动车辆的设备的方法,所述设备例如是控制设备,其中所述复位在所述设备或所述技术系统的持续运行期间(例如在多个不同的可能运行状态之一中)执行。

[0022] 在进一步的优选实施方式中,多个应用,特别是彼此独立的或至少部分相关的应用,同时或至少时间重叠地在所述设备上运行。

[0023] 在进一步的优选实施方式中,可选地设置的另外的组件或电路,特别是外部组件或电路,可以分配给至少一个应用,所述至少一个应用至少临时由所述设备或其计算装置或所述计算装置的至少一个计算核心执行。

[0024] 在进一步的优选实施方式中,将所述组件分配给所述至少一个应用也可以动态地执行,即在所述设备或所述应用的运行时期间执行。

[0025] 在进一步的优选实施方式中,可选地设置的另外的组件或电路可以复位,特别是分开地由监督器和/或至少一个应用复位,特别是不影响所述设备的至少一个、优选多个、特别是所有另外的应用的运行时行为。

[0026] 在进一步的优选实施方式中,所述运行时行为的特征在于保持相同的执行时间,特别是关于带宽和/或关于等待时间边界条件,其中在进一步的优选实施方式中不需要时钟精确相同的行为。

[0027] 在进一步的优选实施方式中,当所述设备的至少一个其他应用对分配给其的模块和/或电路部分复位时,所述设备的另外的应用继续运行。

[0028] 进一步的优选实施方式涉及所述存储装置的存储区域的行为,特别是涉及所述存储装置的非易失性存储区域(“NVM(non-volatile memory,非易失性存储器)存储区域”)的行为,其中特别是非易失性存储区域的特别是一个或多个非易失性存储区域可以分别分配给一个应用或多个应用。

[0029] 在进一步的优选实施方式中规定,至少一个NVM存储区域可以分配给至少一个应用。

[0030] 在进一步的优选实施方式中,所述NVM存储区域被布置为,使得其例如可以a)经由MPU(memory protection unit,存储器保护单元)和/或b)经由监督器、特别是通过分配分区ID分配给所述至少一个应用。

[0031] 在进一步的优选实施方式中,所述设备或所述计算装置具有三个计算核心(“核心”),其中例如在每个核心上执行应用,并且其中例如向每个应用分配可预给定的存储区域,例如4兆字节(MB)。

[0032] 在进一步的优选实施方式中,在所述存储装置中设置多个存储模块,特别是为所述NVM存储区域,其中优选地至少两个、优选地多于两个、更优选地所有存储模块被实施为使得它们要么完整地构建,要么由较小的子模块构建或组成。

[0033] 在进一步的优选实施方式中,所述子模块具有与要分配的存储模块至少部分相同的特性,例如关于共同的字线操控器和/或共同的位线读出电路和/或共同的编程电压输送器。

[0034] 在进一步的优选实施方式中,所述设备或所述计算装置被构造为独立于其他存储区域或模块或子模块的状态来执行分配的存储区域或模块或子模块的重新编程,其中特别是为此所需的资源在每个存储区域中例如多重存在。因此在进一步的优选实施方式中,可以对第一(存储)区域进行重新编程,而从其他(存储)区域来看应用继续运行,就好像一个应用或分配给它的存储区域没有被重新编程一样。

[0035] 在进一步的优选实施方式中,一个应用或分配给它的存储区域的重新编程可以从监督器和/或分区管理器和/或应用进行。

[0036] 在进一步的优选实施方式中,特别是通过提供上述资源,该方法还可以在(特别是相对于所述计算装置或设备的)外部存储器中执行,所述外部存储器特别是NVM存储器,其例如具有多个块并且例如可以具有用于这些块的单独的字线操控器和/或用于这些块的单独的位线读出电路。在进一步的优选实施方式中,所述NVM存储器可以构造为LPDDR(low power double data rate,低功率双倍数据速率)存储器类型。

[0037] 进一步的优选实施方式涉及一种用于对设备或所述设备的或用于所述设备的存储装置进行编程(和/或重新编程)的方法,其中所述设备例如被构造为控制诸如机动车辆的技术系统,其特征至少在于以下方面:

a)所述方法例如在机动车辆中,在持续运行期间(例如在机动车辆的各种运行状

态之一中)执行,

b) 在所述设备或控制器上或借助所述设备或控制器,多个独立的或相关的应用同时运行或至少部分时间重叠地运行,

c) 在所述计算装置内部和/或外部的不同存储区域可以分配给应用,特别是灵活和/或动态地,

d) 在所述计算装置内部和/或外部的不同存储区域可以特别是单独地或彼此独立地由监督器和/或至少一个(特别是分配的)应用重新编程,特别是不影响所述设备或计算装置的至少一个其他应用或多个或所有其他应用的运行时行为(所述运行时行为的特征在于例如保持相同的执行时间(特别是关于可预给定的带宽和/或可预给定的等待时间边界条件),其中根据进一步的优选实施方式,特别是不需要时钟精确相同的行为,

e) 当对一个或多个应用重新编程时,所述设备或计算装置的至少一个其他应用,优选所有其他应用继续工作。

[0038] 进一步的优选实施方式涉及错误收集和控制单元FCCU,即涉及用于收集和管理错误的装置,特别是涉及FCCU的资源的划分。

[0039] 在进一步的优选实施方式中规定,所述FCCU被构造为保证所述设备或计算装置的应用的独立(继续)运行,由此实现例如功能上确定性分离的反应(特别是与功能安全相关,“Safety”),例如对硬件错误的反应。换言之,由此在进一步的优选实施方式中使得例如不受硬件错误涉及的应用可以继续执行。

[0040] 在进一步的优选实施方式中,所述FCCU被构造为收集在诸如核心、RAM(工作存储器)、NVM(非易失性存储器)和/或外围模块的各个模块中的硬件错误(“HW错误”),并且例如执行例如可以借助于安全设置(与功能安全相关方面的设置或配置)设置或预给定的错误反应,例如激活一个或多个错误引脚(错误连接端)、触发中断(中断请求)、触发复位或激活NMI(不可屏蔽的中断请求)。

[0041] 在进一步的优选实施方式中,将错误输入信号分配给一个或多个应用,其中特别是还可能生成错误反应(参见例如上述示例性描述的实施方式)或输出到分区和/或应用和/或分配的引脚。

[0042] 在进一步的优选实施方式中,所述设备或所述计算装置具有三个计算核心(“核心”),其中例如在每个核心上至少暂时执行一个应用,并且其中向每个应用例如至少暂时分配可预给定的存储区域,例如4兆字节(MB)。

[0043] 例如,一旦在三个计算核心中的其上例如运行第一应用(“应用1”)的第一计算核心(“核心1”)中识别出错误,则例如可以将核心1中的锁步错误报告给FCCU。在进一步的优选实施方式中,FCCU被配置为使得所述错误可以优选地仅作用于分配给应用1的动作——例如核心1的GIC((通用)中断控制器)中的中断资源、核心1的复位、核心1的NMI或一个或多个错误引脚。在进一步的优选实施方式中,可以在安全系统设置中——例如通过监督器或应用1——设定,该错误例如触发核心1的复位,或者当出现该错误时应当触发核心1的复位。在进一步的优选实施方式中,其他应用(例如“应用2”和“应用3”)不受核心1中的锁步错误的影响,并且优选地继续以相同的时间行为运行。

[0044] 根据进一步的优选实施方式,例如在三个计算核心中的分配给第三应用(“应用3”)的第三计算核心(“核心3”)中可能识别出错误,例如在分配给应用3的NVM存储区域中不

可纠正的“双比特”错误。FCCU优选地被配置为使得所述错误,特别是仅转发到分配给应用3的动作。更优选地,可以触发对应用3的中断请求(中断),例如由FCCU触发,以例如调用用于双比特错误的错误处理例程。在进一步的优选实施方式中,所述错误处理例程可以例如包含附加测试,以例如确定由所述错误引起的安全影响的严重性并且可选地让应用3相应地继续运行或例如复位(reset)应用3,或还通知其他应用(例如经由监督器)——例如借助于中断——所述其他应用可能会受到影响(也受错误影响),并且例如应当对分配给应用1和2的NVM存储器进行对应的检查。

[0045] 进一步的优选实施方式涉及一种用于对技术系统(例如对机动车辆)的设备(例如控制器)中的应用进行错误处理的方法,其特征在于至少一个以下方面:

a) 所述方法例如在机动车辆中,在持续运行期间(例如在机动车辆的各种运行状态之一中)执行,

b) 在所述设备或控制器上或借助于所述设备或控制器,多个独立的或相关的应用同时运行或至少部分时间重叠地运行,

c) 例如可能在所述计算装置(的外部NVM或RAM)内部和/或外部出现的不同错误或错误事件(例如RAM、核心、NVM.....)可以分别分配给至少一个应用,

d) 至少一个、优选多个、特别是所有应用可以至少在其资源内评估错误或所述错误和/或启动对应的错误反应和/或通知至少一个其他应用例如可能的安全错误,特别是在分配给所述应用的资源内,

e) 至少一个、优选多个、特别是所有应用可以由至少一个其他应用通知错误或所述错误,

f) 其他应用,特别是不受错误或所述错误影响的应用,可以继续运行,特别是继续按照以下方式运行,即保持运行时行为,特别是等待时间边界条件,其中特别是不需要时钟精确相同的行为。

[0046] 进一步的优选实施方式涉及将表征应用的运行状态的信息,特别是表征关于功能安全(“安全”)的运行状态(“安全状态”)的信息转发到至少一个另外的单元,例如外部单元,特别是布置在所述计算装置或设备外部的单元。

[0047] 在进一步的优选实施方式中规定,特别是为了保证关于对硬件错误的功能确定性分离的安全反应,未涉及的(一个或多个)应用以及必要时可选地连接到所述应用的(一个或多个)外部单元(例如,驱动器的操控,例如用于承载安全负载以及例如承担将所述计算装置的连接端(“计算机引脚”)转换为例如物理总线协议的信号的PHY,或组件的操控,如内燃机中的点火/喷射)能独立继续运行,分配给所述应用的(相对于所述计算装置的)外部电路发信号通知例如安全状态“错误”(在进一步的优选实施方式中也可以是“复位”,而且附加于复位地),以特别是不影响分配给未涉及的应用的电路部分。

[0048] 在进一步的优选实施方式中,示例性地设置三个计算核心(3个核心),具有3个应用,其中在每个核心上运行三个应用之一。此外,例如设置三个错误引脚(连接端,例如用于发信号通知错误状态)。在进一步的优选实施方式中,示例性地设置了用于VCU(vehicle control unit,车辆控制单元)(例如核心1上的应用1)的外部接口和用于燃烧应用(例如核心3上的应用3)的喷射的外部接口。

[0049] 在进一步的优选实施方式中,燃烧应用例如想要关闭喷射,以降低发动机的扭矩。

为此例如激活错误引脚3(其例如在启动期间(即所述设备启动时)已分配给应用3),该错误引脚优选连接到(外部)喷射电路(IC),使得该喷射电路特别是与预给定喷射定时的脉冲无关地关闭并且例如不操控喷射阀。在其他优选实施例中,VCU功能同时继续在核心1上的应用1上继续运行——该VCU例如还经由CAN驱动器传输带有安全负载的信号。在进一步的优选实施方式中,不激活错误引脚1(例如,在启动期间分配给应用1),从而来自所述计算装置或所述设备的CAN信号经由当前未停用(用错误引脚1停用)的CAN驱动器转发。由此,核心1上的VCU应用不受应用3的错误影响(继续),并且特别是继续传输所述CAN信号。

[0050] 进一步的优选实施方式涉及一种用于向所述计算装置或所述设备外部的单元或器件发信号通知、特别是转发至少一个应用的安全状态的方法,其特征在于至少一个以下方面:

a) 安全状态的发信号通知可以优选地用作关闭信号,例如针对外部器件(“外围模块”),

b) 可以将所述发信号通知分配给例如在所述计算装置上并行运行的各个应用,其中特别是可以将分配给一个应用的外围模块与其他应用的状态或所述其他应用的外围模块的状态无关地复位,

c) 可以在复位之后进行分配,优选不可更改地,

d) 这些实施方式的方面也可以用于外部安全器件,例如外部密码器件(密码加速器、硬件安全模块)、接口,

e) 既与功能安全方面(“FUST”,“安全(Safety)”)相关又与安全方面相关的用途,例如防止操纵(“保安(Security)”)。

[0051] 进一步的优选实施方式涉及一种用于控制诸如车辆的技术系统的方法,其中将至少一个外围模块分配给至少一个应用。所述应用可以优选地分别在所述计算装置上的分开的分区中运行。

[0052] 在进一步的优选实施方式中,所述至少一个外围模块例如是以下元件中的至少一个:计时器(计时器模块)、通信接口、GPIO端口(通用输入和/或输出连接端)。

[0053] 由此可以优选地实现:多个应用在所述计算装置上运行时不会相互影响。

[0054] 根据进一步的优选实施方式可以避免的不期望的相互影响的示例是:

1. 模拟/数字转换器(ADC)的运行:如果多个应用访问ADC的资源(例如通道/输入端和/或控制寄存器),则一个应用例如可能覆盖另一个应用的设置,例如通道分配、采样时间(采样率)、转换时间、.....

2. CAN(控制器局域网):如果在多个应用中使用同一CAN总线上的CAN标识符,则可以在CAN模块中例如进行队列条目,其中一个分区(即,例如一个应用)的软件可以覆盖另一个应用的设置。

[0055] 在进一步的优选实施方式中规定,至少一个外围模块可以优选完全地分配给一个分区或应用。

[0056] 在进一步的优选实施方式中,在所述设备或计算装置中设置例如模块,例如SPI(串行外围接口)、LIN(本地互连网络)、CAN、ADC,所述模块例如可以优选地完全分配给一个应用,特别是因为这些模块的资源要么完全被所述分区或应用使用,要么这些模块多次存在,特别是频繁存在,以至于对应的各个模块可以完全分配给一个分区或应用。

[0057] 在进一步的优选实施方式中,提出了以下机制,以特别是根据确定性功能的目标来分离这些模块:

- 将至少一个、优选多个或所有模块分配给一个分区或应用(特别是在所述模块中),其中特别是该模块仅从总线(例如用于将该模块连接到所述计算装置或设备的(一个或多个)组件的数据总线)接受带有可预给定标识符(例如“分区ID”)的写入命令和/或读取命令,所述可预给定标识符例如是事先在系统设置时由分区管理器分配给该模块的。

[0058] 因此在进一步的优选实施方式中,模块、优选完整的模块特别是固定地(即静态地)分配给分区,特别是分配给一个分区或应用。

[0059] 在进一步的优选实施方式中可以规定,可以将(外围)模块分配给多个应用,例如可通过至少一个硬件功能(例如地址区域限制)预给定或控制。

[0060] 在进一步的优选实施方式中,例如在设备或计算装置中存在模块,例如GTM(计时器模块)、以太网、HSM(硬件安全模块)(Windows),所述模块的组件或集群或模块部分可以通过地址区域的内部分配被分配给分区或应用。

[0061] 为了根据进一步的优选实施方式分离这些模块,特别是为了确定性功能的目标,提出以下机制:

- 通过地址区域将模块分配给分区或应用,和/或

- 将资源布置在一个模块中,使得分配给一个分区(或应用)的资源在一个地址区域内彼此靠近(例如相邻地),和/或

- 一个或多个地址区域的分配可以例如从外部通过总线桥和/或通过存储器保护装置(MPU)进行,所述存储器保护装置例如确保了不属于分配的分区或应用的内部(一个或多个)主机/从机无法读取和/或写入到该地址区域。

[0062] 因此在进一步的优选实施方式中,(外围)模块向应用或分区的分配可以通过所述地址区域的限制、优选模块内部的限制进行。

[0063] 在进一步的优选实施方式中,例如还存在可以通过软件(SW)机制彼此分离的模块,其中这些模块例如由多个分区或应用使用。根据进一步优选实施方式的一个示例例如是不使用已实现队列的以太网,根据进一步优选实施方式的另一示例是用于处理器间通信的总线,或CAN模块,其中SW分配、特别是各个ID的SW分配是有意义的,因为例如在系统中不存在足够多的CAN模块。

[0064] 因此,在进一步的优选实施方式中提出:

- a)通过配置工具配置这些模块,特别是在启动期间,使得考虑使用这些资源的所有分区或应用的边界条件,

- b)例如CAN/以太网:以满足所述要求的方式实现来自请求的带宽和/或等待时间——将消息ID分配到具有对应待给定的优先级的模块队列,

- c)在持续运行期间,通过分区管理器(在分区或应用上运行在权限模式下的SW)来调节对这些资源的写入/读取——这里优选存在调用分区管理器的多个可能性,例如通过调用(Call)或通过陷阱/模拟(其被故意写入到一个被锁定的资源,从而调用更高的权限级别来解决访问冲突),

- d)根据进一步优选实施方式的另一种可能性是通过在持续运行期间设置DMA通道来调节写入和/或读取——然后这些DMA通道例如优选地仅通过特定触发器被激活,并且所

述读取和/或写入然后包括例如只有模块中的特殊资源,例如然后写入/读取来自固定分配给各个分区的地址区域的数据。

[0065] 因此在进一步的优选实施方式中提出:将所述设备或计算装置的资源(例如,外围模块)分配给多个分区或应用,其中使用SW功能和HW功能。

[0066] 进一步的优选实施方式涉及一种用于控制诸如车辆的技术系统的方法,其中服务质量(QoS, Quality of Service)或至少一个表征服务质量的变量用于至少暂时地将分区或应用彼此分开,即分离。

[0067] 根据进一步的优选实施方式,在多个应用可以同时运行的设备或系统中,特别是为了实现所述应用的相同运行时或为了实现可预给定的资源分布(特别是独立于其他应用),有利地也考虑一个或多个总线,所述总线特别是可用于组件之间的数据传输。

[0068] 由于在进一步的优选实施方式中应用的运行时受到多种因素的影响,在进一步的优选实施方式中这些因素也可以单独地或相互结合地得到解决:核心本身(管理程序(Hypervisor)机制)、对存储器的访问(QoS)、访问计算机中的模块,如SPI、安全、.....。

[0069] 根据进一步的优选实施方式提出,可以将用于分离对存储器的访问的机制用于分离对所述(外围)模块的访问,所述机制例如可以在所述设备或计算装置的总线系统或总线架构中设置。

[0070] 在进一步的优选实施方式中,至少一个应用,优选多个或所有应用,为至少一个外围组件或至少一个外围模块设置服务质量(“QoS”),所述服务质量例如可通过等待时间和/或带宽来表征。例如:

a) 应用1为涉及外围组件的访问设置15个时钟的等待时间和20%的总线带宽,

b) 应用2为对同一外设组件的访问设置40个时钟的等待时间和70%的总线带宽。

[0071] 换言之,在进一步的优选实施方式中,QoS或QoS机制(例如借助于硬件实现)的使用可以用于控制各个应用的带宽和/或等待时间,特别是用于将外围设备访问(应用对外围模块而不是对存储器的访问)分开,其中特别是还可以用于将应用确定性地分开和减少在一个设备或计算装置中(例如在一个控制设备中)实现多个应用情况下的耗费。

[0072] 在进一步的优选实施方式中提出,使用至少一个计数器来模拟服务质量(QoS),根据进一步的优选实施方式,这特别是在不能借助于硬件实现QoS时特别有用。

[0073] 在进一步的优选实施方式中提出,模拟一个或多个QoS机制,例如借助于以下元素中的至少一个:a)实现针对等待时间和/或带宽的计数器,b)由软件在高优先级(例如,高于应用)评估这些计数器。根据进一步优选实施方式的一种可能实现例如规定:对每个总线实现 $x*2$ 个寄存器(例如32比特宽)作为计数器(Counter),其中 x 表征待支持的分区数量,并且优选地在一个或多个寄存器中对相应分配的应用在每个时钟的访问计数。更优选地,每 z 毫秒(ms)将计数器值与预期计数器值进行比较,并且如果所述计数器值大于所述预期计数器值,则通知应用和例如分区管理器,以特别是启动替代措施。

[0074] 在进一步的优选实施方式中,可以取决于所述设备或控制器的类型或取决于所述设备或控制器的目标系统的类型使用时间同步的网格或角度同步的网格(例如关于内燃机曲轴的一转),特别是用于上面借助于(一个或多个)计数器的示例性描述的QoS模拟。

[0075] 在进一步的优选实施方式中,每在具有(特别是可预给定的)分区ID的总线上施加一个动作就将计数器增加一个可预给定的值,例如一,由此例如可以确定表征带宽的度量。

[0076] 在进一步的优选实施方式中,从(特别是可预给定的)分区对总线的请求(Request)开始对时钟进行计数,直到该分区获得所述总线(准许总线访问)为止。例如,如果经过计数的时钟数量小于可预给定的等待时间,则很好,如果经过计数的时钟的值大于可预给定的等待时间,则这在进一步的优选实施方式中可以得到存储,并且例如在所设置的时间间隔结束时可以读出在所考虑的时间间隔中的所述等待时间是否曾经大于预设时间,以及可选地,如果是则读出大多少。

[0077] 在其他优选实施例中,替代或附加地,借助于硬件和/或触发中断来实现例如预设的自动比较。

[0078] 在进一步的优选实施方式中,可以在所述设备或计算装置的至少一条总线上设置一个或多个计数器。

[0079] 在进一步的优选实施方式中,所述计数器可以与对应的软件(和/或硬件)一起使用,例如用于评估保持的分配的带宽和/或(保持的)等待时间。

[0080] 进一步的优选实施方式涉及一种用于控制诸如车辆的技术系统的方法和设备,其中设置存储器保护装置(MPU),其中所述存储器保护装置特别是用于限制关于所述设备或计算装置的至少一个总线系统的访问权限。

[0081] 根据进一步的优选实施方式,在一个设备或计算装置上运行多个应用的优点是数据交换的短等待时间和该交换的高带宽,由此可以以比传统系统中预给定的更短的时间网格来计算例如调节器,因为来自其他应用的数据相对较快地可用。

[0082] 在进一步的优选实施方式中,为了实现这一点并且特别是为了确保多个应用不会不允许地相互影响,提出将在所述计算装置内或所述计算装置外(例如在总线系统的区域中)的MPU用于限制访问权限。

[0083] 在进一步的优选实施方式中,可以示例性地使用以下流程:设置例如核心外部的MPU,例如在总线接口中,其中设置两个应用,其中每个应用都在一个核心上运行。

[0084] 在进一步的优选实施方式中,MPU可以被配置为,例如在系统启动期间,使得在每个分配给另一个核心的本地存储器中分配用于写入的区域,并且在自己的存储器中释放用于读取的区域。由此例如每个应用都可以读取另一个核心的数据并且通过写入向所述另一个核心本地提供数据,特别是不能覆盖其他(存储)区域。

[0085] 因此在进一步的优选实施方式中提出:一种用于借助于MPU使用存储区域分配以确保在所述计算装置或所述设备上运行的多个应用之间的确定性数据交换的方法。

[0086] 因此在其他优选实施例中提出:一种用于使用至少一个MPU确保不同应用的确定性存储器访问和/或数据交换的方法。在此背景下,“确定性”特别优选地与应用定时(即(一个或多个)应用的时间行为)有关,并且特别是与用于访问相应资源的周期的具体数量无关。

[0087] 进一步的优选实施方式涉及一种用于控制诸如车辆的技术系统的方法和设备,其中使用至少一个硬件加速器单元以加速所述系统的启动(startup)。

[0088] 在现代(特别是汽车)系统中,将设备的现有软件替换为其他软件(“Tuning,调谐”),以例如在应用中有更多功率可用(例如更多功率,PS)。识别并在必要时防止这种情况的一种方法提出,在引导(启动)系统时事先检查软件代码以确定所述软件代码是否是实际应当执行的代码或所述代码是否已被操纵,例如在调谐措施的范围内。

[0089] 根据进一步优选实施方式的用于检查SW代码的方法规定,确定或计算关于可预给定的存储区域或(特别是整个)存储器的至少一个校验和(Checksum)。在此的一个问题可能是确定或计算所述校验和需要相对较长的时间,从而引导过程被延长了。在进一步的优选实施方式中,例如应当在30ms-100ms内完成引导过程。但是,由于校验和计算可能会增加大量的毫秒数。

[0090] 因此,在进一步的优选实施方式中提出设置至少一个硬件加速器单元并将其用于计算(一个或多个)校验和(“HW校验和加速器”)。在进一步的优选实施方式中,还可以设置多个硬件加速器单元,这些硬件加速器单元必要时分别处理待检查的存储器的一部分或为对应部分形成校验和。更优选地,在启动(一个或多个)应用之前借助于所述至少一个硬件加速器单元来计算校验和。

[0091] 在进一步的优选实施方式中,硬件加速器单元也可以分配给不同的分区或应用。

[0092] 进一步的优选实施方式涉及一种用于控制诸如车辆的技术系统的方法和设备,其中在至少一个硬件模块或外围组件中实现机制,优选地在所述模块的接口(Interface)中实现,借助于所述机制可以由多个分区或应用下达任务,这些任务特别是分别不能被其他分区覆盖或影响。在进一步的优选实施方式中,该机制也可以被称为“(一个或多个)传输窗口”。

[0093] 在进一步的优选实施方式中,所述硬件模块(或所述模块的控制器,例如所述模块的微控制器)或所述外围组件被构造为根据预给定规则处理所述任务,例如以轮询(Round Robin)方法,由此有利地对于(外部)应用而言代表了确定性时间行为。

[0094] 进一步的优选实施方式规定了在至少一个硬件模块中实现传输窗口,具有至少一个以下方面:

a) 所述传输窗口的地址区域可以可选地分配给不同的应用/分区,

b) 在所述模块中例如借助于SW按照预给定的方法(例如轮询方法)对任务进行处理。

[0095] 进一步的优选实施方式涉及一种用于执行根据前述权利要求中的至少一项所述的方法的设备,其中所述设备特别是被构造为控制技术系统,特别是机动车辆。

[0096] 在进一步的优选实施方式中规定,所述设备具有:具有至少一个计算核心、优选多个计算核心的计算装置(“计算机”),分配给所述计算装置的存储装置,所述存储装置用于至少临时存储以下元素中的至少一个:a)数据,b)计算机程序,特别是用于执行根据实施方式的方法。

[0097] 在进一步的优选实施方式中,所述存储装置具有易失性存储器(例如工作存储器(RAM))和/或非易失性(NVM)存储器(例如闪存EEPROM)或它们的组合或与未明确提及的其他存储器类型的组合。

[0098] 在进一步的优选实施方式中,所述设备具有至少一个模拟/数字(A/D)转换器,和/或至少一个另外的或其他外围组件,例如计时器模块(计时器)和/或数据接口,所述转换器被构造为将接收到的模拟信号(时间连续和/或数值连续的信号)转换为时间离散和/或数值离散的信号。

[0099] 进一步的优选实施方式涉及一种包括指令的计算机可读存储介质,所述指令在由计算机执行时促使所述计算机执行根据实施方式的方法。

[0100] 进一步的优选实施方式涉及一种包括指令的计算机程序,当该程序由计算机执行时所述指令促使所述计算机执行根据实施方式的方法。

[0101] 进一步的优选实施方式涉及一种数据载体信号,其表征和/或传输根据实施方式的计算机程序。例如可以经由所述设备的一个或可选的数据接口接收所述数据载体信号。

[0102] 进一步的优选实施方式涉及根据实施方式的方法和/或根据实施方式的设备和/或根据实施方式的计算机可读存储介质和/或根据实施方式的计算机程序和/或根据实施方式的数据载体信号用于以下元素中的至少一个的用途:a)实现所述设备的至少一些应用、优选所有应用的确定性运行时行为,b)避免对第一应用的新认证,特别是在改变至少一个另外的应用时。

附图说明

[0103] 本发明进一步的特征、应用可能性和优点由以下对在附图的各图中示出的本发明实施例的描述得出。在此,所有描述或示出的特征单独或以任何组合形成本发明的主题,而不管它们如何在权利要求或其引用中的概括如何,也不管它们在说明书中的措辞或附图中的显示如何。

[0104] 在附图中:

图1示意性地示出了根据优选实施方式的技术系统的简化框图,

图2示意性地示出了根据进一步优选实施方式的设备的简化框图,

图3A示意性地示出了参考根据进一步优选实施方式的方法方面的简化流程图,以及

图3B、图3C、图3D、图3E、图3F、图3G、图3H、图3I分别示意性地示出了参考根据进一步优选实施方式的方法方面的简化流程图。

具体实施方式

[0105] 优选实施方式涉及用于控制技术系统1的方法和/或设备200,所述技术系统例如是车辆1,特别是机动车辆,参见图1。

[0106] 在进一步的优选实施方式中,参见图2,规定设备200具有:具有至少一个(在当前情况下为三个)计算核心202a、202b、202c的计算装置(“计算机”)202,分配给计算装置202的存储装置204,所述存储装置用于至少临时存储以下元素中的至少一个:a)数据DAT,b)计算机程序PRG,特别是用于执行根据实施方式的方法。在进一步的优选实施方式中,计算机程序PRG还可以表征至少临时在计算装置202上执行的至少一个应用APP1、APP2、APP3,例如用于控制技术系统1或其组件(例如制动系统、内燃机)。

[0107] 在进一步的优选实施方式中,设备200或计算装置202具有多个计算核心202a、202b、202c。在进一步的优选实施方式中,多于图1中示例性示出的三个计算核心202a、202b、202c也是可能的。

[0108] 在进一步的优选实施方式中,存储装置204具有易失性存储器204a(例如工作(RAM))和/或非易失性存储器204b(例如闪存EEPROM)。

[0109] 在进一步的优选实施方式中,计算装置202具有以下元件中的至少一个或被构造为这些元件中的至少一个:微处理器(μ R)、微控制器(μ C)、专用集成电路(ASIC)、片上系统

(SoC)、可编程逻辑模块(例如FPGA,现场可编程门阵列)、硬件电路或其任意组合。

[0110] 进一步的优选实施方式涉及一种包括指令PRG的计算机可读存储介质SM,所述指令在由计算机202执行时促使所述计算机执行根据实施方式的方法。

[0111] 进一步的优选实施方式涉及一种包括指令的计算机程序PRG,当该程序由计算机202执行时,所述指令促使所述计算机执行根据实施方式的方法。

[0112] 进一步的优选实施方式涉及一种数据载体信号DCS,其表征和/或传输根据实施方式的计算机程序PRG。例如可以经由设备200的可选数据接口206接收数据载体信号DCS。

[0113] 参见图3A,进一步的优选实施方式涉及至少一个硬件组件的复位100、102(“reset”),特别是针对至少一个应用APP1。

[0114] 在进一步的优选实施方式中,设备200的模块和/或可能存在的、特别是外部的电路208(例如,模拟/数字转换器,ADC)的复位100、102被实施为,使得可以运行多个独立的应用APP1、APP2、APP3并且这些应用优选地不相互影响。

[0115] 在进一步的优选实施方式中,设备200被构造为对每个计算核心202a、202b、202c单独地复位。特别地,因此一个计算核心202a的复位不会影响计算装置202中可能存在的另外的计算核心202b、202c。

[0116] 在进一步的优选实施方式中,可以设置多个区域或集群,所述区域或集群的特征例如在于至少一个计算核心202a和可选地与所述至少一个计算核心相关联的存储器204a。在进一步的优选实施方式中,将所述存储器分配给所述至少一个计算核心可以是逻辑的和/或物理的。在进一步的优选实施方式中,至少一个集群可以独立于另外的集群的运行而被复位,特别是不会损害所述另外的集群的运行。由此在进一步的优选实施方式中,例如可以对至少一个集群复位,而可能存在的另外的集群可以独立于所述一个集群的复位而继续运行,以例如执行一个或多个应用。

[0117] 在进一步的优选实施方式中,至少一个集群也可以具有至少一个电路组件或电路部分,例如锁相环(PLL,phased locked loop)。在进一步的优选实施方式中,当至少一个集群复位时,所述至少一个电路组件也可以一起复位。

[0118] 在进一步的优选实施方式中,可能存在的可以例如分配给各个应用APP1、APP2、APP3的外围模块可以在监督器模式下和/或至少一个应用中复位。

[0119] 在进一步的优选实施方式中,可选地存在的外部组件,例如外部逻辑,可以经由至少一个单独的数据线路,例如单独的GPIO(general purpose input output,通用输入输出)来复位,其中根据进一步的优选实施方式,所述复位例如由监督器模式或由应用APP1、APP2、APP3执行。在进一步的优选实施方式中,为此可以将GPIO(信号)例如作为复位信号传导至外部组件(例如外部器件或电路)的复位输入端。

[0120] 在进一步的优选实施方式中,可以为可能存在的外部组件或电路提供多个复位连接端(“管脚”),从而例如可以单独复位属于每个应用的外部电路。

[0121] 在进一步的优选实施方式中,所述复位可以通过以下提到的来源中的至少一个来执行,所述来源特别是彼此独立的:a)信号,特别是硬件信号,其例如由监督器和/或监视逻辑触发,b)通过一个比特,所述比特在被写入时执行复位功能,c)通过让软件(特别是应用)设置比特以对应于复位状态。

[0122] 在进一步的优选实施方式中,仍然可以在上述变体c)中以有针对性的方式保持特

定功能。作为根据进一步优选实施方式的示例,提到了计时器模块(“计时器”),其例如输出经过脉宽调制(PWM)的信号并且在此不应当被中断,特别是也不应当通过所述复位被中断。在此情况下,根据进一步的优选实施方式可以将计时器的其他实例或参数特别是在同一模块中经由寄存器设置(写入或设置比特)带入例如对应于复位值(“重新初始化”)的状态,所述模块根据进一步的优选实施方式也可以通过硬件复位。

[0123] 在进一步的优选实施方式中,根据进一步的优选实施方式,利用上述示例性讲述的电路功能既可以由监督器又可以由至少一个应用APP1本身复位所述应用的运行所必需的组件或电路部分,特别是独立于其他应用APP2、APP3的状态和/或运行(所述其他应用可以处于复位、启动、减速或正常功能)。

[0124] 进一步的优选实施方式涉及一种用于复位用于控制技术系统1、特别是机动车辆的设备200的方法,设备200例如是控制设备,其中所述复位在设备200或技术系统1的持续运行期间(例如在多个不同的可能运行状态之一中)执行。

[0125] 在进一步的优选实施方式中,多个应用APP1、APP2、APP3,特别是彼此独立的或至少部分相关的应用APP1、APP2、APP3,同时或至少时间重叠地在设备200上运行。

[0126] 在进一步的优选实施方式中,可选地设置的另外的组件208或电路,特别是外部组件或电路,可以分配给至少一个应用APP1,所述至少一个应用APP1至少临时由设备200或其计算装置202或计算装置202的至少一个计算核心202a执行。

[0127] 在进一步的优选实施方式中,将所述组件分配给所述至少一个应用也可以动态地执行,即在所述设备或所述应用的运行时期间执行。

[0128] 在进一步的优选实施方式中,可选地设置的另外的组件或电路可以复位,特别是分开地由监督器和/或至少一个应用复位,特别是不影响所述设备的至少一个、优选多个、特别是所有另外的应用的运行时行为。

[0129] 在进一步的优选实施方式中,所述运行时行为的特征在于保持相同的执行时间,特别是关于带宽和/或关于等待时间边界条件,其中在进一步的优选实施方式中不需要时钟精确相同的行为。

[0130] 在进一步的优选实施方式中,当设备200的至少一个其他应用APP2对分配给其的模块208和/或电路部分复位时,设备200的另外的应用APP3继续运行。

[0131] 参见图3B,进一步的优选实施方式涉及所述存储装置的存储区域的行为,特别是涉及所述存储装置的非易失性存储区域(“NVM(non-volatile memory,非易失性存储器)存储区域”)的行为,其中特别是非易失性存储区域SB1的特别是一个或多个非易失性存储区域分别分配110给或可以分配给一个应用APP1或多个应用。

[0132] 在进一步的优选实施方式中规定,至少一个NVM存储区域SB1可以分配给至少一个、特别是恰好一个应用APP1。

[0133] 在进一步的优选实施方式中,所述NVM存储区域被布置为,使得其可以例如a)经由MPU(memory protection unit,存储器保护单元)和/或b)经由监督器、特别是通过分配分区ID分配给所述至少一个应用。

[0134] 在进一步的优选实施方式中,设备200或计算装置202具有三个计算核心(“核心”)202a、202b、202c,其中例如在每个核心上执行应用,并且其中例如向每个应用分配可预给定的存储区域,例如4兆字节(MB)。例如,将第一存储区域SB1分配给第一应用APP1并且将第

二存储区域SB2分配给第二应用APP1,参见根据图3B的步骤110、112。

[0135] 在进一步的优选实施方式中,在存储装置204中设置多个存储模块,特别是为NVM存储区域204b,其中优选地至少两个、优选地多于两个、更优选地所有存储模块被实施为使得它们要么完整地构建,要么由较小的子模块构建或组成。

[0136] 在进一步的优选实施方式中,这些子模块具有与要分配的存储模块至少部分相同的特性,例如关于共同的字线操控器和/或共同的位线读出电路和/或共同的编程电压输送器。

[0137] 在进一步的优选实施方式中,设备200或计算装置202被构造为独立于其他存储区域或模块或子模块的状态来执行分配的存储区域或模块或子模块的重新编程,其中特别是为此所需的资源在每个存储区域中例如多重存在。因此在进一步的优选实施方式中,可以对第一(存储)区域进行重新编程,而从其他(存储)区域来看应用继续运行,就好像一个应用或分配给它的存储区域没有被重新编程一样。

[0138] 在进一步的优选实施方式中,一个应用或分配给它的存储区域的重新编程可以从监督器和/或分区管理器和/或应用进行。

[0139] 在进一步的优选实施方式中,特别是通过提供上述资源,该方法还可以在(特别是相对于所述计算装置或设备的)外部存储器中执行,所述外部存储器特别是NVM存储器,其例如具有多个块并且例如可以具有用于这些块的单独的字线操控器和/或用于这些块的单独的位线读出电路。在进一步的优选实施方式中,所述NVM存储器可以构造为LPDDR(low power double data rate,低功率双倍数据速率)存储器类型。

[0140] 进一步的优选实施方式涉及一种用于对设备或所述设备的或用于所述设备的存储装置进行编程(和/或重新编程)的方法,其中所述设备例如被构造为控制诸如机动车辆的技术系统,其特征在于至少一个以下方面:

a)所述方法例如在机动车辆中,在持续运行期间(例如在机动车辆的各种运行状态之一中)执行,

b)在所述设备或控制器上或借助于所述设备或控制器,多个独立的或相关的应用同时运行或至少部分时间重叠地运行,

c)在所述计算装置内部和/或外部的不同存储区域可以分配给应用,特别是灵活和/或动态地,

d)在所述计算装置内部和/或外部的不同存储区域可以特别是单独地或彼此独立地由监督器和/或至少一个(特别是分配的)应用重新编程,特别是不影响所述设备或计算装置的至少一个其他应用或多个或所有其他应用的运行时行为(所述运行时行为的特征在于例如保持相同的执行时间(特别是关于可预给定的带宽和/或可预给定的等待时间边界条件),其中根据进一步的优选实施方式,特别是不需要时钟精确相同的行为,

e)当对一个或多个应用重新编程时,所述设备或计算装置的至少一个其他应用,优选所有其他应用继续工作。

[0141] 参见图3C,进一步的优选实施方式涉及错误收集和控制单元FCCU 201(图2),即涉及用于收集和管理错误的装置,特别是涉及FCCU的资源的划分。图3C的步骤115象征着FCCU 201的使用。

[0142] 在进一步的优选实施方式中规定,FCCU被构造为保证所述设备或计算装置的应用

的独立(继续)运行,由此实现例如功能上确定性分离的反应(特别是与功能安全相关,“Safety”),例如对硬件错误的反应。换言之,由此在进一步的优选实施方式中使得例如不受硬件错误涉及的应用可以继续执行。

[0143] 在进一步的优选实施方式中,FCCU被构造为收集116(图3C)在诸如核心、RAM(工作存储器)、NVM(非易失性存储器)和/或外围模块的各个模块中的硬件错误(“HW错误”),并且例如执行117例如可以借助于安全设置(与功能安全相关方面的设置或配置)设置或预给定的错误反应,例如激活一个或多个错误引脚(错误连接端)、触发中断(中断请求)、触发复位或激活NMI(不可屏蔽的中断请求)。

[0144] 在进一步的优选实施方式中,将错误输入信号分配给一个或多个应用,其中特别是还可能生成错误反应(参见例如上述示例性描述的实施方式)或输出到分区和/或应用和/或分配的错误引脚。

[0145] 例如,一旦在三个计算核心中的其上例如运行第一应用APP1(“应用1”)的第一计算核心(“核心1”)202a(图2)中识别出错误,则例如可以将核心1 202a中的锁步错误报告给FCCU 201。在进一步的优选实施方式中,FCCU 201被配置为使得所述错误可以优选地仅作用于分配给应用1的动作——例如核心1 202a的GIC((通用)中断控制器)中的中断资源、核心1的复位、核心1的NMI或一个或多个错误引脚。在进一步的优选实施方式中,可以在安全系统设置中——例如通过监督器或应用1——设定,该错误例如触发核心1的复位,或者当出现该错误时应当触发核心1的复位。在进一步的优选实施方式中,其他应用(例如“应用2”和“应用3”)不受核心1中的锁步错误的影响,并且优选地继续以相同的时间行为运行。

[0146] 根据进一步的优选实施方式,例如在三个计算核心中的分配给第三应用APP3(“应用3”)的第三计算核心202c(“核心3”)中可能识别出错误,例如在分配给应用3的NVM存储区域中不可纠正的“双比特”错误。FCCU 201优选地被配置为使得所述错误,特别是仅转发到分配给应用3的动作。更优选地,可以触发对应用3的中断请求(中断),例如由FCCU触发,以例如调用用于双比特错误的错误处理例程。在进一步的优选实施方式中,所述错误处理例程可以例如包含附加测试,以例如确定由所述错误引起的安全影响的严重性并且可选地让应用3相应地继续运行或例如复位(reset)应用3,或还通知其他应用(例如经由监督器)——例如借助于中断——所述其他应用可能会受到影响(也受错误影响),并且例如应当对分配给应用1和2的NVM存储器进行对应的检查。

[0147] 进一步的优选实施方式涉及一种用于对技术系统(例如对机动车辆)的设备(例如控制器)中的应用进行错误处理的方法,其特征在于至少一个以下方面:

a) 所述方法例如在机动车辆中,在持续运行期间(例如在机动车辆的各种运行状态之一中)执行,

b) 在所述设备或控制器上或借助于所述设备或控制器,多个独立的或相关的应用同时运行或至少部分时间重叠地运行,

c) 例如可能在所述计算装置(的外部NVM或RAM)内部和/或外部出现的不同错误或错误事件(例如RAM、核心、NVM.....)可以分别分配给至少一个应用,

d) 至少一个、优选多个、特别是所有应用可以至少在其资源内评估错误或所述错误和/或启动对应的错误反应和/或通知至少一个其他应用例如可能的安全错误,特别是在分配给所述应用的资源内,

e) 至少一个、优选多个、特别是所有应用可以由至少一个其他应用通知错误或所述错误,

f) 其他应用,特别是不受错误或所述错误影响的应用,可以继续运行,特别是继续按照以下方式运行,即保持运行时行为,特别是等待时间边界条件,其中特别是不需要时钟精确相同的行为。

[0148] 参见图3D,进一步的优选实施方式涉及将表征应用(Applikation)APP1、APP2、APP3的运行状态的信息I1-FUSI,特别是表征关于功能安全(“Safety,安全”)的运行状态(“安全状态”)的信息转发120到至少一个另外的单元,例如外部单元300(图2),特别是布置在计算装置202或设备200外部的单元300。

[0149] 在进一步的优选实施方式中规定,特别是为了保证关于对硬件错误的功能确定性分离的安全反应,未涉及的(一个或多个)应用以及必要时可选地连接到所述应用的(一个或多个)外部单元(例如,驱动器的操控,例如用于承载安全负载以及例如承担将所述计算装置的连接端(“计算机引脚”)转换为例如物理总线协议的信号的PHY,或组件的操控,如内燃机中的点火/喷射)能独立继续运行,分配给所述应用的(相对于所述计算装置的)外部电路发信号通知例如安全状态“错误”(在进一步的优选实施方式中也可以是“复位”,而且附加于复位地),以特别是不影响分配给未涉及的应用的电路部分。

[0150] 在进一步的优选实施方式中,示例性地设置三个计算核心(3个核心),具有3个应用,其中在每个核心上运行三个应用之一。此外,例如设置三个错误引脚(连接端,例如用于发信号通知错误状态)。在进一步的优选实施方式中,示例性地设置了用于VCU(vehicle control unit,车辆控制单元)(例如核心1上的应用1)的外部接口和用于燃烧应用(例如核心3上的应用3)的喷射的外部接口。

[0151] 在进一步的优选实施方式中,燃烧应用例如想要关闭喷射,以降低发动机的扭矩。为此例如激活错误引脚3(其例如在启动期间(即所述设备启动时)已分配给应用3),该错误引脚优选连接到(外部)喷射电路(IC),使得该喷射电路特别是与预给定喷射定时的脉冲无关地关闭并且例如不操控喷射阀。在其他优选实施例中,VCU功能同时继续在核心1上的应用1上继续运行——该VCU例如还经由CAN驱动器传输带有安全负载的信号。在进一步的优选实施方式中,不激活错误引脚1(例如,在启动期间分配给应用1),从而来自所述计算装置或所述设备的CAN信号经由当前未停用(用错误引脚1停用)的CAN驱动器转发。由此,核心1上的VCU应用不受应用3的错误影响(继续),并且特别是继续传输所述CAN信号。

[0152] 进一步的优选实施方式涉及一种用于向所述计算装置或所述设备外部的单元或器件发信号通知、特别是转发至少一个应用的安全状态的方法,其特征在于至少一个以下方面:

a) 安全状态的发信号通知可以优选地用作关闭信号,例如针对外部器件(“外围模块”),

b) 可以将所述发信号通知分配给例如在所述计算装置上并行运行的各个应用,其中特别是可以将分配给一个应用的外围模块与其他应用的状态或所述其他应用的外围模块的状态无关地复位,

c) 可以在复位之后进行分配,优选不可更改地,

d) 这些实施方式的方面也可以用于外部安全器件,例如外部密码器件(密码加速

器、硬件安全模块)、接口,

e)既与功能安全方面(“FUSI”,“安全(Safety)”)相关又与安全方面相关的用途,例如防止操纵(“保安(Security)”)。

[0153] 参见图3E,进一步的优选实施方式涉及一种用于控制诸如车辆1的技术系统1的方法,其中将至少一个外围模块206分配给至少一个、特别是恰好一个应用APP1,参见图3E的步骤125。所述应用可以优选地分别在计算装置202上的分开的分区中运行。

[0154] 在进一步的优选实施方式中,至少一个外围模块206例如是以下元件中的至少一个:计时器(计时器模块)、通信接口206、GPIO端口(通用输入和/或输出连接端)。

[0155] 由此可以优选地实现:多个应用APP1、APP2、APP3在计算装置202上运行时不会相互影响。

[0156] 根据进一步的优选实施方式可以避免的不期望的相互影响的示例是:

1. 模拟/数字转换器(ADC)的运行:如果多个应用访问ADC的资源(例如通道/输入端和/或控制寄存器),则一个应用可能例如覆盖另一个应用的设置,例如通道分配、采样时间(采样率)、转换时间、.....

2. CAN(控制器局域网):如果在多个应用中使用同一CAN总线上的CAN标识符,则可以在CAN模块中例如进行队列条目,其中一个分区(即,例如一个应用)的软件可以覆盖另一个应用的设置。

[0157] 在进一步的优选实施方式中规定,至少一个外围模块可以优选完全地分配给一个分区或应用。

[0158] 在进一步的优选实施方式中,在所述设备或计算装置中设置例如模块,例如SPI(串行外围接口)、LIN(本地互连网络)、CAN、ADC,所述模块例如可以优选地完全分配给一个应用,特别是因为这些模块的资源要么完全被所述分区或应用使用,要么这些模块多次存在,特别是频繁存在,以至于对应的各个模块可以完全分配给一个分区或应用。

[0159] 在进一步的优选实施方式中,提出了以下机制,以特别是根据确定性功能的目标来分离这些模块:

-将至少一个、优选多个或所有模块分配给一个分区或应用(特别是在所述模块中),其中特别是该模块仅从总线(例如用于将该模块连接到所述计算装置或设备的(一个或多个)组件的数据总线)接受带有可预给定标识符(例如“分区ID”)的写入命令和/或读取命令,所述可预给定标识符例如是事先在系统设置时由分区管理器分配给该模块的。

[0160] 因此在进一步的优选实施方式中,模块、优选完整的模块特别是固定地(即静态地)分配给分区,特别是分配给一个分区或应用。

[0161] 在进一步的优选实施方式中可以规定,可以将(外围)模块分配给多个应用,例如可通过至少一个硬件功能(例如地址区域限制)预给定或控制。

[0162] 在进一步的优选实施方式中,例如在设备或计算装置中存在模块,例如GTM(计时器模块)、以太网、HSM(硬件安全模块)(Windows),所述模块的组件或集群或模块部分可以通过地址区域的内部分配被分配给分区或应用。

[0163] 为了根据进一步的优选实施方式分离这些模块,特别是为了确定性功能的目标,提出以下机制:

-通过地址区域将模块分配给分区或应用,和/或

-将资源布置在一个模块中,使得分配给一个分区(或应用)的资源在一个地址区域内彼此靠近(例如相邻地),和/或

-一个或多个地址区域的分配可以例如从外部通过总线桥和/或通过存储器保护装置(MPU)进行,所述存储器保护装置例如确保了不属于分配的分区或应用的内部(一个或多个)主机/从机无法读取和/或写入到该地址区域。

[0164] 因此在进一步的优选实施方式中,(外围)模块向应用或分区的分配可以通过所述地址区域的限制、优选模块内部的限制进行。

[0165] 在进一步的优选实施方式中,例如还存在可以通过软件(SW)机制彼此分离的模块,其中这些模块例如由多个分区或应用使用。根据进一步优选实施方式的一个示例例如是不使用已实现队列的以太网,根据进一步优选实施方式的另一示例是用于处理器间通信的总线,或CAN模块,其中SW分配、特别是各个ID的SW分配是有意义的,因为例如在系统中不存在足够多的CAN模块。

[0166] 因此,在进一步的优选实施方式中提出:

a)通过配置工具配置这些模块,特别是在启动期间,使得考虑使用这些资源的所有分区或应用的边界条件,

b)例如CAN/以太网:以满足所述要求的方式实现来自请求的带宽和/或等待时间——将消息ID分配到具有对应待给定的优先级的模块队列,

c)在持续运行期间,通过分区管理器(在分区或应用上运行在权限模式下的SW)来调节对这些资源的写入/读取——这里优选存在调用分区管理器的多个可能性,例如通过调用(Call)或通过陷阱/模拟(其被故意写入到一个被锁定的资源,从而调用更高的权限级别来解决访问冲突),

d)根据进一步优选实施方式的另一种可能性是通过在持续运行期间设置DMA通道来调节写入和/或读取——然后这些DMA通道例如优选地仅通过特定触发器被激活,并且所述读取和/或写入然后包括例如只有模块中的特殊资源,例如然后写入/读取来自固定分配给各个分区的地址区域的数据。

[0167] 因此在进一步的优选实施方式中提出:将所述设备或计算装置的资源(例如,外围模块)分配给多个分区或应用,其中使用SW功能和HW功能。

[0168] 参见图3F,进一步的优选实施方式涉及一种用于控制诸如车辆的技术系统的方法,其中服务质量(QoS,Quality of Service)或至少一个表征服务质量的变量用于至少暂时地将分区或应用彼此分开,即分离,参见步骤130。

[0169] 根据进一步的优选实施方式,在多个应用可以同时运行的设备或系统中,特别是为了实现所述应用的相同运行时或为了实现可预给定的资源分布(特别是独立于其他应用),有利地也考虑一个或多个总线,所述总线特别是可用于组件之间的数据传输。

[0170] 由于在进一步的优选实施方式中应用的运行时受到多种因素的影响,在进一步的优选实施方式中这些因素也可以单独地或相互结合地得到解决:核心本身(管理程序(Hypervisor)机制)、对存储器的访问(QoS)、访问计算机中的模块,如SPI、安全、.....。

[0171] 根据进一步的优选实施方式提出,可以将用于分离对存储器的访问的机制用于分离对所述(外围)模块的访问,所述机制例如可以在所述设备或计算装置的总线系统或总线架构中设置。

[0172] 在进一步的优选实施方式中,至少一个应用,优选多个或所有应用,为至少一个外围组件或至少一个外围模块设置服务质量(“QoS”),所述服务质量例如可通过等待时间和/或带宽来表征,参见根据图3F的可选步骤132。例如:

- a) 应用1为涉及外围组件的访问设置15个时钟的等待时间和20%的总线带宽,
- b) 应用2为对同一外设组件的访问设置40个时钟的等待时间和70%的总线带宽。

[0173] 换言之,在进一步的优选实施方式中,QoS或QoS机制(例如借助于硬件实现)的使用可以用于控制各个应用APP1的带宽和/或等待时间,特别是用于将外围设备访问(应用对外围模块而不是对存储器的访问)分开,其中特别是还可以用于将应用确定性地分开和减少在一个设备或计算装置中(例如在一个控制设备中)实现多个应用情况下的耗费。

[0174] 在进一步的优选实施方式中提出,使用至少一个计数器来模拟服务质量(QoS),根据进一步的优选实施方式,这特别是在不能借助于硬件实现QoS时特别有用。

[0175] 在进一步的优选实施方式中提出,模拟一个或多个QoS机制,例如借助于以下元素中的至少一个:a)实现针对等待时间和/或带宽的计数器,b)由软件在高优先级(例如,高于应用)评估这些计数器。根据进一步优选实施方式的一种可能实现例如规定:对每个总线实现 $x*2$ 个寄存器(例如32比特宽)作为计数器(Counter),其中 x 表征待支持的分区数量,并且优选地在一个或多个寄存器中对相应分配的应用在每个时钟的访问计数。更优选地,每 z 毫秒(ms)将计数器值与预期计数器值进行比较,并且如果所述计数器值大于所述预期计数器值,则通知应用和例如分区管理器,以特别是启动替代措施。

[0176] 在进一步的优选实施方式中,可以取决于设备200或控制器的类型或取决于所述设备或控制器的目标系统1的类型使用时间同步的网格或角度同步的网格(例如关于内燃机曲轴的一转),特别是用于上面借助于(一个或多个)计数器的示例性描述的QoS模拟。

[0177] 在进一步的优选实施方式中,每在具有(特别是可预给定的)分区ID的总线上施加一个动作就将计数器增加一个可预给定的值,例如一,由此例如可以确定表征带宽的度量。

[0178] 在进一步的优选实施方式中,从(特别是可预给定的)分区对总线的请求(Request)开始对时钟进行计数,直到该分区获得所述总线(准许总线访问)为止。例如,如果经过计数的时钟数量小于可预给定的等待时间,则很好,如果经过计数的时钟的值大于可预给定的等待时间,则这在进一步的优选实施方式中可以得到存储,并且例如在所设置的时间间隔结束时可以读出在所考虑的时间间隔中的所述等待时间是否曾经大于预设时间,以及可选地,如果是则读出大多少。

[0179] 在其他优选实施例中,替代或附加地,借助于硬件和/或触发中断来实现例如预设的自动比较。

[0180] 在进一步的优选实施方式中,可以在所述设备或计算装置的至少一条总线上设置一个或多个计数器。

[0181] 在进一步的优选实施方式中,所述计数器可以与对应的软件(和/或硬件)一起使用,例如用于评估保持的分配的带宽和/或(保持的)等待时间。

[0182] 参见图3G,进一步的优选实施方式涉及一种用于控制诸如车辆的技术系统的方法和设备,其中设置存储器保护装置(MPU),其中所述存储器保护装置特别是用于限制关于设备200或计算装置202的至少一个总线系统的访问权限,参见步骤135。

[0183] 根据进一步的优选实施方式,在一个设备或计算装置上运行多个应用的优点是数

据交换的短等待时间和该交换的高带宽,由此可以以比传统系统中预给定的更短的时间网格来计算例如调节器,因为来自其他应用的数据相对较快地可用。

[0184] 在进一步的优选实施方式中,为了实现这一点并且特别是为了确保多个应用不会不允许地相互影响,提出将在所述计算装置内或所述计算装置外(例如在总线系统的区域中)的MPU用于限制访问权限。

[0185] 在进一步的优选实施方式中,可以示例性地使用以下流程:设置例如核心外部的MPU,例如在总线接口中,其中设置两个应用,其中每个应用都在一个核心上运行。

[0186] 在进一步的优选实施方式中,MPU可以被配置为,例如在系统启动期间,使得在每个分配给另一个核心的本地存储器中分配用于写入的区域,并且在自己的存储器中释放在于读取的区域。由此例如每个应用都可以读取另一个核心的数据并且通过写入向所述另一个核心本地提供数据,特别是不能覆盖其他(存储)区域。

[0187] 因此在进一步的优选实施方式中提出:一种用于借助于MPU使用存储区域分配以确保在所述计算装置或所述设备上运行的多个应用之间的确定性数据交换的方法。

[0188] 因此在其他优选实施例中提出:一种用于使用至少一个MPU确保不同应用的确定性存储器访问和/或数据交换的方法。在此背景下,“确定性”特别优选地与应用定时(即(一个或多个)应用的时间行为)有关,并且特别是与用于访问相应资源的周期的具体数量无关。

[0189] 参见图3H,进一步的优选实施方式涉及一种用于控制诸如车辆的技术系统的方法和设备,其中使用至少一个硬件加速器单元HSM(图2)以加速所述系统或所述设备200的启动(startup)。

[0190] 在现代(特别是汽车)系统中,将设备的现有软件替换为其他软件(“Tuning,调谐”),以例如在应用中有更多功率可用(例如更多功率,PS)。识别并在必要时防止这种情况的一种方法提出,在引导(启动)系统时事先检查软件代码以确定所述软件代码是否是实际应当执行的代码或所述代码是否已被操纵,例如在调谐措施的范围之内。

[0191] 根据进一步优选实施方式的用于检查SW代码的方法规定,确定或计算关于可预给定的存储区域或(特别是整个)存储器的至少一个校验和(Checksum)。在此的一个问题可能是确定或计算所述校验和需要相对较长的时间,从而引导过程被延长了。在进一步的优选实施方式中,例如应当在30ms-100ms内完成引导过程。但是,由于校验和计算可能会增加大量的毫秒数。

[0192] 因此,在进一步的优选实施方式中提出设置至少一个硬件加速器单元HSM并将其用于计算(一个或多个)校验和(“HW校验和加速器”)。在进一步的优选实施方式中,还可以设置多个硬件加速器单元,这些硬件加速器单元必要时分别处理待检查的存储器的一部分或为对应部分形成校验和。更优选地,在启动(一个或多个)应用APP1、APP2、APP3之前借助于所述至少一个硬件加速器单元来计算校验和。

[0193] 在进一步的优选实施方式中,硬件加速器单元也可以分配给不同的分区或应用。

[0194] 参见图3I,进一步的优选实施方式涉及一种用于控制诸如车辆1的技术系统1的方法和设备200,其中在至少一个硬件模块208或外围组件中实现机制,优选地在模块208的接口(Interface)中实现,参见根据图3I的步骤150,借助于所述机制可以由多个分区或应用APP1、APP2、APP3下达任务,这些任务特别是分别不能被其他分区覆盖或影响。在进一步的

优选实施方式中,该机制也可以被称为“(一个或多个)传输窗口”。

[0195] 在进一步的优选实施方式中,所述硬件模块(或所述模块的控制器,例如所述模块的微控制器)或所述外围组件被构造为根据预给定规则处理所述任务,例如以轮询(Round Robin)方法,由此有利地对于(外部)应用而言代表了确定性时间行为。

[0196] 进一步的优选实施方式规定了在至少一个硬件模块中实现传输窗口,具有至少一个以下方面:

a)所述传输窗口的地址区域可以可选地分配给不同的应用/分区,

b)在所述模块中例如借助于SW按照预给定的方法(例如轮询方法)对任务进行处理。

[0197] 进一步的优选实施方式涉及根据实施方式的方法和/或根据实施方式的设备和/或根据实施方式的计算机可读存储介质和/或根据实施方式的计算机程序和/或根据实施方式的数据载体信号用于以下元素中的至少一个的用途:a)实现所述设备的至少一些应用、优选所有应用的确定性运行时行为,b)避免对第一应用的新认证,特别是在改变至少一个另外的应用时。

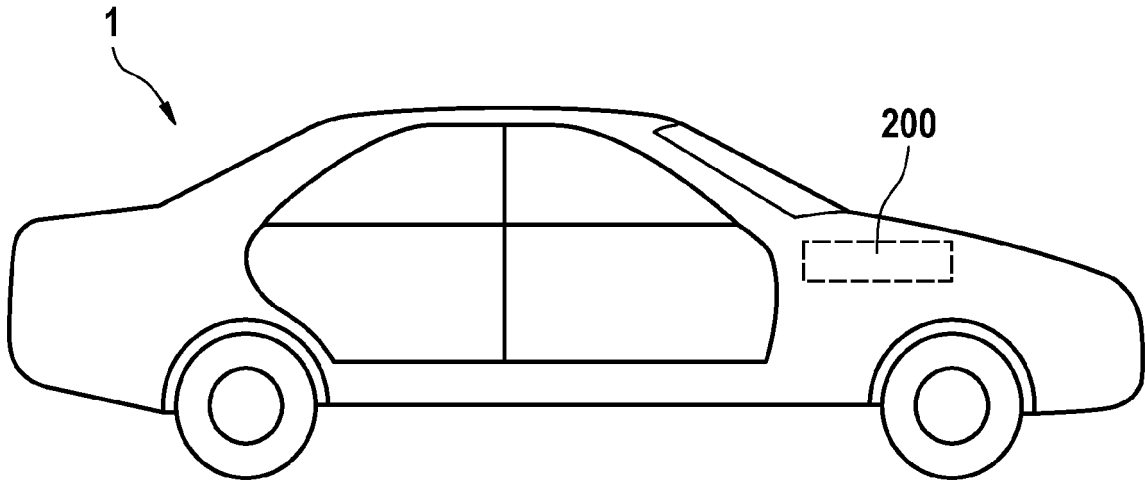


图 1

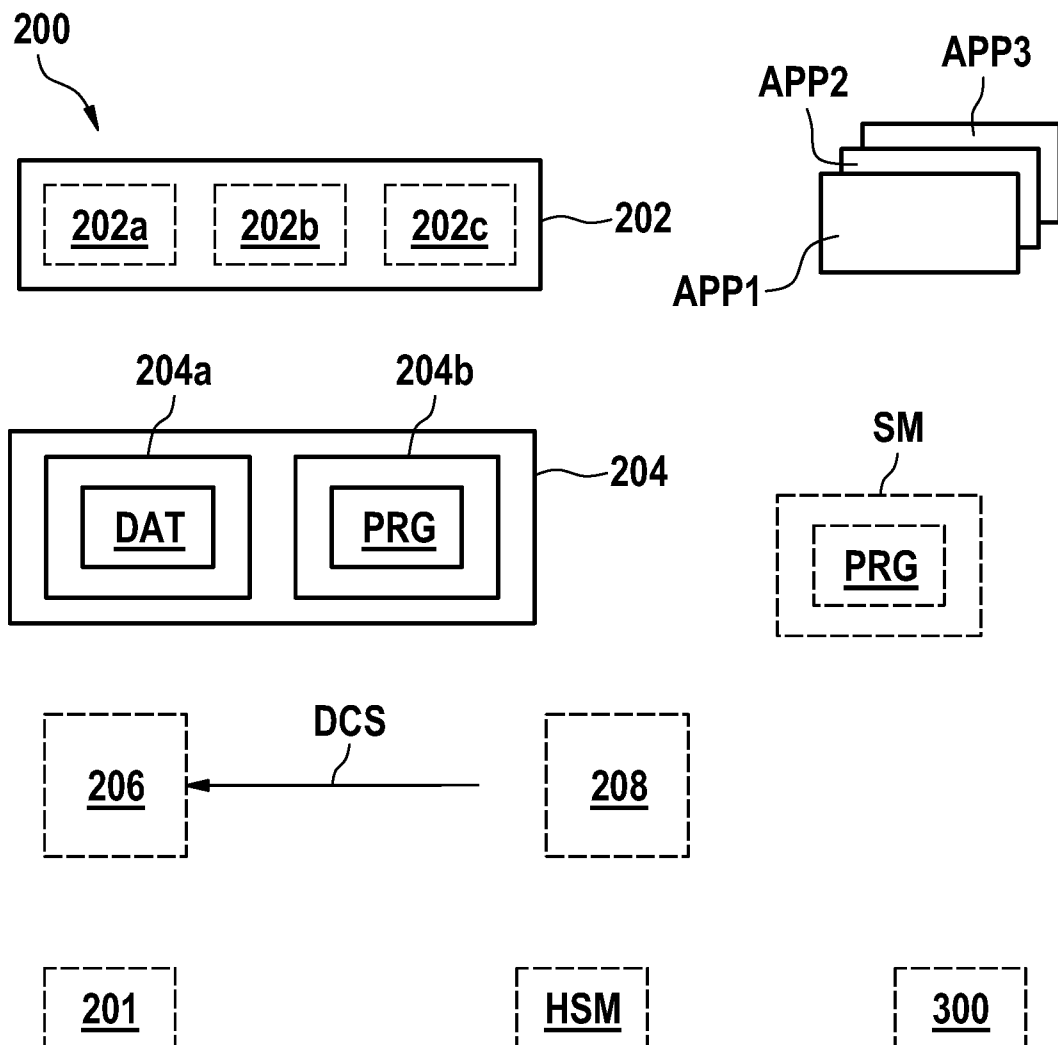


图 2

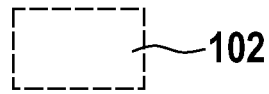
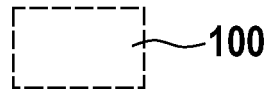


图 3A

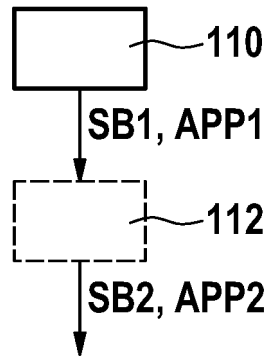


图 3B

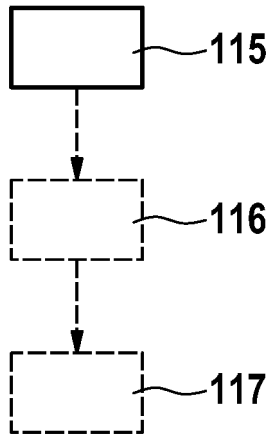


图 3C

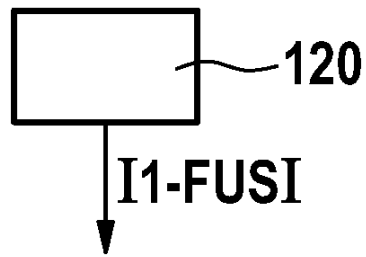


图 3D



图 3E

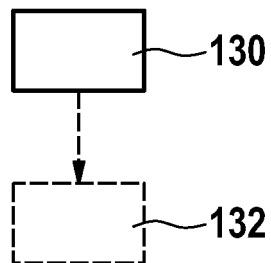


图 3F



图 3G



图 3H

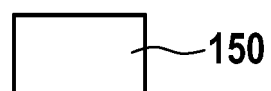


图 3I