(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105074833 B
(45)授权公告日 2018.01.02

(21)申请号 201480007833.9
(22)申请日 2014.01.30
(65)同一申请的已公布的文献号
申请公布号 CN 105074833 A
(43)申请公布日 2015.11.18
(30)优先权数据
102013201937.8 2013.02.06 DE
(85)PCT国际申请进入国家阶段日
2015.08.06
(86)PCT国际申请的申请数据
PCT/EP2014/051837 2014.01.30
(87)PCT国际申请的公布数据
WO2014/122063 DE 2014.08.14
(73)专利权人 阿海珐有限公司
地址 德国埃尔朗根
(72)发明人 齐格弗里德·哈尔比格
(74)专利代理机构 北京弘权知识产权代理事务所(普通合伙) 11363
代理人 许伟群 李少丹
(51)Int.Cl.
G21D 3/00(2006.01)
G05B 23/02(2006.01)
G06F 21/56(2006.01)
G06F 21/57(2006.01)
(56)对比文件
JP 特开平9-211186 A,1997.08.15,全文.
US 2011/0039237 A1,2011.02.17,全文.
US 2013/0044848 A1,2013.02.21,全文.
CN 101038489 A,2007.09.19,全文.
CN 1574727 A,2005.02.02,全文.
审查员 周桂芳

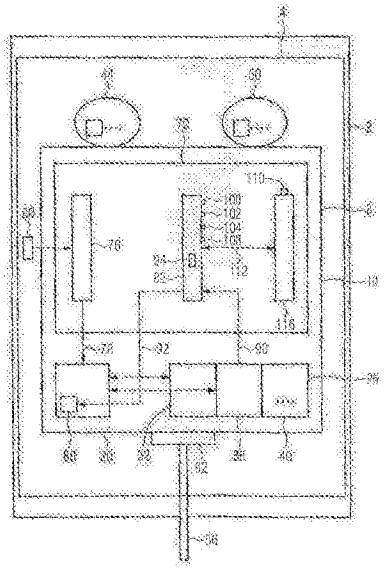
权利要求书1页 说明书10页 附图4页

(54)发明名称

用于识别对控制和调节单元的系统状态的未授权操控的装置以及具有该装置的核设施

(57)摘要

一种用于识别对核设施(2)的控制和调节单元(8)、特别是存储器可编程控制器(10)的系统状态的未授权操控的装置(70),其应当能够以可靠的方式检测未授权的操作。为此,设置有监视模块(82),其监视所述控制和调节单元(8)的工作状态和/或硬件扩展状态和/或程序状态,并且在所述状态改变时产生通知。



CN 105074833 B

1.一种用于识别对控制和调节单元(8)的系统状态的未授权操控的装置(70),其中

设置有监视模块(82),其监视所述控制和调节单元(8)的工作状态和/或硬件扩展状态和/或程序状态,并且在所述状态改变时产生通知,

设置有控制模块(116),其监视所述监视模块(82)的操作,

其中所述监视模块(82)监视所述控制模块(116)的操作,

其特征在于,所述控制和调节单元(8)包括存储器可编程控制器(10),并且监视模块(82)和控制模块(116)是所述存储器可编程控制器(10)的软件块,监视模块和控制模块相互检查在预先给定的时间段内另外的模块是否正常处理程序指令。

2.根据权利要求1所述的装置(70),其中,所述控制和调节单元(8)具有其中存储有数据的至少一个能写入的存储器(26),并且其中所述监视模块(82)在存储在所述存储器(26)中的数据改变时产生通知。

3.根据权利要求2所述的装置(70),其中,所述数据包括程序代码和/或由其生成的程序变量。

4.根据权利要求2或3所述的装置(70),其中,所述数据包括系统数据。

5.根据权利要求1至3中的任一项所述的装置(70),其中,所述监视模块(82)监视所述控制和调节单元(8)的CPU的工作方式选择开关的状态。

6.根据权利要求1至3中的任一项所述的装置(70),其中,所述监视模块(82)监视所述控制和调节单元(8)的安全等级的改变。

7.根据权利要求1至3中的任一项所述的装置(70),其中,所述通知被写入所述控制和调节单元的CPU的存储器和/或所述监视模块的缓冲器(94)。

8.根据权利要求1至3中的任一项所述的装置(70),其中,在所述装置(70)输出(100,102,104,108)处提供所述通知。

9.根据权利要求1至3中的任一项所述的装置(70),其中,设置有安全模块(76),其根据需要切换所述控制和调节单元(8)的安全等级。

10.根据权利要求1至3中的任一项所述的装置(70),其中,该装置用于识别对核设施的控制和调节单元(8)的系统状态的未授权操控。

11.根据权利要求2或3所述的装置(70),其中,所述数据包括硬件配置和/或由其生成的系统变量。

12.根据权利要求1至3中的任一项所述的装置(70),其中,所述通知被写入所述控制和调节单元的CPU的诊断缓冲器(88)和/或所述监视模块的缓冲器(94)。

13.根据权利要求1至3中的任一项所述的装置(70),其中,在所述监视模块(82)的输出(100,102,104,108)处提供所述通知。

14.根据权利要求1至3中的任一项所述的装置(70),其中,设置有安全模块(76),其在操作按键开关(80)时切换所述控制和调节单元(8)的安全等级。

15.一种核设施(2),具有根据权利要求1至14中的任一项所述的装置。

用于识别对控制和调节单元的系统状态的未授权操控的装置以及具有该装置的核设施

技术领域

[0001] 本发明涉及一种用于识别对控制和调节单元、特别是核设施的存储器可编程控制器的系统状态的未授权操控的装置和方法。本发明还涉及一种用于核设施的存储器可编程控制器、数字监视设备以及相应的核设施。

背景技术

[0002] 在例如发电设施的核设施(核电站)中,许多协作的处理并行地进行,这些处理通常包括控制和调节过程。在此,对于相应的处理,使用针对应用而优化和配置的控制和调节单元。

[0003] 由于核设施、特别是发电设施的也日益增加的数据联网以及其到外部网络、直到因特网的连接,这些设施很容易受到病毒或者其他恶意软件的攻击。这种设备被软件病毒攻击的一个已知情况是STUXNET。这种攻击可能导致设施的生产损失直至全部故障,并且产生高额的人力和经济损失。此外,这种渗入的恶意软件可能被用于工业间谍活动。此外,在病毒的初次攻击中,存在病毒扩散的危险,从而病毒可能攻击同一核设施的其他控制装置,或者由此还可能攻击与之联网的设施的控制装置。由于这些危险,在联网环境中,其存储器配置原则上在运行时间期间可能被恶意软件修改的控制系统的使用可能显现高的安全风险。这种控制系统是存储器可编程控制器(SPS)。

发明内容

[0004] 因此,本发明要解决的技术问题是,提供一种装置,利用其能够以可靠的方式检测未授权的操控。此外,要提供一种用于核设施的存储器可编程控制器和数字监视设备、一种核设施以及相应的方法。

[0005] 关于装置,根据本发明,上述技术问题通过设计一种监视模块来解决,该监视模块监视控制和调节单元的工作状态和/或硬件扩展状态和/或程序状态,并且在该状态改变时产生通知。

[0006] 本发明的有利的扩展方案是从属权利要求的主题。

[0007] 本发明基于如下考虑:当病毒或者类似的恶意软件能够影响控制和/或调节系统的系统状态,使得其功能以不希望的方式改变、扩展或者损坏时,病毒或者类似的恶意软件的攻击有效果。这可以通过如下方式进行:恶意程序和/或恶意数据被加载到在工作期间可进行写入的存储器中并且执行。由于该原因,首先在安全关键的设备中使用这种控制和/或调节系统产生问题。在核设施中,需要满足最高的安全标准,因为控制系统的改变可能导致间谍活动、部件失效、故障和严重的事故。

[0008] 在这种攻击中,例如会导致在控制和/或调节单元中渗入附加程序代码,或者已有程序代码被受感染的代码代替。此外,可能导致配置改变,使得无法再从传感器接收到数据,和/或无法再对执行器进行应答或控制。

[0009] 如现在所认识到的，通过监视在这种设施中使用的控制和调节单元的系统内部过程，换句话说，即控制和调节单元的工作状态和/或硬件扩展状态和/或程序状态，并且通知改变，能够实现所需要的高安全标准。

[0010] 通过产生通知，可以立即检查改变是哪种类型的，以及其是否可能是未授权进行的改变。此外，使得能够直接对该改变作出反应。在本申请的范围内，利用控制和调节单元标明仅能够执行控制过程或调节过程或者还能够执行两种类型的过程的每个电子单元。

[0011] 优选的是，控制和调节单元具有至少一个其中存储有数据的可写入的存储器，其中，在存储于存储器中的数据改变时，监视模块产生通知。诸如存储器可编程控制器的具有可写入的存储器的控制和调节单元的工作状态、硬件扩展状态和程序状态主要通过其存储内容来确定。在此，存储内容通常包括程序代码、有关硬件和软件的配置以及动态地设置的数据字段、变量等。在存储器的改变中能够注意到恶意软件从外部的敌意攻击，从而存储器内容的改变可以指示未授权的操控。

[0012] 有利的是，数据包括程序代码或者由此产生的程序变量。程序代码、特别是可加载的用户程序在工作期间在运行时执行，并且包含执行的指令。程序代码的改变指示有操控。然而，为了识别这些操控，不一定必须直接监视代码的改变。在此，更有效并且更经济的是，监视由此得到或者借助程序代码(用户代码、固件、操作系统等)产生的、即一定程度上的次级程序变量的改变(只要其在代码改变时也以足够大的概率使得这些变量改变)。例如在根据代码或代码段或者代码组成部分产生的校验和或长度时，情况如此。在此，有利的是，CPU具有“关于软件块或模块的校验和的异或逻辑”作为内部功能。然后，由监视模块读出结果(例如32比特值)，并且监视改变。诸如SIMATIC S7-300和SIMATIC S7-400的存储器可编程控制器由本身自动产生校验和、特别是横加和(Quersummen)。其必须由监视模块仅仅读出并且监视改变。由此，通过旧/新值比较，能够识别出每个程序改变。

[0013] 有利的是，数据包括系统数据、特别是硬件配置和/或由其产生的系统变量。在此，硬件配置在模块化系统中包括关于所使用的组件的数据。例如，在SIMATIC中经由包含在编程软件STEP7/PCS7中的HWKonfig进行硬件配置的规划。要插入模块化的S7-300或S7-400中的每个组件为了能够运行必须在HWKonfig中参数化，并且随后加载到目标站的CPU上。在HWKonfig中，将相应组件的所有设置诸如组件地址、诊断设置、测量区域设置等参数化。由此，可以省去经由例如桥式开关的设置。在组件更换的情况下，不再需要另外设置。

[0014] 所述规划存储在所谓的系统数据中。检查这些系统数据的改变使得能够检测到可能的攻击。如上面所描述的，控制和调节单元还提供关于校验和的异或逻辑，由监视模块读出该异或逻辑，并且通过旧/新值比较来监视改变。

[0015] 在一个优选实施方式中，监视模块监视控制和调节单元的CPU的工作方式开关的状态。这种工作方式选择可以具有多个设置。其例如可以是：

[0016] -MRES(重置变量存储器)

[0017] -STOP(不能进行程序处理，仅能进行通信)

[0018] -RUN(程序改变可能性被锁定的程序处理)

[0019] -RUN-P(能够进行程序改变的程序处理)

[0020] 在许多当前的没有按键开关的CPU情况下，仅存在开关状态“START”和“STOP”，其中，在状态“STOP”中，不能够进行程序处理，使得在这种情况下，CPU中的程序分析不带来改

变。

[0021] 还可以设计的是，监视模块监视控制和调节单元的安全等级的改变。安全等级例如可以具有分别与密码保护相结合的状态“仅读取”或者“读取和写入”。

[0022] 在监视期间确定工作状态、硬件扩展状态或者程序发生改变的情况下，产生通知，这能够以不同的方式和方法进行。为了该通知在稍后的时刻可供评价使用，有利的是将其写入存储器、特别是控制和调节单元的CPU的诊断缓冲器和/或监视模块的监视缓冲器中。诊断缓冲器例如可以实施为集成在CPU中的存储区域，其能够作为环形缓冲器接收诊断记录。优选的是，对这些记录设置日期/时间戳。优选的是，监视模块具有监视存储器，其中能够写入优选具有日期和时间戳的通知。该监视存储器例如可以实施为环形缓冲器。通知记录可以仅写入两个存储器中的一个中，或者为了产生冗余而写入两个存储器中(如果存在)。

[0023] 替代地或者优选附加地，在装置、特别是监视模块的特别是二进制的输出处提供该通知。由此，其可供设计者用于特定于设备的通知输出。在此有利的是，设置多个输出，其与检测到的改变的各种类型(程序存储器、系统数据存储器、安全等级等)相关联。

[0024] 优选的是设计一种安全模块，其按照需要、特别是在操作按键开关时切换控制和调节单元的安全等级。在此，安全等级尤其是具有状态“读取和写入”以及“仅读取”以及“写入和读取保护”，其中，这些状态可以可选地与密码验证结合。可以用来进行这种切换的按键开关于是例如设置在开关盒中。因此，能够确保仅由授权的人员进行程序改变。于是，在不转换或操作按键开关的情况下，程序改变在一定程度上被锁定，由此不可能进行。按键开关被连接到任意数字输入。在控制程序中，该信号连接到模块(SecLev_2)，该模块于是经由系统函数设置安全水平。

[0025] 在装置的一个优选实施方式中，设置有控制模块，其对监视模块的工作进行监视，其中，该监视模块也对控制模块的工作进行监视。这种构型基于如下考虑：攻击者为了能够在控制和调节单元中进行不被识别的程序改变，他必须首先通过安全等级为“读取和写入”的状态来获得写入访问。附加地，他必须禁止监视模块的活动，也就是说，他必须在实现监视模块时，通过软件模块或者通过软件块，在CPU侧禁止其处理或者其程序指令的处理。为了识别或拦截后者，设置该控制模块。

[0026] 监视模块和控制模块相互监视其工作。因此，这里不存在对控制和调节单元的简单的冗余监视。在监视模块和控制模块作为软件块实现的优选情况下，两个模块在很大程度上相互监视其执行。有利的是，这通过检查在预先给定的时间段、例如一秒期间是否存在分别被监视的模块的正确执行来进行。如果不是这种情况，则通知有缺陷的执行，这可以指明折衷的尝试或者已经进行的折衷。

[0027] 从通过攻击从外部删除软件块只能依次进行。也就是说，如果攻击者即使能够获知这两个模块的存在和它们的功能，则攻击者也必须依次将它们删除或去激活。然而，在删除或者去激活这两个模块中的一个时，这将被相应的另一个模块识别到，并且产生对应的通知，使得可靠地识别出这两个模块中的一个的失效。

[0028] 在控制模块确定监视模块的操作不正常的情况下，其有利地在二进制输出上显示监视模块的错误操作或错误执行。监视模块在上面描述的路径中的至少一个上显示控制模块的操作的不正常：将通知优选与日期/时间戳一起写入CPU或监视模块的存储器或缓冲器

中，或者在至其他设备专用的(二进制)输出上提供通知输出。优选采用所有三种路径。

[0029] 关于存储器可编程控制器，根据本发明，上述技术问题利用通过软件模块集成的上面示出的装置来解决。也就是说，上述模块(监视模块、控制模块、安全模块)分别作为软件模块或软件块来实现，并且在控制和调节单元的工作状态中位于其存储器中。

[0030] 关于用于核设施的数字监视设备，根据本发明，上述技术问题利用上面示出的存储器编程控制器来解决。

[0031] 关于核设施，根据本发明，上述技术问题利用这种数字监视设备来解决。

[0032] 关于方法，上述技术问题通过如下方式解决：监视控制和调节单元的工作状态和/或硬件扩展状态和/或程序状态，并且在该状态改变时输出通知。该方法的有利的扩展方案从结合装置描述的功能中得出。

[0033] 本发明的优点特别在于，通过监视控制和调节单元的工作状态、硬件扩展状态和程序状态，尽量防止并且可靠地通知未发现的操控，使得能够立即并且有针对性地启动措施以避免设施损坏。以这种方式首先使得能够在联网的安全关键的环境中使用存储器编程控制器。通过监视模块和控制模块的相互监视，实现了通过关断监视来进行操控是不可能的。

附图说明

[0034] 根据附图详细说明本发明的实施例。其中在简明示意图中：

[0035] 图1以优选实施方式示出了包括具有控制和调节单元的数字监视单元的核设施，控制和调节单元包括具有监视模块、安全模块和控制模块的集成装置，

[0036] 图2示出了根据图1的装置的安全模块的功能的流程图，

[0037] 图3示出了根据图1的装置的监视模块的功能的流程图，以及

[0038] 图4示出了根据图1的装置的控制模块的功能的流程图。

[0039] 在所有图中，对相同的部分设置相同的附图标记。

具体实施方式

[0040] 在图1中示出的核设施2包括具有作为模块化的存储器可编程控制器(SPS)10实现的控制和调节单元8的数字监视设备4。在此，例如可以是西门子公司的SIMATIC S7-300或S7-400。其包括CPU 20以及存储器26，该存储器包括多个存储区域。在程序存储区域32中存储在SPS 10工作期间执行的程序。附加地，存储代码的校验和及其长度，它们由CPU 20在传输程序到CPU时计算，并且在发生改变时即刻更新。同样计算关于这些校验和的异或逻辑，存储在系统数据存储器38中，并且在发生改变时更新。还可以设计为，将这些从程序代码导出的变量存储在单独的存储区域中。

[0041] 此外，CPU 20将配置数据、特别是硬件的配置数据存储在系统数据存储区域38中。为了如在当前情况下那样在模块化地构造的SPS 10中使得组件能够运行，必须将其在硬件配置中参数化，随后上传到CPU 20。在硬件配置中，将相应组件的所有设置、例如组件地址、诊断设置、测量区域设置等参数化。于是在组件更换的情况下，不再需要其他设置。此外，存储器26还包括其他存储区域40。

[0042] SPS 10在输入侧连接到包括多个传感器的传感器组44，并且在输出侧连接到在其

方面包括多个执行器的执行器组件50。数据线56从外部引导到核设施中，并且经由接口62将SPS 10连接到局域网(LAN)或者还有因特网。由于这种连接，存在如下可能性：潜在的攻击者企图使病毒渗入CPU 20或者在CPU 20中安装其他类型的恶意软件，以获得关于存储在CPU 20中的数据的信息(工业间谍活动)，或者改变、阻止或损坏SPS 10的功能。当SPS 10用于对安全关键的过程的控制时，成功的这种攻击可能导致严重的人员伤害以及经济损失。

[0043] 为了防止这些损失，并且能够可靠并且快速地识别出对SPS 10的工作状态、硬件扩展状态和程序状态的攻击和由此未授权的操控，根据本发明，设计了一种装置70，其在当前情况下集成在SPS 10中。装置70包括三个模块76、82、116，其将在下面描述。这些模块作为软件块来实现并且存储在程序存储区域中。

[0044] 如箭头78所示，安全模块76有权访问CPU 20的安全等级。其被设计为在“读取和写入”、“仅读取”和“写入和读取保护”之间或者相反之间切换安全等级。该功能与内置到开关盒(未示出)中的按键开关80耦合。也就是说，在按键开关的第一状态中，安全模块76激活安全等级“读取和写入”，并且在按键开关的第二状态中，安全模块76激活安全等级“仅读取”或者替选地激活“写入和读取保护”。在持续工作时，该第二状态是正常状态，使得未授权的人员无法在存储器26中进行程序改变或者其他改变。仅当按键开关处于第一状态中时，才能进行改变。因此，攻击者必须获得对按键开关的访问，也就是说必须设法接近设备，这通过常见安全措施基本能够防止。他也可能在按键开关位于第一状态中时，通过渗入用于进行删除的恶意软件或者然后还通过程序直接在CPU中改变安全等级。

[0045] 为了可靠地发现任意形式的恶意软件的渗入或者未授权地对SPS 10的工作状态、硬件扩展状态和程序状态的改变，设置监视模块82。如由箭头90所示出的，监视模块82监视存储器32的程序存储区域中的改变。这以如下方式进行：CPU 20根据存储在程序存储区域32中的程序代码针对每个块产生校验和与程序长度。通过关于这些各个校验和与程序长度的异或逻辑运算，形成总校验和(32比特数)，并且存储在系统数据存储器38中。监视这些逻辑运算的结果(总校验和)的改变。为此，在预先给定的时间间隔中进行旧/新值比较。

[0046] 如箭头90所指示的，监视模块82还监视系统数据存储区域38的改变。这又通过检查由CPU 20产生并提供的关于系统数据的长度和校验和的异或逻辑运算的改变来进行。此外，监视模块82监视同样存储在系统数据存储器中的CPU 20的安全等级的改变。

[0047] 在所监视的结果发生改变时，监视模块82以三种不同的方式产生通知。一方面，将通知写入SPS 10的诊断缓冲器88。其是在CPU 20中实施为环形缓冲器的、可以接收多达500个诊断记录的集成存储区域。即使在“全部删除(Urlöschen)”(全部删除是除了诊断缓冲器88之外将CPU的整个存储器删除的功能，也就是说，全部删除的CPU不(再)工作)或者同时电池和网络失效之后，也仍然能够读出该存储器。通过将通知写入诊断缓冲器88，由此确保即使在电源失效之后，通知也不丢失。一方面，诊断缓冲器的内容可以经由编程软件STEP7/PCS7读出并显示。另一方面，特定HMI设备/软件系统、例如WinCC或PCS7OS同样可以以具有日期/时间戳的明文显示这些诊断缓冲记录。

[0048] 监视模块82还将通知写入在监视模块82中实现的、作为环形缓冲器实施的监视缓冲器94中，其在当前情况下可以接收50个记录。每个记录由针对每个发生的改变的日期/时间戳和一比特构成。监视缓冲器94可以借助STEP7/PCS7读出并进行分析。

[0049] 此外，分别在监视模块上的二进制输出100、102、104处提供或显示通知，由此供进

一步处理使用。在报警之后，操作员在需要时可以经由诊断缓冲器或者监视缓冲器读出更深入的信息。上面描述的三种监视(程序代码、系统数据、安全等级)中的每一种分别与单独的二进制输出100、102、104相关联，使得设置一比特足以进行通知。程序代码改变时的通知在二进制输出100处，系统数据改变时的通知在二进制输出102处，而安全等级改变时的通知在二进制输出104处，通过分别设置一比特进行。

[0050] 通过所描述的监视模块82，可以基于所产生的通知识别对系统数据和/或程序代码进行改变的企图，其例如可能是要损害SPS 10功能的病毒攻击的结果。然而，通过在监视模块82注意到入侵并且能够产生通知之前，攻击者部分或完全删除或去激活监视模块82，可能阻止通知的产生。为了防止这种场景，设置有控制模块116。如通过双箭头112所示出的，监视模块82和控制模块116彼此相互监视。在此，这以分别监视程序指令的执行的方式进行。为此，分别检查在预先给定的时间间隔、这里为1秒内(通常控制程序在10至100毫秒的时隙中运行)是否持续进行程序代码的指令的执行。如果这两个模块82、116中的一个发现在相应的另一个模块82、116中处理没有持续进行，则其产生对应的通知，从而能够对可能的攻击作出反应。

[0051] 控制模块116在二进制输出110处显示监视模块82的错误或者缺失的执行。如上面结合对存储器26的监视所描述的，监视模块82的错误或缺失的执行分别与日期和时间戳一起写入诊断缓冲器88和监视缓冲器94中，以及在二进制输出110处供其他的特定于设备的通知输出使用。

[0052] 这种机制极其可靠，因为攻击者必须首先完全从外部获知两个相互控制或监视的模块82、116的存在。此外，他不可能同时删除两个模块82和116，使得这两个模块82或116中的至少一个产生通知，由此能够识别出攻击。然而，即使在没有攻击的情况下，也能够发现这两个模块82、116中的一个的失效或功能故障。

[0053] 在图2中示出了在安全模块76的工作状态中进行的方法步骤的流程图。在安全模块76中通过软件实现的方法在开始120处开始。在判断126中，检查按键开关80是否给出了使得能够进行写入/读取访问的有效信号，并且检查该信号的状态是否同时有效或者存在模拟。如果满足所有这些条件，则该方法分支到方框132，其中，将CPU 20的安全水平切换为写入/读取访问，这对应于安全等级1。

[0054] 否则，该方法分支到判断134，其中，检查在没有密码证明的情况下是否应当阻止写入和读取访问。如果这是肯定的，则该方法分支到方框136，其中，将CPU 20的安全水平或安全等级切换为没有密码证明的写入/读取访问。当上面的两个判断126、134都为否定的时，在方框138中，将安全水平切换为具有密码证明的写入保护，这对应于安全等级2。在方框140中，读出并显示当前安全水平。该方法在结束142处结束。

[0055] 在监视模块82中通过软件实现的方法在图3中借助流程图示出，并且在开始150处开始。在方框152中，读出硬件配置HWKonfig和程序代码的校验和、这里为横加和以及安全水平。在判断154中，借助旧值/新值比较来检查HWKonfig的校验和的值与来自最后一次查询的值是否一致。如果情况为否，则该方法分支到方框145。其中，将通知记录“HWKonfig改变”分别与日期/时间戳一起登记在或写入监视缓冲器94中和诊断缓冲器88中，并且设置二进制输出102，用于特定于设备的进一步处理，也就是说，对该比特设置与通知相对应的值(例如，对于有通知为1，对于无通知为0)。如果通过旧值/新值比较确定横加和没有改变，则

在方框158中，将输出102复位，由此确保不错误地显示通知。

[0056] 在判断160中，检查读出的程序代码的横加和的值是否相对于来自最后一次查询的其先前的值发生了改变。如果发生这种情况，则该方法分支到方框162。其中，将通知记录“程序改变”、包括日期/时间戳写入监视缓冲器94和诊断缓冲器88中，并且设置输出100。否则，在方框164中，将输出100复位。

[0057] 在判断166中，检查自最后一次查询起CPU 20的安全等级是否发生了改变。如果是这种情况，则在方框168中，将通知记录“安全等级改变”与时间戳一起写入监视缓冲器94和诊断缓冲器88中。此外，设置输出104。否则，在方框170中，将该输出复位。

[0058] 在判断172中，测试对所描述的方法步骤的调用是否在1秒以前。如果是这种情况，则在方框中输出参数化错误(所描述的三个模块76、82、116将与库中的其他模块一起提供给应用使用。用户可以通过模块的参数化在编程中或者在投入运行时选择/设置不同的特性。当用户对不允许的特性进行了参数化/选择时，他得到参数化错误显示，并且可以对其参数化进行校正)。否则，该方法分支到方框176，其中，将参数化错误复位。

[0059] 在本实施例中，监视模块82和控制模块116的相互监视通过如下方式来实现：每个模块分别具有自己进行向上计数的计数器以及由相应的另一个模块进行向上计数的计数器。当两个模块82和116按照规定工作时，计数器分别具有相同的值。如果一个模块失效，则在另一个模块中由其向上计数的计数器不再增加，从而能够识别该模块的失效。

[0060] 现在，该方法进一步进行到判断178，其中，将由监视模块82向上计数的监视计数器的值与由控制模块116向上计数的控制计数器的值进行比较。如果这些值一致，则在方框180中，将监视计数器增加。如果这两个值不一致，则在判断182中检验控制计数器的最后的计数器增加是否在1s以前，并且是否尚未进行在监视缓冲器94和诊断缓冲器88中的登记。如果是这种情况，则这表明控制模块106未按照规定工作。因此，然后在方框184中，将通知记录“删除监视错误”或“控制模块错误”分别与时间戳一起登记在监视缓冲器94和诊断缓冲器88中，并且在显示控制模块116的错误的二进制输出108处设置一比特。然后，该方法在结束186处结束。否则，在判断188中，检查在CPU的诊断缓冲器88中是否已经存在方框184中已登记的记录“监视模块又工作”。如果是这种情况，则在方框190中，将输出108复位。否则，在方框192中，在监视缓冲器94和诊断缓冲器中，与时间戳一起进行通知登记“控制模块工作ok”或者“删除监视ok”。

[0061] 在控制模块116中通过软件实现的方法作为流程图在图4中示出，并且在开始194处开始。在判断196中，检查与监视模块82的连接是否符合规定或正确。即，在本实施例中，用户必须在规划/编程时，使用鼠标通过点击在CFC编辑器(连续功能图，ContinuousFunction Chart)中在两个模块之间制作连接/线路。通过这种连接，控制模块116可以读取和写入监视模块82的实例数据块。控制模块自己没有单独的数据存储器。如果不是这种情况，则在方框198中输出参数化错误。否则，在判断200中，检查对该功能的最后的调用是否在1s以前。如果不是在1s以前，则在方框202中，输出参数化错误。如果是，则该方法进一步进行到方框204，其中，将参数化错误复位。

[0062] 当监视模块82向上计数的计数器大于控制模块116的计数器时，在控制模块116中将控制计数器向上计数。在判断206中，将监视计数器和控制计数器相互进行比较。如果监视计数器大于控制计数器，则在方框208中，将控制计数器增加。随后，在判断210中，检查是

否在诊断缓冲器88中登记了记录“监视模块又工作”。如果未登记，则在方框212中补做。然后，在方框214中，将对应的二进制输出复位。

[0063] 当存在一致时，则在判断216中检查监视计数器的最后的计数器增加是否在1s以前，并且尚未在诊断缓冲器88中进行登记。当尚未进行登记时，在方框218中，在诊断缓冲器88中进行登记“监视模块不再工作”。然后，在方框220中设置输出110。

[0064] 如果最后的计数器增加在1s以前，并且不存在登记，则该方法从判断216直接分支到方框220。该方法在结束222处结束。

[0065] 在所有三个模块中，方法步骤的顺序也可以以不同的顺序或者并行地进行，只要所描述的功能得以保持即可。分别在开始和结束之间描述的方法步骤的次序以规则的时间间隔重复。相应地，在开始和结束之间，相应的模块将由其更新的其计数器向上计数1。

[0066] 附图标记列表

[0067] 2 核设施

[0068] 4 数字监视设备

[0069] 8 控制和调节单元

[0070] 10 存储器可编程控制器

[0071] 20 CPU

[0072] 26 存储器

[0073] 32 程序存储区域

[0074] 38 系统数据存储区域

[0075] 40 其他存储区域

[0076] 44 传感器组件

[0077] 50 执行器组件

[0078] 56 数据线

[0079] 62 接口

[0080] 70 装置

[0081] 76 安全模块

[0082] 78 箭头

[0083] 80 按键开关

[0084] 82 监视模块

[0085] 84 箭头

[0086] 88 诊断缓冲器

[0087] 90 箭头

[0088] 92 箭头

[0089] 94 监视诊断缓冲器

[0090] 100 二进制输出

[0091] 102 二进制输出

[0092] 104 二进制输出

[0093] 108 二进制输出

[0094] 110 二进制输出

[0095]	112	双箭头
[0096]	116	控制模块
[0097]	120	开始
[0098]	126	判断
[0099]	132	方框
[0100]	134	判断
[0101]	136	方框
[0102]	138	方框
[0103]	140	方框
[0104]	142	结束
[0105]	150	开始
[0106]	152	方框
[0107]	154	判断
[0108]	156	方框
[0109]	158	方框
[0110]	160	判断
[0111]	162	判断
[0112]	164	方框
[0113]	166	判断
[0114]	168	方框
[0115]	170	方框
[0116]	172	判断
[0117]	174	方框
[0118]	176	方框
[0119]	178	判断
[0120]	180	方框
[0121]	182	判断
[0122]	184	方框
[0123]	186	结束
[0124]	188	判断
[0125]	190	方框
[0126]	192	方框
[0127]	194	开始
[0128]	196	判断
[0129]	198	方框
[0130]	200	判断
[0131]	202	方框
[0132]	204	方框
[0133]	206	判断

[0134] 208 方框

[0135] 210 判断

[0136] 212 方框

[0137] 214 方框

[0138] 216 判断

[0139] 218 方框

[0140] 220 方框

[0141] 222 结束

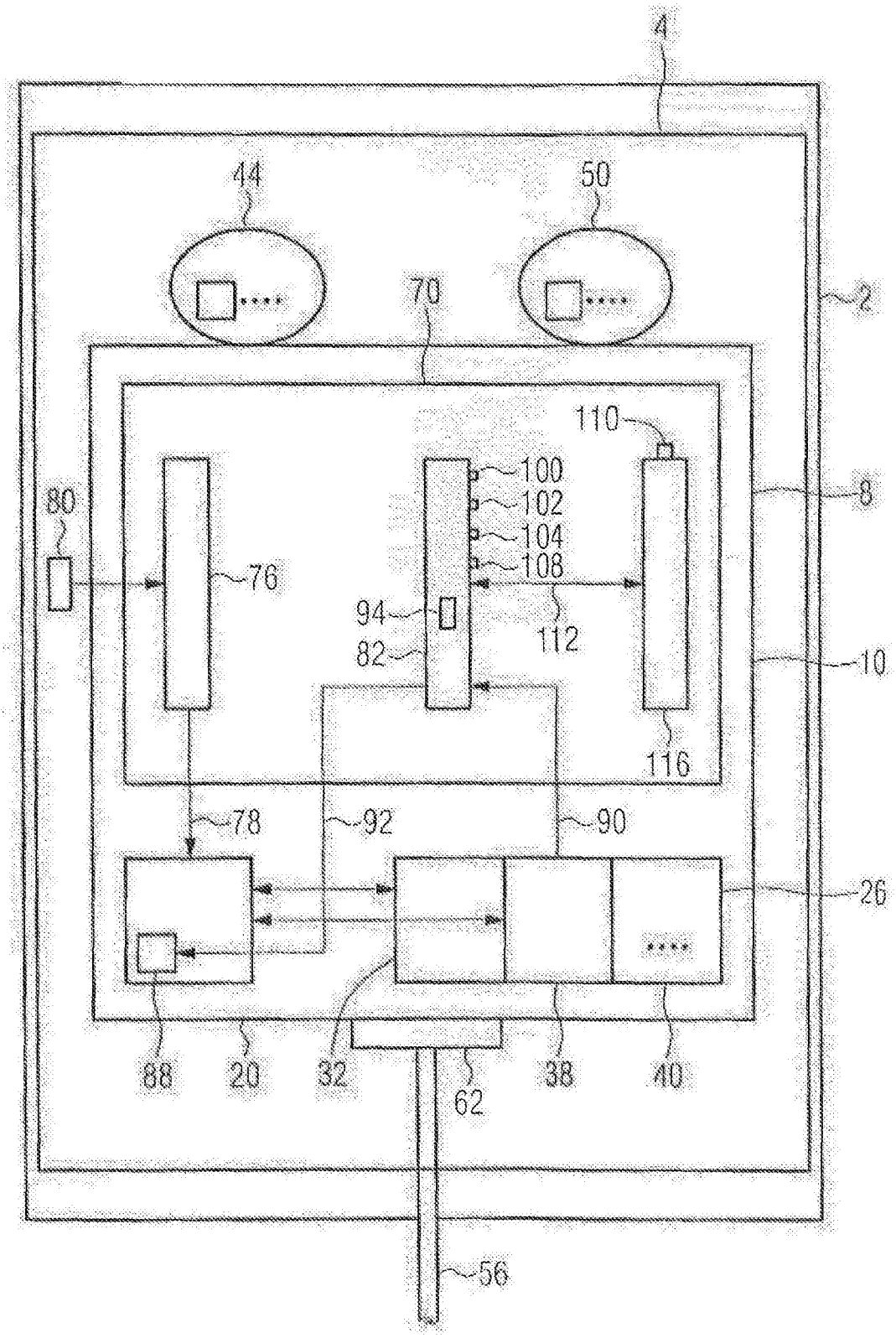

4
44
50
70
2
110
100
102
104
108
80
8
76
94
112
82
10
116
78
92
90
26
88
20
32
62
38
40
56

图1

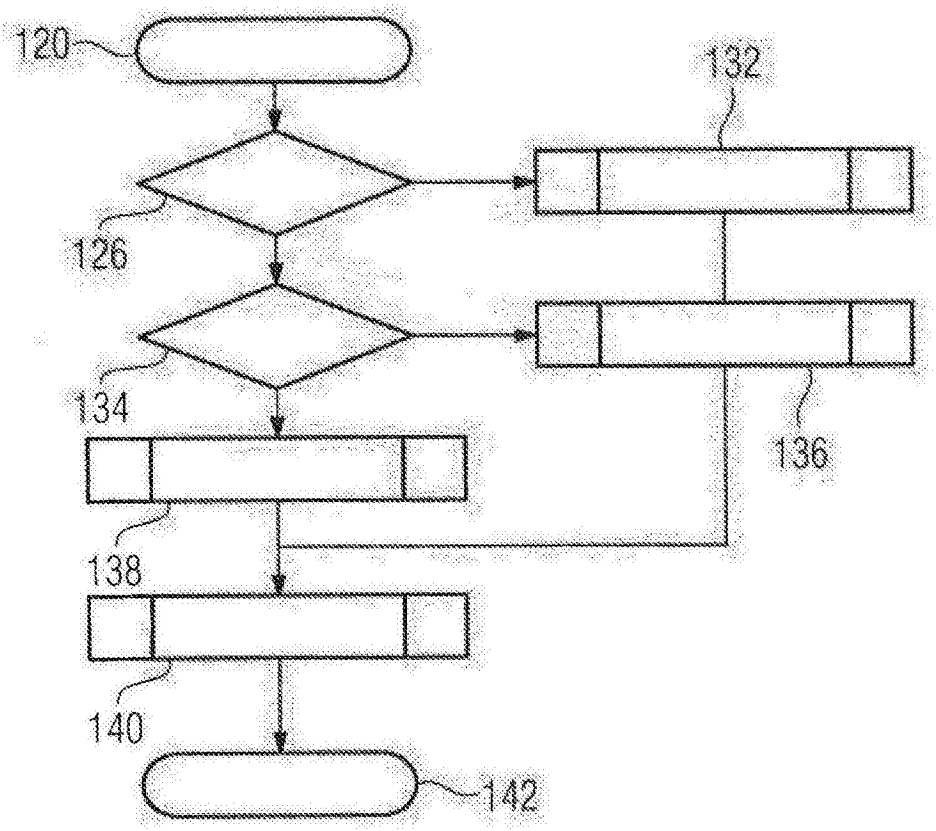


图2

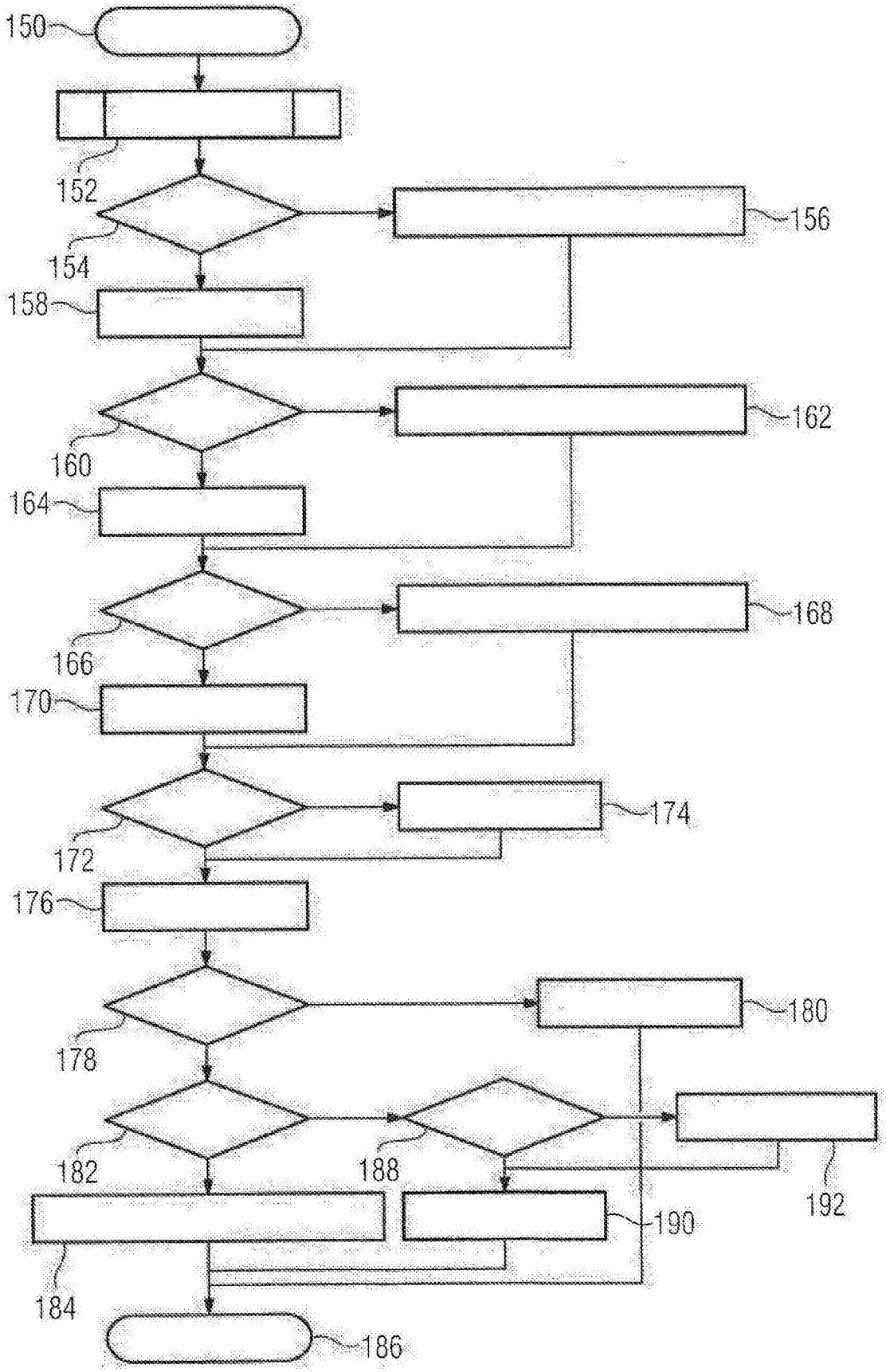

150
152
154
156
158
160
162
164
166
168
170
172
174
176
178
180
182
184
186
188
190
192

图3

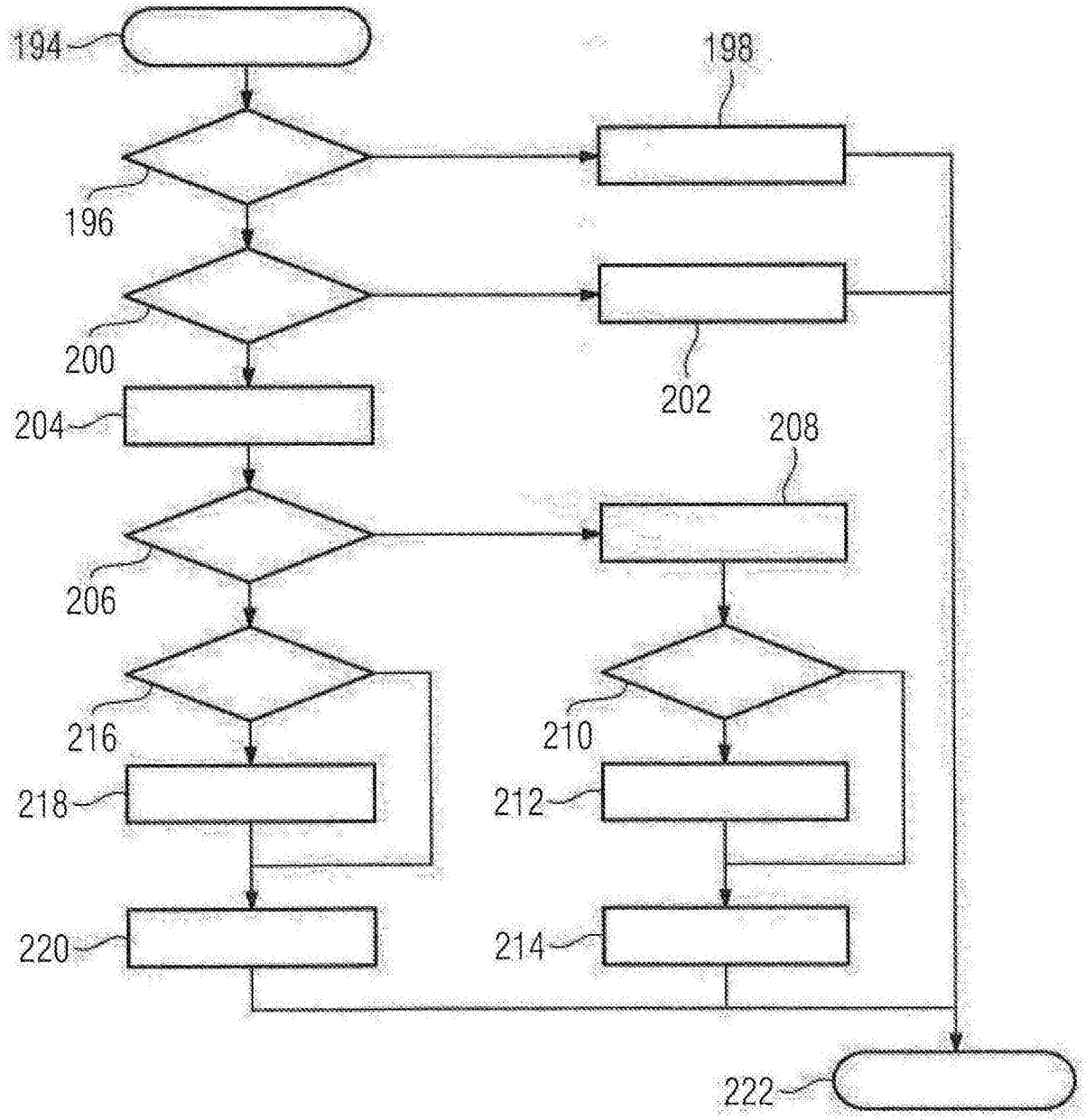


图4