(54) 发明名称
用于运行安全控制设备的方法

(57) 摘要
本发明涉及一种用于运行安全控制设备的方法。该方法具有下述步骤:提供多个计算单元(36, 38);检测输入信号,根据输入信号确定浮点值;根据浮点值确定输入区间;确定多个结果区间,其中借助于计算单元(36, 38)分别确定结果区间,并且其中计算单元(36, 38)构成用于分别将至少一个第一计算规则应用于输入区间,所述计算规则具有区间算术;当满足输出标准时,根据结果区间确定输出值;根据输出值确定输出信号;并且输出输出信号。
1. 一种用于运行安全控制设备（26,82,99）的方法，所述方法具有下述步骤：
   - 提供多个计算单元（36,38）;
   - 检测输入信号（162）；
   - 根据所述输入信号（162）确定浮点值（166）；
   - 根据所述浮点值（166）确定输入区间（172）；
   - 确定多个结果区间（196,198），其中借助于所述计算单元（36,38）分别确定结果区间（196,198），并且其中所述计算单元（36,38）构成用于分别将至少一个第一计算规则（194）应用于所述输入区间（172），所述计算规则具有区间算术；
   - 当满足输出标准时，根据所述结果区间（196,198）确定输出值；
   - 根据所述输出值确定输出信号（208）；以及
   - 输出所述输出信号（208）。

2. 根据权利要求1所述的方法，其特征在于，确定所述计算单元（36,38）中的至少一个的计算精度。

3. 根据权利要求2所述的方法，其特征在于，根据所述计算精度确定所述输入区间（172）的区间宽度。

4. 根据权利要求2或3所述的方法，其特征在于，当所述计算精度低于阈值时，执行至少一个反应步骤（60）。

5. 根据权利要求1至4之一所述的方法，其特征在于，确定所述结果区间（196,198）中的至少一个的结果区间宽度，其中当所述结果区间宽度超过最大宽度时，那么执行至少一个所述反应步骤（60）。

6. 根据权利要求1至5之一所述的方法，其特征在于，对所述计算单元（36,38）的所述结果区间（196,198）阶段性地检查区间交叠（204），其中当所述结果区间（196,198）中的至少一个位于另外的所述结果区间（196,198）之外时，那么执行至少一个所述反应步骤（60）。

7. 根据权利要求1至6之一所述的方法，其特征在于，借助至少一个计算单元（36,38）根据所述浮点值（166）确定结果值（214），其中分别将至少一个另外的第二计算规则（212）应用于所述浮点值（166），所述第二计算规则等价于所述第一计算规则（194）中的一个。

8. 根据权利要求7所述的方法，其特征在于，将所述结果值（214）与所述结果区间（196,198）中的至少一个相比较，其中当所述结果值（214）位于所述结果区间（196,198）之外时，那么执行至少一个所述反应步骤（60）。

9. 根据权利要求4至8之一所述的方法，其特征在于，所述反应步骤在所述计算单元（36,38）的至少一个中停止所述方法。

10. 根据权利要求4至9之一所述的方法，其特征在于，所述反应步骤（60）将所述计算单元（36,38）中的至少两个同步。

11. 根据权利要求1至10之一所述的方法，其特征在于，检测来自数据总线（104）所述输入信号（162）。

12. 根据权利要求1至11之一所述的方法，其特征在于，将所述输出信号（208）输出给所述数据总线（104）。

13. 根据权利要求1至12之一所述的方法，其特征在于，借助于所述输出信号（208）控
制用于机器（12,76）的安全相关的状态参数的执行器（62,64,94）。

14. 根据权利要求1至13之一所述的方法，其特征在于，将传感器（22,78）的传感器信号作为输入信号（162）来检测，所述传感器检测所述机器（12,76）的安全相关的状态参数。

15. 根据权利要求1至14之一所述的方法，其特征在于，能够接收紧急制动按钮（68）的开关信号。

16. 一种安全控制设备（26,82,99），所述安全控制设备具有多个计算单元（36,38），所述安全控制设备构成用于检测输入信号（162）；根据所述输入信号（162）确定浮点值（166）；根据所述浮点值（166）确定输入区间（172）；确定多个结果区间（196,198），其中借助于所述计算单元（36,38）分别确定结果区间（196,198），并且其中所述计算单元（36,38）构成用于分别将至少一个第一计算规则（194）应用于所述输入区间（172），所述计算规则具有区间算术；当满足输出标准时，根据所述结果区间（196,198）确定输出值；根据所述输出值确定输出信号（208）；并且输出所述输出信号（208）。
用于运行安全控制设备的方法

技术领域
[0001] 本发明涉及一种用于运行安全控制设备的方法。

背景技术
[0002] 安全控制设备通常用于监控工业中安全关键的区域并且在存在安全关键问题的情况下执行应对措施。典型地，安全控制设备与信号处理以交换信号的方式来分配并且另一方面与执行器以交换信号的方式来连接。用于安全控制设备的日常使用信号是紧急制动按键、保护门开关、双手开关、光栅和提供所监控的设备或机器设备的安全相关的信号的不同的传感器。因此，安全控制设备监控来自信号仪器的安全相关的信号并且评估所述信号。接下来，所述安全控制设备根据评估来产生用于控制执行器的控制信号。然后，所述控制信号典型地被控制，使其引起设备的安全状态。这例如能够通过失效安全地关断相应的设备来进行。替换的，或附加地，能够输出用于保护设备的报警信号。

[0003] 为了建立安全控制设备的尤其安全的运行能力，所述安全控制设备典型地制造为具有冗余组件的。例如，安全控制设备因此具有两个或多个计算单元，所述计算单元并行地处理相同的任务。为了改进安全运行能力，多样化地设计组件以及由组件处理的软件组件，由此能够补偿内部的系统错误。为此例如能够提出：计算单元来自不同的制造商并且具有不同的体系结构。重要的是，可以比较来自不同计算单元的两个或多个结果，所述结果以不同的方式基于相同的输入数据来确定。如果所述结果不一致，那么在安全控制设备之存在安全相关的错误。能够通过执行适当的反应步骤来实现安全控制设备对这种错误的反应。例如，能够输出报警信号和/或关断设备。也能够考虑的是，将控制任务移交给次级安全控制设备。

[0004] 如果安全控制设备具有多于两个冗余组件，那么在比较结果时能够进行多数决定法。由此实现，当仅在一个组件中存在内部错误时，控制任务能够继续进行。如果仅提供两个组件，那么通常进行自动的应对措施。其结果是，大多数情况下需要通过机器操作员对相关设备进行手动干预。

[0005] 实现冗余构成的安全控制设备的前提条件是组件之间的计算结果的可比较性。为了能够确保所述可比较性，在安全控制设备中能执行整数运算。整数能够精确地表现在数字数据处理中，并且在应用整数时的存储耗费仅是很低的。这同样适用于基础的计算类型，例如加法、减法、乘法和结果还必须是整数的整数除法。此外，整数算术遵循基础的代数法则，例如结合律、分配律和交换律。因此，仅进行整数运算的算法相对于置换操作符（Operatoren）的算法是稳定的进一步鲁棒的。

[0006] 在此不利的是，安全控制设备限制于整数运算。由此降低了结果的精确性，因为输入信号仅能够表现为整数而在于大多数情况下必须被取整成整数。

[0007] 为了改进计算精度，从计算机技术的领域中已知：使用浮点数。浮点数（也称作Gleitpunktzahl或Fließkommazahl）是实数的近似表示形式。浮点数与从计算机代码中已知的定点数不同。在浮点数中存储有受限的数位序列、尾数，其中在固定位置上采用小数
点。该尾数与另一表达形式相乘，所述表达形式由一个底数组成并且具有指数。底数的数值典型地经由协定协调一致。指数暗示地说明小数点的实际位置。浮点数的应用能够地容易简单地以小的存储耗费表示极其大以及极其小的数字。这根据乘法的展式情况及使用情况容易计算。浮点数的应用能够允许与整数计算情况相比能够实施明显更精确地和更复杂的运算。在此，最佳地利用计算单元的存储器，使得确保最大可能实现的精度。

为了借助浮点数进行运算，从数字数学中已知特殊的浮点数算法。在该浮点数算法中，基础代表法则部分地是不适用的，因为代表法则由于在小数点处操作符号的方向且由于浮点数是有符号的，所以受到损害。为了说明而提出下述（简化的）示例：

表达式 $0.125+4.5-4.0$ 由十进制数组成并且应当借助于浮点数变换算式二进制系统。表达式进而所指示的十进制数在二进制系统中具有有限的表示方式：

$0.001+100.1-100.0$。

如果提供四个位用于显示二进制数，那么能够完整地表示所有十进制数。在使用括号的情况下，得出下述运算：

$(0.001+100.1)-100.0=100.1-100.0=0.1$

如果不同地放置括号，那么得到具有不同结果的下述运算：

$0.001+(100.1-100.0)=0.001+0.1=0.101$

如所示出的那样，括号的选择在二进制系统中得到不同的结果，而将括号相应地应用到具有十进制数的表达式时则不对结果产生影响。

此外，许多十进制数值作为二进制数值不具有有限的表示方式。因此，以有限大小的数据类型存储在大多数情况下要求对可显示的数值进行取整。此外，如乘法或除法的运算能够提高用于精确显示所需要位数的数。多频繁进行取整以及在此形成何种取整错误，基本上取决于应用浮点运算的算法的实施方式。由此可见；在具有多种硬件和软件组件的冗余的实施方式中，不能够确保运算结果的可比较性。因此，利用浮点数的自动化的情况下，存在根据具有潜在不受限的错误的数据进行控制的可能性。安全的自动化以这种方式是不可行的。

可以设想的是，通过下述方式产生可比较性；不使用多种硬件或软件或者将多种硬件和软件彼此协调成，使得必须实现完全相同的计算结果。然而，在多种硬件和软件中的完全相同的计算结果将不以完全相同的顺序、以完全相同的精度和以相同的取整方法尤其相对于其时间点和取整方向来执行运算时才是能够预期的。然而，无论是计算精度还是顺序都不能够被可靠地确定，因为可用的编译器和计算单元在这方面显著地彼此不同。因此，相应的安全控制设备必须冗余地配备有不同的硬件组件和软件组件。然而，这与安全自动化的基本思想相冲突，因为刚好通过多种硬件和软件实现极其高的安全性。

同样能够设想的是，浮点数能够通过定点来取代进而能够应用定点算术。定点算术又能够借助整数算术来实现。然而在相同精度的情况下导致极其高的存储需求，这是不经济且不实用的。

此外，在所述方案中运算结果的精度变差，因此还可能基于任意有错的数据来实施控制。因此，没有消除在将浮点算术用在安全的自动化中时的主要缺点。
发明内容
[0019] 因此，本发明的目的是，提供一种用于运行安全控制设备的方法，所述方法提高了安全控制设备的精度并且同时保持安全性。
[0020] 所述目的根据本发明的一个方面通过开始所述类型的方法来实现，其具有下述步骤：
[0021] - 提供多个计算单元；
[0022] - 检测输入信号；
[0023] - 根据输入信号确定浮点值；
[0024] - 根据浮点值确定输入区间；
[0025] - 确定多个结果区间，其中借助于计算单元分别确定结果区间，并且所述计算单元构成用于，分别将至少一个第一计算规则应用于输入区间，所述计算规则具有区间算术，
[0026] - 当满足输出标准时，根据结果区间确定输出值，
[0027] - 根据输出值确定输出信号，并且
[0028] - 输出所述输出信号。
[0029] 根据本发明的另一方面，所述目的通过具有多个计算单元的安全控制设备来实现。所述安全控制设备构成用于检测输入信号；根据输入信号确定浮点值；根据浮点值确定输入区间；确定多个结果区间，其中借助于计算单元分别确定结果区间，并且所述计算单元构成用于，分别将至少一个第一计算规则应用于输入区间，所述计算规则具有区间算术，当满足输出标准时，根据结果区间确定输出值；根据输出值确定输出信号；并且输出输出信号。
[0030] 因此本发明基于下述思想：在计算单元中分别应用第一计算规则，所述第一计算规则使用区间算术。其分析了允许能够安全地处理浮点数并且接下来进行比较的公差范围。由此在实施计算规则时提高安全控制设备的精度，因为取整错误在数值方面保持为小的。此外，在检测输入信号时相对于整数运算提高了精度，因为输入信号能够映射为浮点值来代替整数。此外，能够输出更精确的输出信号。
[0031] 计算单元优选构成为微控制器。在优选的设计方案中，在安全控制设备中使用多种类型的多个不同的计算单元。其例如能够是不同结构类型的。由此得出在对输入信号进行取整处理时以及在对输出信号进行冗余处理时的极其高的安全性。
[0032] 区间算术的应用尤其能够实现，能够使用多种硬件和软件，因为其将区间作为结果来确定。即使计算单元的结果彼此不同，不同计算单元的结果区间现在能够相互比较。
[0033] 区间算术是能够实现借助数值得到范围来替代借助各个数值得到计算的方法。开始所述的问题，即必须对浮点数进行多次取整通过下述方式来解决：浮点值形成具有区间上限和区间下限的输入区间。浮点值的精确的数值位于区间边界之间。区间算术提供匹配的计算类型，借助于所计算类型能够安全地且精确地借助输入区间来计算。在此进行的取整通过以下方式来考虑：根据取整来自动地扩大或缩小区间使得结果区间包含精确的结果值。因此，区间算术被理解为使用区间作为操作数（Operand）的方法。
[0034] 适当的方法例如从下面的文献中已知，在此全面地参考下述文献：

6
and Image Processing, 1993;
[0036] De Figueiredo, Luiz Henrique; Stolfi, Jorge, Self-Validated Numerical Methods and Applications, Brazilian Mathematics Colloquium Monograph, IMPA, Rio de Janeiro, Brazil, 1997;
[0038] Neumaier, Arnold, Taylor Forms—Use and Limits, Reliable Computing, 9, 2002;
[0039] Sengupta, Atanu; Pal, Tapan Kumar; Theory and Methodology: On comparing interval numbers, European Journal of Operational Research, 127, 2000; and

[0041] 输入信号优选与信号仪器关联。根据输入信号确定浮点值。当输入信号是模拟信号时，这例如能够通过 A/D 转换器进行。然后，借助于浮点值确定包含浮点值的输入区间。区间的宽度能够以不同的方式和方法确定，进而确定区间上界和区间下界的数值。在此，浮点值应当包围得尽可能窄，以便实现高的精确度。一个可行性是，预设固定的区间宽度，所述区间宽度例如从存储器中读出。区间宽度在优选的设计方案中能够根据输入信号的公差值来确定。所述公差值例如从传感器的测量错误的和 / 或从 A/D 转换器的精度中得出。

[0042] 在优选的设计方案中，通过安全控制设备检测并且以相应的方式进一步处理多个输入信号。此外，优选提出，当不能够精确地或者仅在高的存储消耗的情况下精确地映射另外的所需要的控制数据时，另外的所需的控制数据对于计算单元而言同样映射为区间。这种操作数例如能够是所需的变量值和用于第一计算规则的常数。

[0043] 在多个计算单元中至少将第一计算规则应用于输入区间的。第一计算规则例如能够作为软件实施但是也能够以硬件的形式实施。计算规则优选具有多个计算运算，所述计算运算例如连续地被处理。计算规则也能够是上级规则的一部分，例如各个程序例程或程序模块。第一计算规则应用区间算术，使得确定结果区间。在此，结果区间的宽度尤其与基于区间算术的自验证特性而进行的错误估计相关。因此，优化了相应的结果区间的区间宽度，以便说明应存在精确值的最小可能的区间。

[0044] 在多个计算单元的情况下，优选地，每个计算单元具有第一计算规则的自身的实现方案，以便遵守多种原理。不同的计算单元的第一计算规则在此彼此等价，以便确保可比较性。然而，其优选不是相同的，由此得出：不同计算单元的结果区间具有不同的数值。所述数值现在能够相互比较，因为不需要精确地一致，而是部分一致就已足够，例如在存在相交区间的情况下。

[0045] 为了通过计算单元实施进一步的、后续的第一计算规则，例如能够进一步处理相应的结果区间或者例如能够基于不同的结果区间进一步处理相交区间。通过在计算单元之内进一步处理相交区间，所述计算单元自动地彼此同步。这具有降低结果区间的区间宽度进而提高计算精度的优点。

[0046] 因此，当满足相应的输出标准时，安全控制设备才输出信号。具体的输出标准与安全控制设备的任务相关。当结果区间中的一个具有预设的值时，输出标准才例如能够被满足。选定地或附加地也能够考虑，当执行完预设的第一计算规则时，才满足输出
标准。也能够考虑的是，当不存在相交区间时，才满足输出标准。在该情况下优选提出：确定替代值，例通过对各个结果区间取平均值来进行。这也能够通过加权地取平均值来进行。如果满足输出标准，那么根据至少一个输出区间来确定输出值，也就是说，确定具体的数值，所述数值优选表示为浮点数，以便保持计算精度。

[0047] 输出信号接下来根据输出值来确定。这个优选在安全控制设备和相应的外围设备之间的接口之间进行。例如能够通过D/A转换器来实现。在此，得到输出值的高精度能够出现在输出所述输出信号时的高的精度的优点。

[0048] 在优选的设计方案中，以冗余的方式执行另外的方法步骤。此外能够考虑的是，在所述计算单元中执行另外的或全部方法步骤。

[0049] 因此总体上得到下述可行性：极其准确地在安全控制设备之内进一步处理输入信号并且以极其高的精度确定输出信号。在此，保持安全自动化的基本概念，使得能够实现高精度的且极其安全的自动化。

[0050] 因此，本发明的目的被完全实现。

[0051] 在本发明的一个优选的设计方案中，确定计算单元中的至少一个的计算精度。

[0052] 在该设计方案中，确定计算精度，计算单元中的一个以所述计算精度确定相应的结果区间。尤其能够应用计算错误作为计算精度的度量。

[0053] 计算精度例如能够通过下述方式确定：监控冗余步骤并且确定其对于结果区间的影响。此外，能够考虑的是，在此考虑近似的计算方法，如多种数字的计算方法的精度。

[0054] 此外，区间算术的使用提供将结果区间的精度作为计算精度的可行性进而极其简单地确定输出值的精度。这优选通过确定区间宽度来执行。因此，能够评估相应的结果区间的精度。

[0055] 在此有利的是，能够使用已知的计算精度，以便确定安全控制设备是否处于安全运行中。例如，结果区间的/或输出信号能够根据计算精度来调整。这也能够实现以浮点数安全地运行安全开关设备，所述安全开关设备仅具有唯一的计算单元，因为根据计算精度能够避免存在错误的输出信号。

[0056] 在本发明的另一设计方案中，根据计算精度确定输入区间间的区间宽度。

[0057] 在本发明的该设计方案中，为了产生输入区间自动地确定进而形成区间的情况下考虑区间宽度。根据计算精度调整区间宽度。例如能够分析已经执行的计算规则并且确定最佳的区间宽度。在此有利的是，区间宽度动态地匹配于当前的输入信号，使得持续地优化计算精度。

[0058] 在本发明的另一设计方案中，当计算精度低于阈值时，执行至少一个反应步骤。

[0059] 在该设计方案中，当不能保证需要用于安全运行的计算精度时，那么执行至少一个应对措施。因此，该应对措施以反应步骤的形式执行。该反应步骤是方法的另一步骤。该反应步骤能够作为确定的预设的应对措施进行或者也根据当前的结果区间作为应对措施来进行。当计算精度低于预设的阈值时，才进行该反应步骤。因为计算错误是计算精度的度量，所以当预设错误超过预设的错误阈值时，这等同于上述内容。在此有利的是，检查安全控制设备的安全运行并且主动地进行保护。

[0060] 例如能够将满足输出标准设为反应步骤。此外，能够提出，然后根据预设的数值或者根据另外的计算单元的结果区间来确定输出值。
[0061] 在另一设计方案中，确定结果区间中的至少一个的果结果区间宽度，其中当结果区间宽度超过最大宽度时，就执行至少一个反应步骤。

[0062] 在该设计方案中，通过监控结果区间宽度，即结果区间中的至少一个的区间宽度来附加地保护安全控制设备。最大宽度降低能够作为预设的数值存在。替选地或附加地能够考虑的是，结果区间与具有最大宽度的基准区间进行比较。因此优选地提出，基准区间基于输入区间或基于之前的果结果区间来确定。尤其提出，因此根据输入区间的区间宽度来确定最大宽度。此外，最大宽度能够替选地或附加地根据期望值、经验值、测量精度和/或计算精度来确定。

[0063] 如果结果区间的区间宽度超过最大宽度，那么执行至少一个反应步骤。在此有利的是，极其有效地排除安全关键的错误，所述错误可能通过计算规则的特定次序导致具有任意宽的区间宽度的结果区间。因此，安全控制设备的安全性整体上被进一步提高。

[0064] 本发明的另一设计的计算单元的区间宽度根据区间有性定性地检查区间交叠，其中当结果区间中的至少一个位于另外的果结果区间之外时，就执行至少一个反应步骤。

[0065] 在该设计方案中，反复地将结果区间进行相互比较。确定例如能够作为相交区间来计算的区间交叠。相交区间因此包含两个不同计算单元的至少两个结果区间的共同集合的数值。替代地能够考虑，实施区间交叠的比较。因此以有效的方式提供能够使用结果区间的可比较性进而检查安全开关设备的安全性的可行的可行性。

[0066] 在优选的实施方案中，以规则的间距确定区间交叠，使得尤其良好地确保安全控制设备的安全的且正确的运行。这例如能够以预设的时间间隔来进行或者也在执行完第一计算规则的特定的计算步骤之后进行。

[0067] 例如能够将满足输出标准设为反应步骤。此外，能够提出，然后根据预设的数值或者根据另外的计算单元的区间宽度确定输出值。

[0068] 在本发明的另一设计方案中，指定至少一个计算单元根据浮点数值来确定结果值，其中分别将至少一个另外的、第二计算规则应用于浮点值，所述第二计算规则等价于第一计算规则中的一个。

[0069] 在该设计方案中，执行完两个计算规则，这与第一计算规则并行地实施。优选地，这除第一计算规则之外在计算单元中的一个中进行。第一和第二计算规则彼此等价，其中第一计算规则应用区间算术并且处理区间，并且其中第二计算规则优选具有替选的算术并且以具体的数值工作。所述替换的算术例如能够是浮点算术或定点算术。等价在此表示：第二计算规则执行相对于第一计算规则相同的步骤或等同的步骤。

[0070] 因此，在计算单元中借助于第一计算规则能够确定类似的果结果区间。第二计算规则能够实现：能够根据结果值检测第一计算规则的结果。在此有利的是，能够检查结果区间并且基于结果值对所述结果区间附加地进行限制，使得避免过大的结果区间而避免不准确的结果区间。在此，另外的优点是，存在准确的结果值并且同时通过结果区间确保结果的可比较性，这使安全开关设备的运行更加准确和安全。

[0071] 此外，根据结果值能够确定应用于另外的第一计算规则的区间。为此优选地根据结果区间确定相应的数值，所述数值与结果值相等特定的量值。然后，为了形成后续的区间能够采用该量值，以便限定区间上限和区间下限，其中以高精度的结果值为基础并且为区间上限将该量值加到结果值上或者为区间下限将该量值减去。在此有利的是，更加简单且
更安全地运行安全控制设备。

[0072] 在本发明的第一设计方案中，将结果值与结果区间中的至少一个进行比较，其中当结果值位于结果区间之外时，实施至少一个反应步骤。

[0073] 在该设计方案中，结果区间附加地通过结果值来验证。为此，来自第二计算规则的
结果值优选地与另一计算单元的结果区间进行比较。换言之，将结果区间和结果值“交叉地”进行比较。在此，结果值必须位于相应比较的结果区间之内，因此存在安全运行。如果这不是这种情况，那么执行反应步骤。

[0074] 在本发明的第一设计方案中，反应步骤在计算单元的至少一个中停止所述方法。

[0075] 在该设计方案中，作为反应步骤而停止方法。此外，例如当多个计算单元还能够确保冗余运行时，这能够在仅一个计算单元中进行。替换地，也能够将整个安全控制设备在其运行时停止。

[0076] 此外，在优选的方案中提出，那么满足输出标准。在另外的优选的方案中，然后输出预设的输出信号，即确保由安全控制设备所控制的活动的安全状态。

[0077] 在此有利的是，基于可能的错误的输出信号的机器的控制被有效地解除。

[0078] 在本发明的第一设计方案中，反应步骤将计算单元中的至少两个同步。

[0079] 在该设计方案中，将计算单元同步到共同输出上作为反应步骤来进行，所述数值应当以另外的运作为基础。在此，例如能够将输入区间、结果区间或针对重复的计算规则提交的数值进行同步。由此有利地实现：在处理安全控制设备时检查安全设备本身，进而确保更高的安全性。

[0080] 为了完整性起见，需要指出的是，反应步骤的不同的起因也能够引起不同地构成的反应步骤。同时也能触发多个不同的反应步骤。

[0081] 在本发明的一个设计方案中，检测来自数据总线的输入信号。

[0082] 在该设计方案中，安全控制设备接收来自数据总线的输入信号，即以数字的形式接收。由此实现，安全控制设备例如能够与输入模块连接。然后，输入模块从相应的信号仪器读取数据并能够将所述数据转换成数字形式。特别地，得出下述可能性：输入信号本身已经以浮点数的形成转给安全控制设备。在这种情况下，输入信号能够直接地相应于浮点值。

[0083] 从这个优点是，能够实现具有安全控制设备的布置的模块化结构，其中安全控制设备能够与不同的输入模块共同工作。由此形成模块化的结构，并且安全控制设备能够通过调整输入模块而以更简单的方式与不同的信号仪器连接。

[0084] 在另一设计方案中，将输出信号输出至数据总线。

[0085] 在该设计方案中，安全控制设备将输出信号发送到数据总线，即以数字的形式发送。由此实现，安全控制设备例如能够与输出模块连接。输出模块然后将信号发送至相应的执行器，所述信号控制机器的安全相关的调节变量。特别地，存在下述可行性：输出信号本身以浮点数的形式被转发给执行器。在该情况下，输出值能够直接相应于输出信号。

[0086] 从这个优点是，能够实现具有安全控制设备的布置的模块化结构，其中安全控制设备能够与不同的输出模块共同工作。由此形成模块化的结构，并且单独的安全控制设备能够通过调整输出模块而以简单的方式与不同的执行器连接。

[0087] 例如能够使用 CAN 总线（CAN-BUS）或安全总线（Safety-BUS）作为数据总线。
本发明具有下述优点：所述 CAN 总线通常在工业中可进而能够实现实时控制设备的经济的实施方案和兼容性。安全总线具有专门为安全相关的目的的体系结构的优点，使得通过使用安全总线而实现运行的尤其高的安全性。

在另一设计方案中，借助于输出信号来控制用于机器的安全相关的状态参数的执行器。

在该设计方案中，将高精度的输出信号用于极其准确且安全地控制机器。根据要控制的机器，能够考虑将例如温度、压强、转速或空间位置（例如在铣床中的刀具位置）作为状态参数。在此的优点是，不仅能够监控安全关键的系统，而且也能够高度精确地进行控制。

在另一设计方案中，将传感器的传感器信号作为输入信号检测，所述传感器信号检测机器的安全相关状态的参数。

在该设计方案中，输入信号相应用于机器的状态参数。由于高的精度，状态参数能够直接在安全控制设备之内被进一步处理。在一个尤其优选的设计方案中，借助于用于机器的状态参数的执行器根据所检测到的状态参数进行机器的调节。

优选地，能够考虑匹配于状态参数的传感器作为传感器，例如温度传感器、压强传感器、转速传感器和/或位置测量传感器。

在另一设计方案中，能够接收紧急制动按健的开关信号。

在该设计方案中，紧急制动按键与安全控制设备连接。紧急制动按键的开关信号由安全控制设备接收。这能够用于：满足输出标准。这意味着，按下紧急制动按健而触发开关信号，然后输出所述输出信号。替换地或附加地能够考虑，在检测紧急制动按键的开关信号时，根据预设的数值来确定输出值，使得设定所控制的机器的已知的且限定的状态。

不言而喻，上面提到的和下面还要阐明的特征不仅能够以分别说明的组合的形式应用，而且也能够在其他组合或单独地应用，而不会偏离本发明的范围。

**附图说明**

本发明的实施例在附图中示出，并且在下面的说明中详细阐明。附图示出：

图 1 示出第一机器设备中的安全控制设备的第一实施例的示意图；

图 2 示出第二机器设备中的安全控制设备的第二实施例的示意图；

图 3 示出第二机器设备中的安全控制设备合体数据总线的第三实施例的示意图；

图 4 示出根据本发明的方法的一个优选的实施例的流程图；

图 5 示出图 4 中的流程图的一部分，其中附加地确定计算精度；

图 6 示出图 4 中的流程图的一部分，其中附加地确定结果值；

图 7 示出信号曲线的示意图，其中确定冗余的结果区间和/或值；

图 8 示出信号曲线的示意图，其中附加地确定结果值。

**具体实施方式**

在图 1 中示出整体在附图标记 10 标识的具有新型的安全控制设备一个实施例的设施。设施 10 在此例如包括机器人 12，所述机器人在工作运行时的运动对于停留在机器人 12 的工作区域中的人员而言构成危险。出于该原因，借助具有防护门 16 的防护围栏 14 来
保护机器人 12 的使用范围。保护门 16 例如为了维护工作或为了安装工作能够实现通到工作区域中的入口。在正常工作运行时，机器人 12 应当仅在保护门 16 关闭时才工作。一旦保护门 16 被打开，那么机器人 12 必须被断开或者以其他的方式来置于安全状态下。

【0107】为了检测保护门 16 的状态，将保护门开关 18 安装在保护门 16 上，所述保护门开关具有门部件 20 和框架部件 22。框架部件 22 在线路 24 上产生保护门信号，所述保护门信号经由线路 24 作为输入信号被送给安全控制设备 26。

【0108】安全控制设备 26 具有带有多个设备接口的输入单元 28，其中线路 24 经由设备接口中的一个与输入单元 28 连接。此外，为了产生输入信号提供，输入单元 28 与信号线路 30 连接，经由所述信号线将在脉冲信号发送给框架部件 22。在电路 24 上的输入信号在输入单元 28 中转换成浮点值。浮点值是数值值，所述数值值以浮点数的数据类型显示。经由信号线路 32 和 34，将浮点值转换给计算单元 36 和 38。计算单元 36 和 38 分别构成为一个微控制器。在此，其为不同结构类型的微控制器，使得存在多样的硬件结构。在计算单元 36 和 38 之内分别根据浮点值形成输入区间。接下来，在每个计算单元 36 和 38 中单独地执行第一计算规则。在计算单元 36 和 38 之内使用的计算规则都以多样的方式实现，使得由此确保其极高的安全性。

【0109】能够显示中间结果或最终结果的结果区间经由箭头 40 和 42 转发给比较单元 44 和 46。比较单元 44 和 46 此外经由箭头 48 和 50 获得其他计算单元 36 或 38 的相应的结果区间。在比较单元 44 和 46 之内，也将结果区间相互比较。如果结果区间小，则检查是否满足输出标准。当结果区间包含相应于打开的保护门 16 的同一数值时，那么在此就满足输出标准。

【0110】在所述出的情况下，当门 16 打开时，那么就发送输出信号。在该情况下，比较单元 44 和 46 分别确定输出值。输出值在此对应于晶体管 52 或 54 的充足的供电。因此所述晶体管根据输出值产生输出信号，所述输出信号经由输出线路 56 和 58 能够被冗余地输出。此外，计算单元 36 和 38 能够相互同步，这通过双箭头 60 显示地示出。同步能够规则地进行和/或作为对相应的起因的反应步骤进行。输出信号经由线路 56 和 58 引导至保护器 62 和 64，所述保护器根据输出信号中断机器人 12 的电源 66。

【0111】经由输入单元 28 将安全控制设备 26 借助于线路 70 和 72 附加地与紧急制动按键 68 连接。如果操作紧急制动按键 68，那么经由线路 72 将开关信号转发给安全控制设备 26。如果接收到所述开关信号，那么所述开关信号由计算单元 36 和 38 本身识别并且直接满足输出标准。在该实施例中，然后将输出值自动地设置为预设值，以用于对晶体管 52 和 54 充足地供电，以至于保护器 62 和 64 中断电源 66。

【0112】图 2 示出整体用附图标记 74 标识的具有安全控制设备的另一设备。设备 74 具有自动马达 76，所述自动马达的转速通过转速传感器 78 来检测。关于转速的信息经由线路 80 转发给安全控制设备 82，所述安全控制设备调节转速。安全控制设备 82 具有输入单元 28，所述输入单元对应于图 1 中的输入单元 28。此外，设有如图 1 中示出的具有线路 70 和 72 的紧急制动按键 68。来自输入单元 28 的浮点值经由线路 32 和 34 转发给计算单元 36 和 38。通过计算单元 36 和 38 确定的结果区间经由线路 84 和 86 转发给单独的比较单元 88。比较单元 88 检查，在结果区间之内是否存在区间交叠。

【0113】如果这是这种情况，那么确定输出值。这例如能够通过对于一个或多个结果区间取
平均值或取加权平均值来进行。如此形成的输出值由经 D/A 转换器形式的输出单元 90
以及经由输出线路 92 转发给功率电子装置 94。功率电子装置 94 接收输出信号并且根据输出
信号产生控制信号，所述控制信号经由线路 96 转发给电动马达 76。
【0114】 如果不存在区间交叠，那么根据两个结果区间通过取平均值来确定替代值并且将
所述替代值转发给输出单元 90。同时，计算单元 36 和 38 经由箭头 60 相互同步。
【0115】 选地或附加地提出，当不存在区间交叠时，那么满足输出标准。在该情况下，输
出值优选设定为预设值，所述预设值例如能够是转速 0 或是低的且安全的转速。因此，当结
果区间不至少部分一致时，那么电动马达 76 被关断或者转到稳定状态下。
【0116】 如果按压紧急制动按键 68，那么设施 74 相应地转入安全状态下。
【0117】 图 3 时出整体附图标记 98 标识的另一设施。其与图 2 中的设施 74 的不同之处
在于，在控制设备 99 与外部的输入模块 100 和外部的输出模块 102 共同作用。
【0118】 在该实施例中，输入模块 100 接收线路 80 上的信号并且将其转换成数字信号，所
述数字信号经由安全总线 104 作为输入信号转发给安全控制设备 99。输出信号作为数字值
以相应的方式经由安全总线 104 转发给输出模块 102，所述输出模块将控制信号经由线路
92 转发给功率电子装置 94。
【0119】 输入模块 100 根据来自线路 80 的信号确定呈浮点数形式的数值。数值经由安全
总线 104 来转发。因此，来自线路 80 的信号能够被尤其准确地评估并且由安全控制设备 99
处理。此外，数值作为呈浮点数形式的输出信号经由安全总线 104 转发给输出模块 102，得
使所述输出模块能够输出高度精确的信号。由此得到用于具有安全控制设备 99 的用于
控制和/或调节设施 98 的系统的模块化结构。因此，安全控制设备 99 能够使用在不同的
设施中，其中根据对信号仪器和执行器的要求能够选择相应的模块。
【0120】 图 4 时出整体附图标记 105 标识的流程图。流程图 105 描述根据本发明的方法
的一个实施例。
【0121】 在一个步骤 106 中，由安全控制设备接收输入信号。这例如能够是数字的或模拟
的输入信号。
【0122】 在步骤 108 中，确定作为浮点数示出的浮点值。浮点值的具体数值在此从输入信
号中得出，其中，所述数值在模拟输入信号中例如能够通过 A/D 转换器来确定。
【0123】 在步骤 110 中，根据浮点值来确定至少一个输入区间。为此，限定区间上限和区间
下限，其中浮点值位于两个区间边界之间。区间边界距浮点值的间距能够以不同的方式来
限定。在此，这通过从存储器中读出的预设值来进行。此外，在步骤 110 中限定另外的区间，
所述区间是必要的，以便为稍后的计算准备附加的操作符。
【0124】 此外能够考虑的是，冗余地进行输入区间的确定，使得根据一个浮点值能够彼此
并行地确定不同计算单元中的两个输入区间。
【0125】 输入区间在并行运行的步骤 112 和 114 中被进一步处理。在此，计算单元分别确
定结果区间，所述结果区间在此为了更好的区分而称为结果区间 I 和结果区间 II。结果区
间 I 和 II 通过第一计算规则根据输入区间和根据附加的参数来确定。
【0126】 结果区间 I 和 II 转发给另一步骤 116。在步骤 116 中确定区间交叠，例如以相交
区间的形式。这能够通过简单的集合运算来进行。
【0127】 区间交叠传递给另一步骤 118。所述步骤检查：是否存在区间交叠。如果存在区间
说明

交叠，那么在一个后续步骤 120 中检查；该区间交叠是否满足输出标准。如果区间交叠或替选地结果区间间满足输出标准，那么根据区间交叠或结果区间间在步骤 122 中确定输出值。所述输出值在此通过确定区间交叠来计算。由此再次得出浮点数作为输出值。

[0128] 根据浮点数，在另一步骤 124 中产生输出信号。这例如能够通过 D/A 转换器来进行。

[0129] 最后，在步骤 126 中进行将输出信号输出给外围设备，所述外围设备与安全控制设备以交换信号的方式连接。

[0130] 当通过区间叠加不满足输出标准时，从步骤 120 起循环状地经过步骤 128 进行另一个第一计算规则的过程。因此确保，在步骤 112 和 114 中的第一计算规则进行完之后定期确定：结果区间是否提供类似的结果并且同时不中断复杂程序的进行，所述复杂程序由第一计算规则的次序构成。

[0131] 当不存在区间叠加时，那么从步骤 118 起转至步骤 130。在步骤 130 中，作为反应步骤确定替代值，这例如通过对结果区间 I 和 II 取平均值来进行。然后，将所述数值返回给计算单元，其中作为另外的反应步骤进行同步 60。替代值或叠加值能够考虑，替代值经由在此虚线示出的箭头 132 输出给步骤 120。因此，在步骤 120 中可见，其为替代值而不存在区间交叠。根据所述信息，能够实施不同的另外的反应步骤。反应步骤是满足选择标准的反应步骤。此外，在步骤 122 中应用替代值以用于确定输出值。作为替选方案的是，能够考虑停止安全控制设备或方法。

[0132] 附加地指出，在步骤 134 中检测紧急制动按钮 68 的紧急制动信号。所述紧急制动信号被递给给步骤 120，所述紧急制动信号在那里能够满足输出标准。通过紧急制动信号满足输出标准又能够具有不同的结果。一方面，能够由此强制输出瞬时的输出值。替选地能够考虑，输出值在步骤 122 中根据紧急制动信号本身形成，如这例如通过虚线箭头 136 示出。作为另外的替选方案能够考虑的是，当通过紧急制动信号满足输出标准时，那么根据预设值来确定输出值。

[0133] 整体上由此得出一种方法，所述方法允许将浮点数进行运算，其中同时考虑下述方面，如冗余地执行所述方法，用于使用多种硬件和软件的可行性以及用于验证所述方法的可行性。

[0134] 在这里没有示出的另外的实施形式中，所示出的所有步骤能够设计为单独的或多重冗余的，使得由此进一步提高安全性。

[0135] 图 5 的出图 4 中的方法的一部分，其中附加地在步骤 112 和 114 中检测计算精度 I 和 II。在步骤 138 中并行于步骤 112 确定步骤 112 的计算精度 I。相应地，并行于步骤 114 在步骤 140 中确定计算精度 II。

[0136] 计算精度例如能够通过下述方式来确定，在第一计算规则之内检测冗余过程和数字的评估方法并且将其错误相加。

[0137] 计算精度 I 和 II 被转交给步骤 142 和相应的 144。在步骤 120 和 144 中，计算精度 I 和 II 与相应的阈值进行比较。如果计算精度 I 和 II 位于阈值之上，那么不进行行动。但是如果其位于相应的阈值之下，那么在步骤 146 中确定另一替代值，其中为了该目的也将来自步骤 112 和 114 中的结果区间 I 和 II 递交到步骤 146。来自步骤 146 的替代值随后用于实施计算单元处的同步 60。
在一个备选的设计方案中，当低于来自步骤 120 和 144 中的阈值中的一个时，那么在步骤 120 中满足输出标准。这通过虚线示出的箭头 147 和 148 示出。

如果通过低于阈值而满足输出标准，那么又得到下述可行性：根据最后的区间交叠确定输出值，或者根据对所述数的预设值来确定输出值。

图 6 同样示出图 4 中的流程图的一部分。除了图 4 中示出的步骤之外，并行于关于结果区间间执行第一计算规则也确定结果值 I 和 II。这在步骤 150 和 152 中进行。浮点值从步骤 108 中传递到步骤 150 和 152 中。在步骤 150 和 152 中，分别将所调整的两个计算规则应用于浮点数，使得能够确定结果值 I 和 II。来自步骤 150 和 152 的第二计算规则分别与步骤 112 和 114 的第一计算规则等价。所述第二计算规则与步骤 112 和 114 中的第一计算规则的不同之处在于在考虑区间。

结果值 I 和 II 被转发给步骤 154 和 156。在步骤 154 中，来自步骤 150 的结果值 I 与来自步骤 152 的结果区间 II 进行比较。如果结果值 I 位于结果区间 II 中，那么不进行另外的应对措施。如果结果值 I 不位于结果区间 II 中，那么在步骤 146 中确定另一替代值。其中步骤 146 包含来自步骤 112 和 114 中的当前的结果区间 I 和 II。接下来，作为反应步骤实施同步 60。替选于此，能够相等地如在图 5 中描述的那样经由箭头 158 满足输出标准。由此同样得出根据需要不同地确定输出标准的可能性。

步骤 156 相应地如步骤 154 那样工作，其中在此检查：来自步骤 152 的结果值 II 是否位于来自步骤 150 的结果区间 I 中。

为了完整性起见，在此需要指出的是，该方法不被限制于图 4、5 或 6 的各个实施例，而是相反，不同变型形式的组合是可行的。

图 7 示出根据本发明的安全控制设备之内的信号曲线 160。输入信号 162 经由箭头 164 转发给计算单元 36 和 38。两个计算单元 36 和 38 以等价的方式运行，其中所述两个计算单元多样地构成。

输入信号 162 转换成浮点值 166，所述浮点值在数轴 168 上显示。箭头 170 指向下一步骤。在所述步骤中，根据浮点值 166 确定具有区间上限 174 和区间下限 176 的输入区间 172。并行于此，从存储器 178 中经由箭头 180 读出参数值 182。参数值 182 同样在数轴 184 上显示。在箭头 186 中形成具有区间上限 190 和区间下限 192 的区间 188。

第一计算规则 194 显示为方块箭头。所述计算规则递交输入区间 172 和区间 188。第一计算规则然后确定结果区间 196。

由计算单元 38 以相应的方式确定结果区间 198。该结果区间与结果区间 196 不同。经由箭头 200 和 202 合并结果区间 196 和 198。接下来，确定区间交叠 204。最后，能够执行如已经被描述并且通过箭头 206 示出的另外的步骤，使得形成输出信号 208。

图 8 示出单独的计算单元 210 的另一信号曲线。所述计算单元具有图 7 中的计算单元 36 中的信号曲线。所述计算单元在此设有相同的附图标记。此外，执行第二计算规则 212，所述计算规则显示为方块箭头。第二计算规则 212 直接根据浮点值 166 和参数值 182 确定结果值 214。经由箭头 216 和 218 将结果区间 196 和结果值 214 相互比较，以便验证结果区间 196。如果完成上述内容，那么输出结果区间 196。

在这里没有示出的另一实施例中，将计算单元 36 的结果值 214 与计算单元 38 的结果区间 198 进行比较，以便验证结果区间 198。
图 5
图 6
图 7
图 8