[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 12/28
H04L 1/22

[12] 发明专利说明书

[21] ZL 专利号 96103130.1

[43] 授权公告日 2003 年 6 月 18 日

[11] 授权公告号 CN 1111994C

[22] 申请日 1996.3.15 [21] 申请号 96103130.1

[30] 优先权

[32] 1995. 3.16 [33] DE [31] 19509558.8

[71] 专利权人 ABB. 专利有限公司

地址 联邦德国曼海姆

[72] 发明人 E·迪马 H·D·科斯

H·希尔马

审查员 焦景梅

[74] 专利代理机构 中国专利代理(香港)有限公司

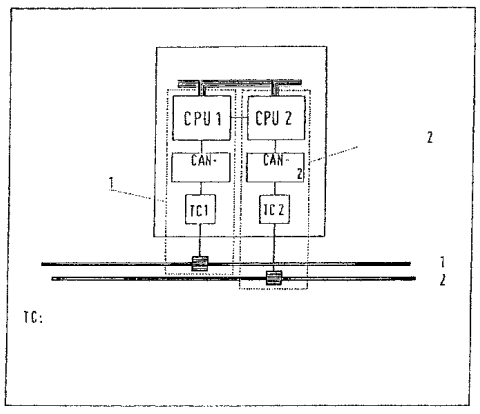
代理人 董江雄 王 岳

权利要求书 2 页 说明书 9 页 附图 2 页

[54] 发明名称 在严格实时条件下容错通讯方法

[57] 摘要

本发明涉及在局域网络中在严格实时条件下容错通讯方法，使用双总线体系结构，用于报告故障和容许全局总线故障。 为了在故障情况下保持一致性和为了遵守有关数据传输的时限，提出一种主动故障检测和通知机理。 在无故障运行时所有过程数据在其中一个冗余总线系统中传输，和状态信息在另一总线系统中传输。 在故障情况下，每条总线用作监视器总线，从而通知网络用户在各自另一总线系统中发生的故障。 该方法适用于与过程有关的控制和自动系统。



ISSN1008-4274

1. 在局域网络中具有严格实时要求的信息的可靠和容错传输方法，使用基于双总线体系结构，即为冗余总线系统的主动故障检测和通知机理，其特征在于，

a) 在无故障运行时，一个总线系统的总线作为处理总线传输所有处理数据，和在无故障运行时另一总线系统的总线传输其部件的状态信息和其他信息，

b) 在另一总线发生故障情况下每一总线用作监视器总线，用于通知所有作为网络节点的网络用户故障发生，

b1) 在处理总线发生故障情况下通知故障触发所有网络节点切换到另一总线系统，因而处理数据在无故障的总线上继续传输，和

b2) 在不是处理总线的总线发生故障情况下通知故障不触发任何切换，

c) 所使用的网络节点全都有两个完整的总线连接部分—包括通讯CPU，通讯控制器和收发机，

c1) 每个通讯 CPU 用作监视处理器，其功能为监视其节点的另一连接部分和监视其连接部件，和

c2) 在检测到其节点另一连接部分的故障以后，通讯 CPU 启动故障报文经过其总线的传输。

2. 根据权利要求 1 所述的方法，其特征在于，使用功能为监视所有部件和检测所有类型故障的故障检测机理，

a) 一个网络节点的两个通讯CPU循环地互相交换生存信号，以检测CPU故障，和

b) 当检测到参数传输故障，通讯控制器向它连接的通讯CPU传输一故障中断，这通讯CPU接着通知该节点另一连接部分的CPU，和

c) 通讯CPU通过执行测试程序执行循环功能，监视它连接的部件，和

d) 通讯CPU执行自测试程序，从而检测其本身的故障。

3. 根据权利要求 1 所述的方法，其特征在于，在处理总线发生故障情况下一致地发生切换，

a) 在检测到故障和可能的切换之间的故障等待时间在大多数故障情况下如此之短，以致不会发生任何报文丢失，和

b) 故障复盖范围如此之高，以致不会有任何报文的窜改未被发现，和

c) 在可能的报文丢失，窜改或复制的情况下恢复一致的系统状态的恢复机理。

4. 根据权利要求 2 所述的方法，其特征在于，在处理总线发生故障情况下一致地发生切换，

a) 在检测到故障和可能的切换之间的故障等待时间在大多数故障情况下如此之短，以致不会发生任何报文丢失，和

b) 故障复盖范围如此之高，以致不会有任何报文的窜改未被发现，和

c) 在可能的报文丢失，窜改或复制的情况下恢复一致的系统状态的恢复机理。

5. 根据权利要求 1 至 4 的其中任一权利要求所述的方法，其特征在于：两个总线系统都使用控制器局域网络传输协议，

a) 使用控制器局域网络的故障计数量机理，

a1) 故障的控制器局域网络控制器破坏已被检测为故障的报文，因而导致传输的连续重复，直至故障计数器达到状态（127），和

a2) 在故障计数器状态（96）时已从控制器局域网络控制器传输到 CPU 的故障中断启动故障报文经过监视处理器传输至监视器总线，和

a3) 由故障报文可能触发的所有网络用户切换到无故障的总线，而在故障总线上传输仍被迫重复，因此不发生任何报文丢失。

在严格实时条件下容错通讯方法

技术领域

本发明涉及局域网络中具有严格时间要求的数据的可靠和容错传输方法，该方法使用基于双总线体系结构，即冗余总线系统的主动故障检测和通知机理。基于本发明方法系统的应用范围在于以与过程有关方式分布和必须实现高可靠性要求的控制和自动系统的领域。

背景技术

分布控制系统的近代概念某种程度上并不能实现高可靠性和严格实时性能。例如，高可靠系统通常被要求具有自动分层结构的更高层次的特征。在这些层次中通讯的特点为大量待传输的数据，中等的数据传输的时间要求和较少量的通讯用户（网络节点）。由于高开销和与连接有关的传输原理，在这领域中经常使用的通讯协议 TCP/IP 不能有效地传输在与过程有关的系统中居支配地位的少量数据。此外，为例如 CSMA./CD 或记号(token)总线所使用的总线访问方法或者不能确定地使用于具有少量节点的网络，或者只能使用于具有少量节点的网络。为了确保高度可靠性和可利用性实现容错的概念往往导致增加处理时间，这在时间是至关 紧要的系统中是不能允许的。

这与来自现场和传感器/执行器总线领域的协议相反，这些协议被优选供使用于与过程有关的系统中，对该系统而言时间是至关紧要的。它们容许对于小量信息传输的短处理时间和基于决定性总线访问方法。

这些协议的缺点是容错和确保数据在系统范围的一致性的机理不能充分地支持高可靠性系统。具体地说，在多数情况下广播通讯受到支持是不可靠的，即不牢固的。这中间的一例是FIP(Factory Instrumentation Protocol)。FIP 容许二个通讯用户经过一个逻辑点到点连接经确认的报文交换，同时发生一报文传输到若干接收机（广播），但并不应答正确接收。这样，确认的广播通讯只能借助若干顺序点到点传输来实现。在这过程中发生的长处理时间在时

间是关键的系统中，具体地说在大数量用户（接收机）的网络中是不能接受的。

而且，许多现场总线协议的以冗余实现的总线不受支持和需要附加的措施，这继而对数据的时间性能和一致性产生负面的影响。

总之，本发明方法构成的要求，和从所述要求得到的系统特点可以分类为如下：

· 高可靠性和可利用性

—确保数据在系统范围的一致性（即使在发生错误的情况下）

—实现容错

· 严格的实时性能

—决定性访问方法

—短处理时间

上述要求得以实现是考虑到对于与过程有关的通讯典型的报文量：报文具有短信息长度往往主要与事件有关，即是说不会循环发生。而且，应该可能与系统连接大量节点（≈100）。

具有高可靠性和可利用性的系统必须具有容错性能。即是说尽管有故障的系统部件，整个系统的功能将被保持。分布系统的特点为信息的多次重复和分配给局部分开的功能模块。多次重复和分配必须一致地发生，即源信息项目必须在特定时间内以同一状态出现于所有接收机中。与一致性相联系的，容错意味即使发生错误，分布数据库的一致性仍将保持，或在错误的传播会导致整个系统的严重出错以前被恢复。容错的实现借助于系统部件的冗余结构发生的。例如，在分布系统中一总线的故障只有通过切换到一冗余总线系统才能被容许。切换过程的发生必须只能使运行系统的运行有最短的可能暂时中断，使得系统内的时间限制不被破坏。此外，数据库的一致性一定不能受到有害的影响，即切换时必须不发生信息的丢失、窜改和复制。这些技术条件要求非常迅速的错误检测（也称为错误等待时间）和错误复盖的宽范围。而且，冗余性要求冗余部件被很好地隔离，从而防止错误向两个系统都传播。

分布系统的可靠性由通讯协议的传输原理明确决定。数据的可靠性和一致性只有通过有效的确认机理来实现。这意味报文接收机必须通过对发射机的应答证实正确接收。在这过程，可靠性程度随确认的接收机数量而增加。运用

原子(atomic)广播原理能获得传输数据的可能的最高可靠性,原子广播原理即为:一报文或者被所有能运行的网络用户正确接收,或者不能被任一能运行的网络用户接收。这一原理可以通过例如使用多相确认周期的2相重复方法的传输概念来实现:

1 发射机向其目标组的所有用户发送报文。

2 每个接收机通过发射应答报文确认正确接收数据。

3 发射机在最大时间周期(超时)内等待应答。

4·假如应答在超时内到达,发射机发射允许报文,因而允许在接收机中处理。

·否则,发射机重复该报文的发射。

多相概念具有非常高的通讯量,这导致长处理时间和高总线负载。因而,它们不适合于严格实时系统。在此例中,显然为增加可靠性的措施通常对系统的时间性有负面影响,反之亦然。因此,可靠性和严格实时性能的两个特性难以组合在一起。

发明内容

本发明基于公开一种在局域网络中传输数据的方法的目的,这个方法既能满足高可靠性要求,又能满足严格实时要求。

这目的是通过该方法的特点达到的,该方法使用基于双总线体系结构的主动故障检测和通知机理。在随后的说明中可以看到这优越的改进之处。

本发明的方法使用双总线体系结构。冗余总线结构一方面用于增加系统可靠性,在发生故障时切换至第二总线;另一方面实现主动故障检测和通知机理。这一机理过临视处理器提供被检测到的节点故障,并通过第二总线系统间所有网络用户通知故障。因而,有可能迅速地检测和处理部件故障,和一致地切换至冗余部件,即不会有报文的丢失,窜改和复制。最好二个总线系统都使用 CAN(Controller Area Network,控制器局域网络)总线协议,因为这对实现本发明方法有合适的特性。

原先为用作汽车车辆中传感器/执行器总线开发的 CAN 由于其灵活性适用于自动技术的广泛领域。尤其是,高可靠和有效原子多版(multicast)传输

原理的实现和故障检测和容错的机理使 CAN 成为高可靠实时系统的一个基础。

在 CAN 网络中数据的传输如下方式发生:

1. 一个节点（发射机）广播发射一报文。

2. 假如任何节点发现发射故障，为发射仍在发生时通过用一故障帧重写该总线电平使报文破坏。

3. 所有节点不理会受破坏的报文。

4. 发射机开始新的发射。

实现被动确认机理，即只要没有任何节点通过重写破坏报文，那么报文发射机认为其发射已被所有网络用户正确接收。因为一报文要么被所有节点正确接收，要么不被任何节点接收，这一程序保证数据在系统范围的一致性; 这正与原子广播的原理相对应。

在无故障的情况，处理的执行（一个信息项目的发射和接收机的应答）需要仅仅一个报文的发射。这样 CAN 比起其他使用多相主动确认机理（见上）的原子广播协议实质上更为有效（短处理时间，低总线负载）。

每个 CAN 节点控制内部的接收和发射故障计数器，该计数器在一次发射故障之后增量，在每一无故障发射之后减量。假如故障计数器达到值 127，CAN 模块自动从故障主动进入故障被动状态，即它能继续发射和接收报文，但不能通过发射故障帧破坏任何错误报文。故障计数器达到值 256 的 CAN 控制器切换进入总线断开状态，即不再以任何方式参与总线通讯量。这意味故障节点直至其进入被动状态才通过发射故障帧中断总线通讯量。

仅仅使用由 CAN 协议提供的机理的分布系统相对于与高可靠性和容错有关的已解释的要求有若干不足之处。消除这些不足之处是本发明方法的出发点。

CAN 的局限在于:

1. 在 CAN 协议中没有提供冗余的管理。

2. 当一系统部件发生故障时，在一些情况下可能发生高故障等待时间。

注 1.): 系统部件，尤其是为了容许总线故障的总线线路的冗余实现需要在故障发生时一致切换到冗余部件的附加机理。这样，要实现用于故障检

测，故障寻找和切换过程控制的措施。一个重要方面是切换准则，即触发切换的系统状态的明确说明。

注 2.)：CAN 的被动确认机理有以下缺点：报文发射机并不检测另一网络用户的故障，而且宁可假定假如没有发生故障帧。所有接收机已没有故障地接收到该报文。试图运用所谓救生方法消除这缺点。“救生”一词用于指由所有网络节点循环发射生存报文。假如一个用户的生存报文没有发生，这指示在这个节点内部件故障。根据生存报文的循环时间，到检测出节点故障时可能已经过无法接受的长时间，因此丢失报文，导致不一致性。尤其是大量的连接节点时故障等待时间太长。此外，救生通讯量增加总线负载，使得其他报文的访问时间可能变得太长和时限要求不能被遵守。本发明方法运用主动故障检测和通知机理避免这些问题。每个节点借助一监视处理器监视，通过第二总线系统立即通知其他网络用户发生故障。

附图说明

图 1 示出带有多个节点（站）的系统，其中每一个节点被连接至一个冗余总线系统，

图 2 示出图 1 所示节点的结构的各个部件，和

图 3 示出根据图 1 的系统中的监视器功能。

具体实施方式

基于本发明方法的系统包括一系列总线站(节点)，根据图 1 这些总线站通过两个并行总线系统相互连接。如图 2 所示，每个节点通过两个分开的连接部分与两个总线相连。一个连接部分至少包括一个 CAN 通讯控制器，一个通讯 CPU 和一个收发机 TC。CAN 控制器执行在 CAN 协议中规定的所有机理。根据 CAN 技术规范 2.0 这些机理包括:

· 报文过滤

· 包形成

· 总线访问控制

· 故障检测

· 故障信号发生

· 报文确认

· 同步

收发机执行节点与传输媒体的物理连接；电耦合的参数在用于高速通讯的 ISO/DIS 11898 道路车辆—数字信息互换—控制器区域网络(CAN)中有规定。微控制器用作通讯CPU；微控制器启动数据的发射，选择接收的数据和传递数据以供处理。此外，根据本发明方法实现的冗余管理和故障控制（监视器机理，故障通知...）由通讯CPU执行。

总线结构或星形结构可以用作总线技术。例如绞合对和同轴电缆和光波导的两个电传输媒体可以被使用。必须根据由CAN协议所规定的对节点数的限制，最大数据速率和总线长度进行选择布局和传输媒体。

通讯CPU之间的节点内部的信息交换经过并行总线进行。可以任选地使用一个附加的串行连接部分。上述部件用作控制网络通讯；另外的处理单元通过并行总线与系统相连。

根据本发明的方法包括系统故障的管理机理。为了阐明运行方法，以下给出局域网络中可能的故障情况。

通讯部件的故障和失效情况可能分为以下两类：

· 全局故障阻止所有网络用户的通讯和从而中断整个系统的功能。全局故障一方面可能直接由于线路故障而发生和间接由于连接部件的总线阻塞故障而发生。“线路故障”一词用于指总线线路的短路和中断。总线阻塞部件故障可以是CAN控制器和收发机的总线侧输出的短路。这些故障由于一参数电压电平的产生导致总线的持续堵塞。而且，总线可能由高优先级报文的持续发射而被阻塞接收其他报文。通过切换到一冗余总线系统使全局故障可以被容许。

· 局部故障从系统范围通讯中除去一节点和根据故障用户的功能导致对整个系统功能或多或少的不利影响。“局部故障”一词包括CAN控制器，CPU和收发机的所有故障，这些故障使这些部件不能发挥功能，但并不使其他总线用户的数据通讯量处于危险境地。例如这些故障包括CAN模块和收发机之间以及收发机和总线线路之间的线路故障。而且，它们包括导致数据丢失或窜改的内部模块故障。局部故障可以采用部件的冗余结构而被容许。

以下说明故障情况和正常运行之间的区别。正常运行应理解为包括由CAN协议的故障机理所容许的瞬时传输和部件故障的无故障运行 状态。

基于本发明方法的分布系统容许在通讯部件范围内全局和局部故障。这是通过双总线结构和通讯CPU，CAN控制器和收发机连接部件的冗余实现来达到的。一个突出的优点是切换到冗余部件而保持分布数据库的一致性的可能性。这样，在故障发生后为恢复正确系统状态的复杂恢复措施被大部分地避免。本发明方法的基础是将在以下结合实例说明的主动故障检测和信号发出机理。

在正常运行时，整个处理数据通讯通过总线系统（此处为总线 1，见图2）。“总线系统”一词可以理解为总线线路和有关的CPU，CAN控制器和收发机连接部件。在正常运行时，总线系统2仅仅用于传输其部件的状态报告和其他报文。连接模块2的通讯CPU临视连接模块1以及其节点的运行性能，从而实现监视处理器的功能。同样，连接部分2由CPU1监视。假如在总线系统1中发生一故障，故障检测监视处理器借助经过总线系统2传输一故障报告，通知其他网络用户，这样实现监视器总线的功能。故障报文请求所有网络节点(假如在进一步系统检查后适当的活）阻塞总线系统1和经过总线2处理处理数据通讯量。

假如CPU1在总线系统2中检测到一故障，通过总线系统1发布 故障报告，但它不导致总线之间切换，因为处理数据通讯量不受影响。因此两个总线系统在检测各自的另一系统中故障时用作监视器总线（见图3）。

根据所述的程序，通讯CPU实现五个任务:

· 在正常运行时控制通讯

· 监视节点内另一总线的连接模块的功能

· 监视其本身连接部件的功能

· 在检测到另一总线系统中故障后控制故障报告的传输

· 切换过程的协调

根据出现一方面是CPU故障，还是另一方面是CAN控制器，收发机或线路故障，故障检测和信号发生过程是相互有区别的。

线路故障和CAN控制器或收发机误动作通常表现为总线报文的窜改和运

用 CAN 协议的即在 CAN 模块中故障检测机理发现的。发现这种故障的 CAN 控制器破坏故障报文，而通过传输故障帧使传输仍在进行（见上）。同时，所有网络节点的故障计数器增量。假如出现局部故障，根据 CAN 技术规范故障节点的故障计数器增加 8，另一 CAN 控制器的故障计数器增 1，因此，故障的控制器首先进入被动故障状态。假如 CAN 控制器的故障计数器达到值 96，它向其通讯 CPU 传输故障中断。这个中断指示极大地中断总线通讯量，和通知 CPU: CAN 控制器可能在不久进入被动状态（故障计数器状态 127）。在收到故障中断后，通讯 CPU 向有关的监视处理器报告该中断。监视处理器现在通过其总线系统（现在为监视器总线）启动传输故障通知。

这方法的优点事实上在于在处理总线故障情况下执行切换过程，而故障节点的 CAN 控制器仍处于主动故障状态（故障计数器状态≤127）。因此这控制器继续破坏所检测到的故障的报文，直至切换过程；因而直至切换没有任何报文丢文，没有任何故障报文被处理和没有任何报文被复制。这样，实现在故障情况下保持数据一致性的先决条件。而且，马上得知在整个系统内节点故障和故障定位，这在通常 CAN 系统（见上）中不是如此的。在总线和通讯 CPU 之间部件（收发机，CAN 芯片和连线）中发生的故障未被故障检测的 CAN 功能所覆盖，根据本发明方法运用附加监视机理加以检测。这机理以通讯 CPU 的软件实现，它提供对部件监视的循环功能。当发生一故障时，故障检测 CPU 继而通知有关的监视处理器，监视处理器通过经过监视器总线传输有关故障的故障报文，通知其他节点。

在 CAN 协议中没有提供对通讯 CPU 范围中故障的检测和处理，根据本发明方法需要附加的执行过程。在正常运行时，每 CPU 向有关的监视处理器发送循环生存信号。假如这些信号没有发生，这指示 CPU 有故障。假如处理总线的 CPU 受影响，监视处理器通过发生故障报告启动切换过程（见上）。以这样方法选择生存信号的周期，使得故障切换和切换尽可能不丢失报文地发生。除了运用监视处理器监视外，通讯 CPU 执行自测试。假如自测试检测到误动作，通知监视处理器，从而启动发送故障报告。

在特定部件故障情况时，在一些情况下不可能完全排除在误动作发生和切换过程之间报文丢失。例如假如故障等待时间大于报文发送持续时间，就可

能发生这种情况，在这些情况时要提供恢复一致系统状态的恢复措施。

总之，导致切换到冗余部件的准则可以分类如下:

· 发生 CAN 控制器的故障被动中断

· 通讯 CPU 的生存信号发生故障

· CPU 自测试程序检测到 CPU 故障

· CPU 监视程序检测到 CAN 控制器，收发机或连接部分故障。

假如处理总线的部件有故障，才发生切换。否则，另一系统用户仅仅被通知故障。

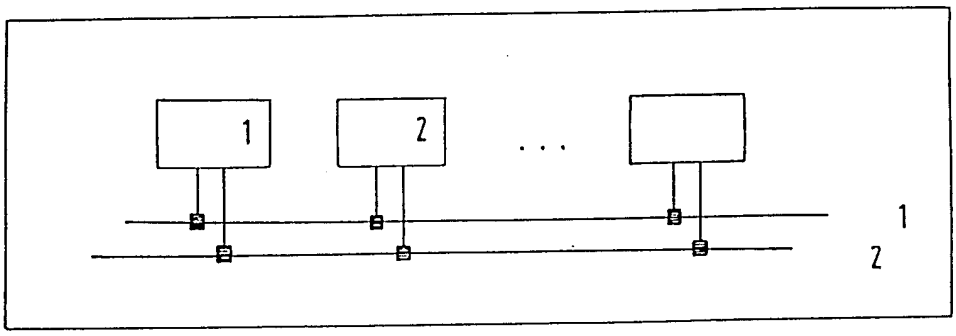


图 1

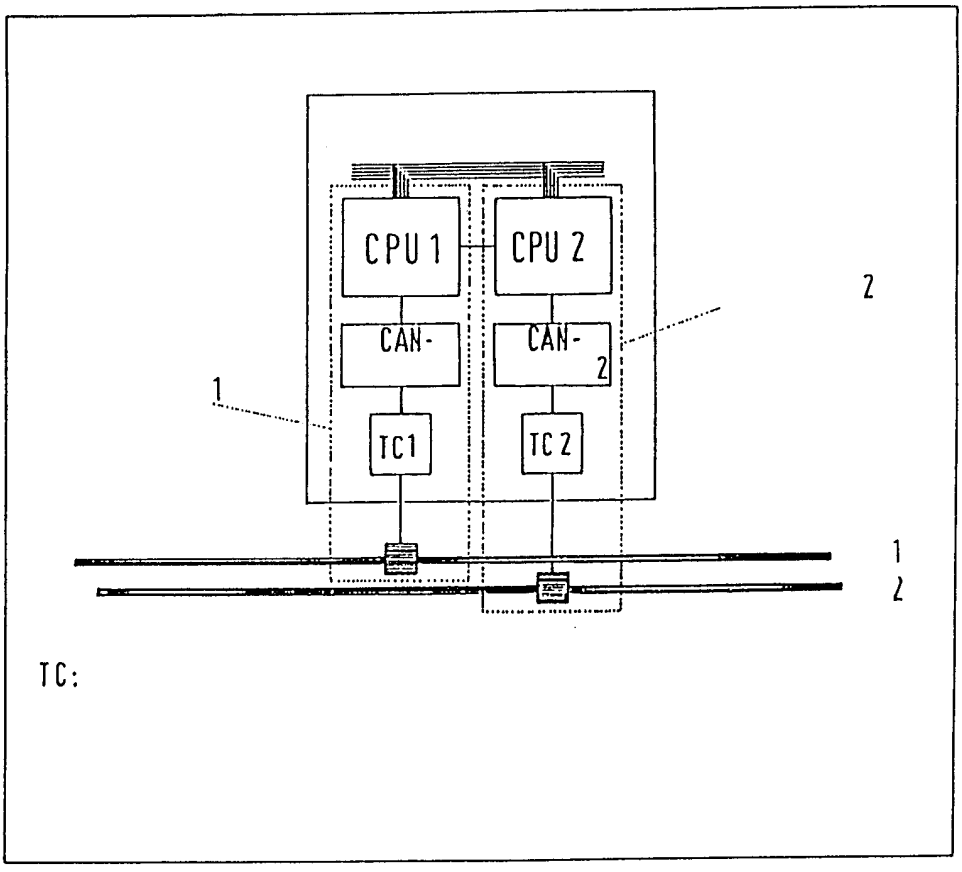


图 2

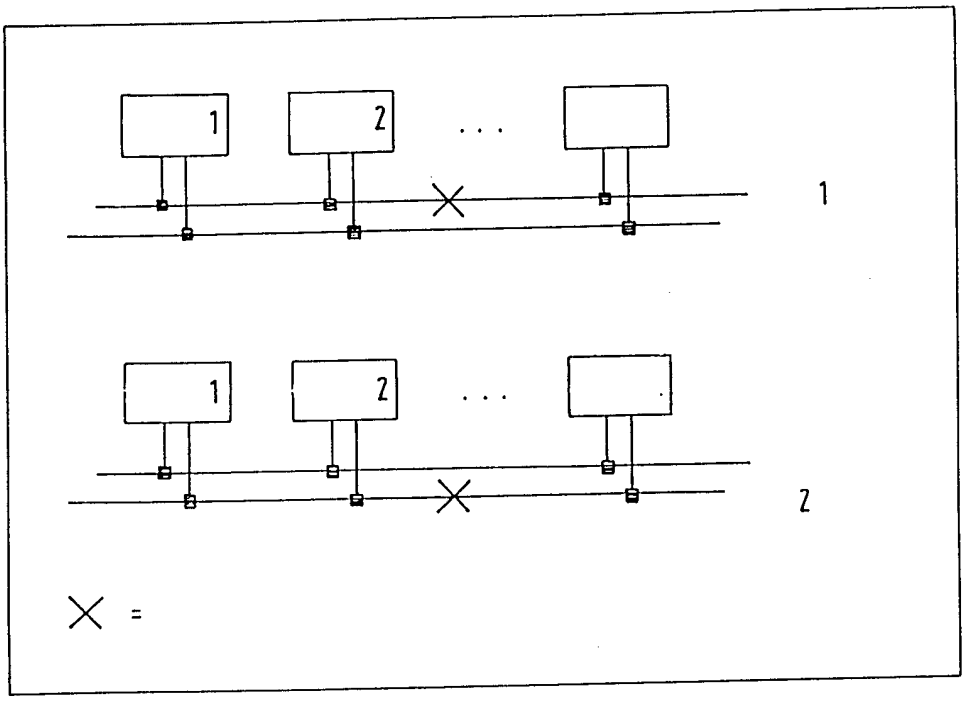


图 3