

[19] 中华人民共和国国家知识产权局



[12] 发明专利说明书

专利号 ZL 200510070448.1

[51] Int. Cl.

H04L 1/00 (2006.01)

H04L 1/22 (2006.01)

G05B 19/042 (2006.01)

[45] 授权公告日 2008 年 4 月 16 日

[11] 授权公告号 CN 100382474C

[22] 申请日 2005.5.9

[21] 申请号 200510070448.1

[30] 优先权

[32] 2004.5.10 [33] EP [31] 04011105.6

[73] 专利权人 西门子公司

地址 联邦德国慕尼黑

[72] 发明人 赫伯特·巴塞尔 弗兰克·希勒

埃德加·西格沃特

[56] 参考文献

WO0038021A1 2000.6.29

EP1043640A2 2000.10.11

CN1342129A 2002.3.27

CN1250530A 2000.4.12

DE10219501A1 2003.11.27

IEC61508: an opportunity for reliability.
Rooney J. P. Reliability and Maintainability Symposium, 2001. Proceedings. Annual. 2001

审查员 罗 玮

[74] 专利代理机构 北京市柳沈律师事务所

代理人 马 莹 邵亚丽

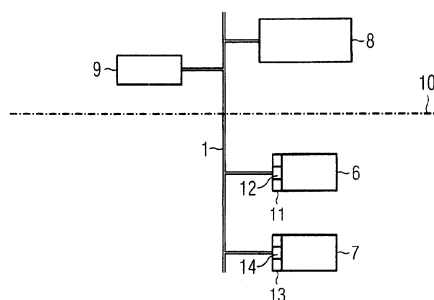
权利要求书 2 页 说明书 7 页 附图 2 页

[54] 发明名称

安全传输数据的系统和方法

[57] 摘要

本发明公开了用于安全传输数据的一种系统和一种方法,其中,该系统包括至少一个能够安全传输数据的组件(2,6,7)。为了能够以减少的硬件开销来安全传输数据,按照本发明建议这样使单通道组件(2,6,7)能够安全传输数据:该组件通过总线(1)与安全计算机单元(8)连接、并具有用于以正常形式和不同形式引导数据的通信驱动器(23),通信驱动器(23)具有一个标记值,用于指示以正常形式和不同形式引导的数据是安全替代值还是真实值,在通信驱动器(23)中产生以不同的形式引导的数据的校验和,以及设置了用于监控程序运行的程序控制。



1. 一种用于安全传输数据的系统，其包括至少一个能够安全传输数据的单通道组件（2，6，7），其中：

- 该组件通过总线（1）与安全计算机单元（8）连接；
- 该组件具有用于以正常形式和不同形式引导数据的通信驱动器（23）；
- 通信驱动器（23）具有一个标记值，用于指示以正常形式和不同形式引导的数据是安全替代值还是真实值；
- 在通信驱动器（23）中，产生以不同形式引导的数据的校验和；以及
- 设置了用于监控程序运行的程序控制。

2. 根据权利要求1所述的系统，其特征在于，所述真实值是过程值，所述组件（2，6，7）是用于处理该过程值的外围设备，所述总线（1）是现场总线。

3. 根据权利要求1所述的系统，其特征在于，所述安全计算机单元（8）是相应于一种安全标准认证的。

4. 根据权利要求1所述的系统，其特征在于，所述组件（2，6，7）是扩充安全通信驱动器（23）的运行保障组件。

5. 根据权利要求1至4中任一项所述的系统，其特征在于，所述组件（2，6，7）具有屏蔽的安全附加数据和活跃的安全单通道通信驱动器（23），用于至少在非安全重要的应用中临时应用，其中，该安全附加数据在该时间过后被准许。

6. 根据权利要求1至4中任一项所述的系统，其特征在于，所述组件（2，6，7）是传感器或运行器。

7. 一种用于安全传输数据的方法，其中，利用至少一个单通道组件（2，6，7）安全传输数据，其中，该组件（2，6，7）通过总线（1）与安全计算机单元（8）连接；通信驱动器（23）将数据以正常形式和不同形式引入该组件（2，6，7）；该通信驱动器（23）具有一个标记值，用于指示以正常形式和不同形式引导的数据是安全替代值还是真实值；在通信驱动器（23）中，产生以不同形式引导的数据的校验和；以及由程序控制监控程序运行。

8. 根据权利要求7所述的方法，其特征在于，该方法用于过程自动化，

其中，所述真实值是过程值，所述组件（2，6，7）是用于处理该过程值的外围设备，所述总线（1）是现场总线。

9. 根据权利要求7所述的方法，其特征在于，所述安全计算机单元（8）是相应于一种安全标准认证的。

10. 根据权利要求7所述的方法，其特征在于，所述组件（2，6，7）是扩充安全通信驱动器（23）的运行保障组件。

11. 根据权利要求7至10中任一项所述的方法，其特征在于，所述组件（2，6，7）具有屏蔽的安全附加数据和活跃的安全单通道通信驱动器（23），用于至少在非安全重要的应用中临时应用，其中，该安全附加数据在该时间过后被准许。

12. 根据权利要求7至10中任一项所述的方法，其特征在于，所述组件（2，6，7）是传感器或运行器。

安全传输数据的系统和方法

技术领域

本发明涉及一种安全传输数据的系统和方法，其中，该系统具有至少一个能够安全传输数据的组件。

背景技术

为了通过总线安全节点安全传输数据，采用具有两个微控制器的外围设备。这样的安全外围设备的安全级别通常能达到 IEC 61508 的 SIL 2 至 SIL 3。而在加工工业中则对于安全应用通常采用无总线连接的运行保障设备。

根据 DIN V VDE 0801 以及 VDI/VDE 3542，概念“安全（防故障）”表示一个系统在发生中断的情况下保持在安全状态或立即过渡到安全状态的能力。作为同义语也采用概念“防故障”或“安全”。

发明内容

本发明要解决的技术问题是，利用减少的硬件开销使数据的安全传输成为可能。

本发明的技术问题是通过一种安全传输数据的系统来解决的，其包括至少一个能够安全传输数据的单通道组件，其中，该组件通过总线与安全计算机单元连接；该组件具有用于以正常形式和不同形式引导数据的通信驱动器；该通信驱动器具有一个标记值，用于指示以正常形式和不同形式引导的数据是安全替代值还是真实值；在该通信驱动器中，产生以不同形式引导的数据的校验和；以及设置了用于监控程序运行的程序控制。

本发明的技术问题还通过一种安全传输数据的方法来解决，其中，利用至少一个单通道组件来安全传输数据，其中，该组件通过总线与安全计算机单元连接；通信驱动器将数据以正常形式和不同形式引入该组件；该通信驱动器具有一个标记值，用于指示以正常形式和不同的形式引导的数据是安全替代值还是真实值；在通信驱动器中，产生以不同形式引导的数据的校验和；以及由程

序控制监控程序运行。

按照本发明，可以基于单通道组件、尤其是微控制器来采用可实现安全级为 SIL 2（根据 IEC 61508）的通信驱动器。不需要开销大的、完全冗余的组件的硬件或软件实现。对于在冗余实施方式下采用两个微处理器同步的情况，按照本发明仅需调用程序控制，其检查这些同步点是否以正确的顺序被处理。此外还将数据和标记值加倍，即同时以正常形式与不同形式、尤其是以非反向和反向形式来引导。其它故障可由安全计算机单元来识别。

尤其是在加工工业中出于对费用的考虑要避免开销大的组件冗余。为了达到加工工业所要求的安全级别，按照本发明的优选实施方式建议，真实值是过程值、组件是用于处理这些过程值的外围设备，而总线是现场总线。按照本发明的另一优选实施方式组件尤其是传感器或运行器。

为了达到所期望的安全级别，按照本发明的另一优选实施方式计算机单元是相应于一种安全标准认证的。

如果按照本发明的另一优选实施方式，组件是扩充通信驱动器的运行保障组件，则这些组件的尽可能广泛的应用可以得到简化。为了获得部分所要求的运行保障，按照本发明的另一优选实施方式，组件具有屏蔽的安全附加数据和活跃的安全单通道通信驱动器，用于至少在非安全重要的应用中临时应用，其中，该安全附加数据可被准许。

附图说明

下面借助附图所示实施例详细描述和解释本发明。图中：

图 1 示出能够安全传输数据的单通道组件；

图 2 示出用于安全传输数据的系统；

图 3 示出另一种安全传输数据的组件。

具体实施方式

下面借助 PROFIsafe 特性来描述本发明。PROFIsafe 是满足 IEC 61508 安全要求的现场总线标准 PROFIBUS DP 的特性。在此，安全和标准通信都通过一个唯一的通道进行。PROFIsafe 将 PROFIBUS 扩展为满足过程技术和制造技术的高要求的安全总线。

通过所建议的系统和方法，可以实现按照安全级别 SIL 2（按照 IEC 61508）

的防故障通信。此外还可以实现：

- 采用具有 PROFIsafe 的运行保障传感器/运行器，
- 采用测量转换器（MU），其本身不是按照 IEC 61508 认证的，而是按照 IEC 61511/NE79 对于那些由制造商声明为“在使用中证明”的而存在，
- 所谓的 F-通信部件（PROFIsafe 中的安全通信部件；F=防故障（failsafe））可以相应于 SIL 2（IEC 61508 部分 3）认证，请见 NE97（即“充分减少在传感器/运行器上的系统故障”），
- 相应于按照 IEC 61508 部分 1 和 3 的 SIL 2 控制通信路段上的通信故障，
- 可以实现 PROFIsafe 驱动器，其可对双通道以及附加地对“在使用中证明”测量转换器参数化，即可用于单通道设备。

为了达到所期望的系统安全级别，须将现场设备的传感器/运行器以及现场设备信号的总线耦合器如在常规构造的过程技术保护装置中那样保障运行，或为了足够减少系统故障须至少满足 SIL 2 的要求，而无需显式地认证。上述 NE97 规定了，为了安全传输数据在传感器和运行器中按照 IEC 61508 采用协议栈，其将可靠产生的信号置于总线上。在传输介质（如总线导线、总线主设备、总线耦合器）本身上不需设置安全技术要求。该保证安全性的协议（除传输层以外的现有安全层，例如 PROFIsafe）可以通过开关有选择地在现场设备中被激活。由此可使现场设备既用于安全重要的装置，也用于非安全重要的装置。只要设备是安全重要的，就必须例如通过闭锁功能来保证安全重要的设置不会被改变。通过所述措施使得至可存储程序控制器（SPS）的安全通信成为可能。总线系统在安全运行中须保证随后的故障能在容错时间内被识别，并进行特定的安全反应：

- 伪造地址
- 重复
- 丢失
- 插入
- 顺序错误
- 伪造信息
- 延迟。

按照本发明，采用由单个微处理器实现的保障运行的组件，尽管如此，仍能实现加工工业中通常要求的按照 IEC 61508 的安全级别 SIL 2。由此，尤其是

可以避免只能采用具有认证的组件的保护装置,而这通常要求额外地保持备件。按照加工工业的要求,由此可以将同样的组件用于安全技术和其它自动化技术。此外还可实现,按照 IEC 61511/IEC 61508 改变固件/硬件至新的运行保障,由此保障 SIL 2 安全级。

图 1 示出用于安全传输数据的单通道组件 2 的功能单元,在此是具有总线功能的现场设备。组件 2 通过总线耦合器 4 连接到总线 1 上,总线耦合器 4 具有协议栈 5,总线 1 在此是现场总线。附图标记 3 标记出组件 2 的传感器及过程耦合器。

图 2 示出用于安全传输数据的系统,其包括两个能够安全传输数据的单通道组件 6、7。按照图 2 所示实施例,组件 6、7 是一个运行器和一个传感器,它们通过总线 1 与安全计算机单元 8 连接,在此,总线 1 为现场总线、安全计算机 8 例如为安全可存储程序控制器。组件 6、7 分别具有带有协议栈 12、14 的总线耦合器 11、13。在总线 1 上还连接有总线主设备 9。附图标记 10 标示出电路空间(总线主设备 9 和安全计算机 8)和现场设备(组件 1、2)之间的界线。

安全通信驱动器的实施例是 PROFIsafe 驱动器。随着相应于 IEC 61508 部分 3 的 PROFIsafe 驱动器的协议栈的认证,可以实现按照 SIL 2 安全级所要求的足够减少的系统故障。在此,协议栈在本身没有系统故障的情况下覆盖相应于 SIL 2 (IEC 61508 部分 3)要求的数据传输故障。由此,通过单通道 PROFIsafe 驱动器可将偶然故障降低到足够少。同样,如同在双通道 PROFIsafe 驱动器的情况,在单通道 PROFIsafe 驱动器的情况下也要求足够地覆盖偶然硬件故障,这通过下述措施来实现。

按照本发明的实施方式,对运行保障设备扩充 PROFIsafe 驱动器,并通过现场总线连接到认证的安全控制器上。PROFIsafe 驱动器具有能够发现下述传输故障的功能:

- 电文重复
- 电文丢失
- 电文插入
- 电文顺序错误
- 伪造有效数据
- 电文延迟

- 安全重要的和标准消息的耦合
- 地址错误（双地址和错地址错误）。

由此，驱动器相应于按照 IEC 61508 的 SIL 2。在有足够存储空间的情况下可以毫无问题地对现有运行保障现场设备补充该驱动器。这样补充的现场设备包括总线通信，因此适于 SIL 2 应用或 NAMUR 应用（见 NAMUR NE97）。

图 3 示出按照 SIL 2（IEC 61508）能够用于安全传输数据的单通道组件。组件 20 通过总线节点 28 连接到现场总线 29（例如标准 PROFIBUS）。组件 20 具有防故障传感器 21，其也称为 F-传感器（F=防故障），该传感器 21 将数据传送到组件 20 的微处理器 22。传感器 21 由于运行保障或相应的开发而是防故障的。传感器 21 可以直接是组件 20 的组成部分，或设置于其外并通过适当的连接与组件 20 连接。至此常规的防故障现场设备具有一个防故障传感器 21，其通过技术固件 30 耦合在微处理器 22 上，并以这种组合按照 SIL 2 认证。但按照现有技术这样的组合的安全总线连接是不可能的。在图 3 所示的本发明的实施方式中，微处理器 22 还具有通信驱动器 23，在此例中其是 PROFIsafe 驱动器。通信驱动器 23 用于安全传输数据 25，数据 25 与称为 F 附件的防故障附件 26 一起被传输。在此，传输借助微处理器的 DP 栈 IF（DP=分散式外围设备；IF=接口）至一个 DP 栈、一个在 PROFIBUS ASIC 27 上的协议栈来进行。该协议栈也可以集成到微处理器本身中。

通过下述措施来发现要控制的故障：电文重复由所谓的 F-主机（如安全计算机单元）来识别。F-主机还可以以安全可存储程序控制器的形式、以在计算机（如 PC 机）上运行的安全程序等形式来实现。同样通过 F-主机可以识别电文丢失。其它发送者的电文插入通过所谓的 F-地址来识别。F-地址被参数化并在运行开始时进行检验。电文顺序错误（重排序）在 F-主机中通过保持期望的顺序号来识别。伪造有效数据同样由 F-主机来识别，因为 F-主机对于校验和（例如，CRC=循环冗余校验）具有保持的期望值。如果处理器错误地产生了 CRC，则该结果仅以足够小的概率与错误的数据相匹配。电文延迟由 F-主机通过时间监控来识别。安全重要的和标准消息的耦合由 F-主机根据地址期望值来识别。地址错误通过在 F-主机中保持期望的顺序号和应答检验来识别。因此，大部分故障通过 F-主机来识别。对于所述防故障应用总是有 F-主机用于安全部分。F-主机具有按照要求的质量来发现故障的特性。此外，还可以控制在 PROFIsafe 驱动器工作中出现的偶然硬件故障。这些偶然故障是在所发送的过程数据中的

数据错误，以及状态位“FV”（=标记所使用的是安全替代值还是过程值）的数据错误和程序运行中的错误。为了也能在过程容错时间（典型地为1秒）内发现这样的错误，将补充下述特性：

- 还将过程数据以不同的形式、如反向的形式传送给 PROFIsafe 驱动器，并由该驱动器继续引导。
- 在 PROFIsafe 驱动器中还将状态位“FV”以正常和不同的形式、特别是以正常和反向的形式进行引导。
- 在 PROFIsafe 驱动器中由本身相互独立的数据段产生校验和（例如 CRC）。
- 引入单通道程序控制，即在程序控制中对所有同步点进行转换。

该措施足以由从前的作为双通道驱动器采用的驱动器产生更可靠的用于传感器的单通道驱动器。该单通道 PROFIsafe 驱动器同样是按照 IEC 61508 部分 3 认证的。在 PROFIsafe 设备中对系统故障的验证首先是通过观察其次是通过由认证协会进行的 F-协议的一致性测试来实现。

运行保障意味着按照 IEC 61511 在一年的时间里将设备用于十种不同的应用进行分析的结果（见 IEC 61511 部分 1，第 6.7.3.3.3 节）。这是通过使设备具有实现的（以及活跃的）PROFIsafe 驱动器、但屏蔽的 PROFIsafe 附加数据在一年中在十种不同的非安全重要的应用中运行实现的。在该一年之后也将该设备用于安全重要的应用中。在这种情况下，需要 PROFIsafe 协议。为此仅需准许 PROFIsafe 数据并将设备与 PROFIsafe 驱动器一起视为运行保障的。因此，PROFIsafe 驱动器总是接通，转换的仅有数据的准备。因此 PROFIsafe 驱动器总是一起运行，由此也可达到相同的用于运行保障的传感器的时间和数据特性。如果如通常那样仅在设备用于安全应用时才激活 PROFIsafe 驱动器，则随着 PROFIsafe 驱动器的激活可能丢失运行保障，因为设备被视为被改变。另一种可能性是，将设备从一开始就作为安全设备开发，但其相对于在此提出的解决方案明显开销大且更耗时。

总之，本发明涉及用于安全传输数据的一种系统和一种方法，该系统包括至少一个能够安全传输数据的组件 2、6、7。为了能够以减少的硬件开销来安全传输数据，按照本发明建议这样使单通道组件 2、6、7 能够安全传输数据：使组件通过总线 1 与安全计算机单元 8 连接，具有用于以正常形式和不同形式引导数据的通信驱动器 23，通信驱动器 23 具有一个标记值，用于指示以正常

形式和不同形式引导的数据是安全替代值还是真实值，在通信驱动器 23 中，产生以不同形式引导的数据的校验和，以及设置了用于监控程序运行的程序控制。

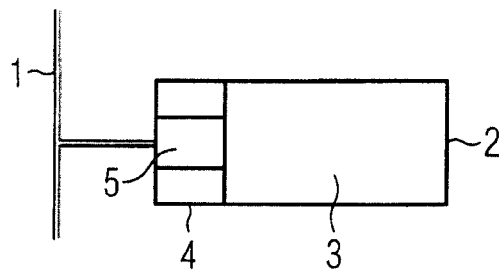


图 1

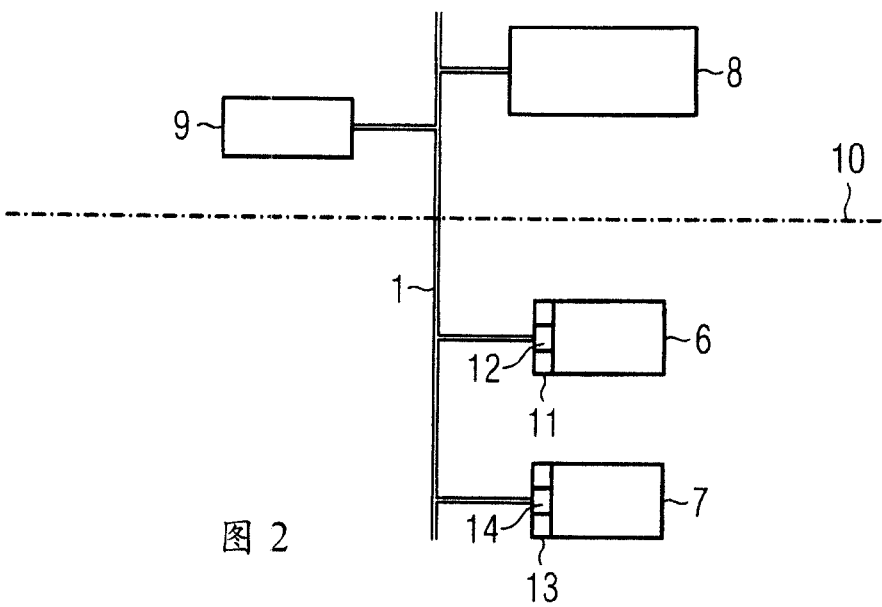


图 2

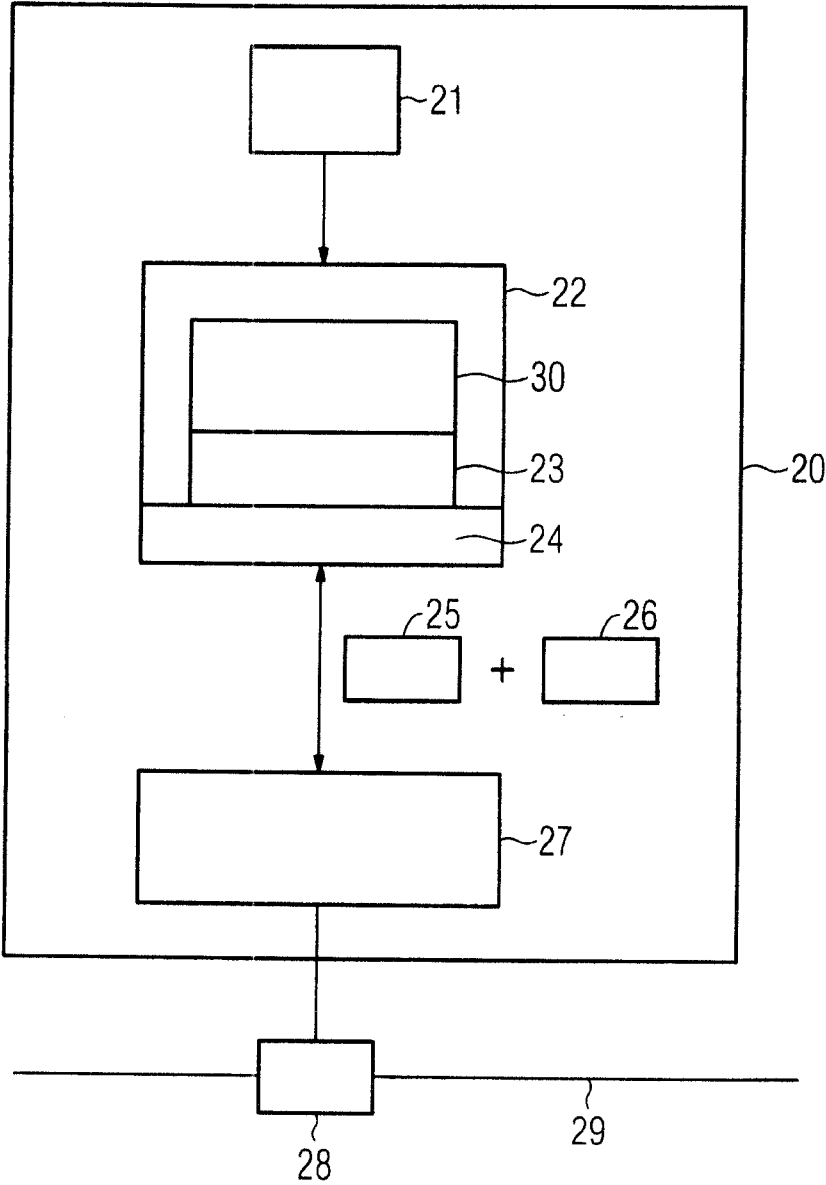


图 3