

一种功能安全的开关量输出模块和诊断处理方法

相关申请

本申请要求 2020 年 12 月 29 日申请的，申请号为 202011587822.6，发明名称为“一种
5 功能安全的开关量输出模块和诊断处理方法”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及工业自动化控制技术领域，特别是涉及一种功能安全的开关量输出模块和诊
10 断处理方法。

背景技术

工业现场的开关量输出控制系统，是 DCS、SIS 等工业控制系统中最主要的一个输入
组件。相关技术中大部分功能安全相关的开关量输出模块采用 2003 架构，此架构往往需
15 要大量的硬件来构建实现，根据此架构设计出的产品一般成本较高并且体积较大，当实际
应用中对安装空间和成本有要求时，2003 架构产品会具有局限性。

随着技术的日渐成熟，SIS 产品设计正在朝向更小体积以及更低成本的方向迈进，更
多的设计开始采用 1002D、1002 或 1001D 等架构。

采用 1002D 的架构，如图 1 所示。该设计中采用双通道、双 CPU 分别控制输出并分
20 别读取本通道诊断数据，而该方案当中的两个通道缺少必要的信息交互，假设其中一路通
道发生故障且无法关断输出电路，未出现故障的通道的 CPU 单元是无法获取诊断信息并执
行关断导向安全的，两通道相对独立且缺少交互的设计是存在一定的隐患的。

采用 1001D 架构的设计，如图 2 所示。该设计在一个 CPU 单元控制一个输出单元的
基础上加上了一个诊断单元，诊断单元和输出单元分别控制一个开关，两个开关串联，诊
25 断单元可诊断输出单元同时将信息发给 CPU，还可以在发生故障时关断其控制的开关导向
安全，但是如果诊断单元本身发生故障并无法向 CPU 提供可靠的诊断信息时，整个模块就
存在安全隐患了。

发明内容

30 本申请的目的在于解决开关量输出模块的双输出通道缺少交互设计以及诊断单元本

身发生故障无法向 CPU 提供可靠的诊断信息，在两路输出电路之间增加交互诊断的措施，并且增加了通过关断 CPU 与输出电路之间的通信来关断输出，提高了模块的安全性能，确保模块的导向安全，在满足功能安全的同时降低开发成本并减小产品体积。

本申请的第一个方面提供了一种功能安全的开关量输出模块，包括，CPU 单元，以及，
5 分别与 CPU 单元耦接的第一输出单元和第二输出单元；所述 CPU 单元用于向第一输出单元或第二输出单元发送通信数据，并基于接收的第一输出单元或第二输出单元反馈的诊断数据输出故障信息，从而控制第一输出单元或第二输出单元导向安全；所述第一输出单元或第二输出单元至少包括依次耦接的逻辑电路、驱动电路、回检电路和输出开关，以及，与驱动电路耦接的电源电压检测电路，其中，第一输出单元的输出开关 SW1 和第二输出
10 单元的输出开关 SW2 串联；所述逻辑电路的输入端输入 CPU 单元发送的通信数据，并输出至驱动电路，以及，用于接收另一个输出单元的电源电压检测电路输出的故障信号，控制 CPU 单元与驱动电路之间的通信通断；

所述驱动电路用于接收和校验 CPU 单元发送的通信数据，并在校验通过后依据通信数据信息控制输出开关断开或闭合，以及采集回检电路的输出状态和输出开关的线路诊断信
15 息；所述回检电路用于检测开关输出状态并将其发送至驱动电路；所述电源电压检测电路用于检测驱动电路的电源电压并基于检测电压发送控制信号至另一输出单元的逻辑电路。

进一步的，所述输出单元还包括与驱动电路耦接的监控电路，所述监控电路用于接收驱动电路数据校验后输出的信号，并输出控制信号控制驱动电路输出开通或关断信号，从而控制输出开关断开或闭合。

20 进一步的，若所述驱动电路数据校验失败不输出脉冲信号至监控电路，从而控制监控电路输出低电平信号至驱动电路；若所述驱动电路数据校验成功后发送脉冲信号至监控电路，从而控制监控电路输出状态保持不变。

进一步的，所述监控电路包括但不限于单稳态触发器电路。

进一步的，所述逻辑电路至少包括逻辑门芯片和逻辑器件；所述逻辑门芯片的输入端
25 输入 CPU 单元发送的通信数据，输出经逻辑门芯片转换后的通信数据至驱动电路；所述逻辑器件用于接收另一个输出单元的驱动电路的电源故障信号，从而控制本输出单元的逻辑门芯片通断。

进一步的，所述 CPU 单元还用于发出 CPU 单元内部故障信号至逻辑器件，从而通过逻辑门芯片控制断开 CPU 单元与驱动电路之间的通信。

30 进一步的，所述输出开关 SW1 和输出开关 SW2 为具有负载电流检测功能的开关。

进一步的，所述驱动电路包括但不限于逻辑芯片 CPLD。

本申请的第二个方面提供了一种基于功能安全的开关量输出模块的诊断处理方法，至少包括基于输出开关故障进行诊断处理，具体包括：

S1，根据预设状态周期性控制输出开关 SW1 和输出开关 SW2 的输出状态；

S2，回读回检电路检测的输出状态；

5 S3，将一个周期内回读的实际回检结果与预设的回检结果进行比较，并基于比较结果判断是否关断输出开关 SW1 和输出开关 SW2 的输出。

进一步的，所述步骤 S3 具体包括：

S31，若 CPU 单元的实际回检结果与预设的回检结果相同，则重复步骤 S1-S3 诊断开关输出状态；

10 S32，若 CPU 单元实际回检结果与预设的回检结果不一致，则 CPU 单元控制两个驱动电路同时关断输出开关 SW1 和输出开关 SW2 的输出。

进一步的，诊断处理方法还包括基于通信故障诊断处理，具体包括：基于 CPU 单元与驱动电路之间通信数据校验，并基于检验通过后的通信数据信息控制输出开关的输出。

进一步的，诊断处理方法还包括基于 CPU 单元内部故障诊断处理，具体包括：基于
15 CPU 单元内部软件或硬件故障发出故障信号至逻辑电路，从而控制通信的通断。

进一步的，诊断处理方法还包括基于电源故障诊断处理，具体包括：基于检测的电源故障，控制另一个输出单元的驱动电路和 CPU 单元之间关闭通信，从而控制输出开关的输出。

进一步的，诊断处理方法还包括基于线路故障诊断处理，具体包括，CPU 单元回读的
20 输出开关检测的负载电流与预设阈值比较，根据比较结果控制输出开关的输出。

本申请的有益技术效果是：

1、主控 CPU 单元以及两路构成 1002 架构的输出电路构成本申请 1001D 的整体架构。可以在保证满足功能安全的同时实现更小体积、更低成本，以满足狭小空间或恶劣环境中的应用。

25 2、通过两路输出电路之间增加交互诊断的措施，在一路通道发生故障且无法关断输出开关时，确保了另一路可以关断输出开关，进一步提升了产品的安全性能。

3、增加了通过关断 CPU 单元与输出单元之间的通信，然后由监控电路关断输出的导向安全的机制，确保了 CPU 无法直接控制输出时仍然能够关断输出。

4、具有对模块中多个部件失效的诊断处理，方法简单易实现，满足了功能安全。

30

附图说明

此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

图 1 为 1002D 架构的功能安全数字量输出电路结构框图；

图 2 为 1001D 架构的高诊断覆盖率的功能安全开关量输出模块结构框图；

5 图 3 为 1002 架构示意图；

图 4 为本申请实施例的功能安全开关量输出模块原理框图；

图 5 为本申请实施例中输出开关故障诊断处理方法流程示意图。

具体实施方式

10 为了进一步理解本申请，下面结合实施例对本申请优选实施方案进行描述，但是应当理解，这些描述只是为进一步说明本申请的特征和优点，而不是对本申请权利要求的限制。

在描述本申请之前，首先对专有名词进行解释：

1002 架构：1002 架构包含两个并列的通道，任何一个都能执行安全功能。在不影响安全功能执行的前提下，它能容许一个通道发生失效，只有当两个通道都发生危险失效时，
15 才会导致安全功能的失效。其架构示意如图 3 所示。

基于上述解释，以下是对本申请的技术方案进行详细描述。

如图 4 所示，本实施例所述的一种功能安全的开关量输出模块，包括 CPU 单元，以及，分别与 CPU 单元耦接的第一输出单元和第二输出单元。其中，CPU 单元用于向第一输出单元或第二输出单元发送通信数据，并基于接收的第一输出单元或第二输出单元反馈的诊
20 断数据输出故障信息，从而控制第一输出单元或第二输出单元导向安全。第一输出单元或第二输出单元至少包括依次耦接的逻辑电路、驱动电路、回检电路和输出开关，以及，与驱动电路耦接的电源电压检测电路，其中，第一输出单元的输出开关 SW1 和第二输出单元的输出开关 SW2 串联。逻辑电路的输入端输入 CPU 单元发送的通信数据，并输出至驱动电路，以及，用于接收另一个输出单元的电源电压检测电路输出的故障信号，控制 CPU
25 单元与驱动电路之间的通信通断。驱动电路用于接收和校验 CPU 单元发送的通信数据，并在校验通过后依据通信数据信息控制输出开关断开或闭合，以及采集回检电路的输出状态和输出开关的线路诊断信息；回检电路用于检测开关输出状态并将其发送至驱动电路；电源电压检测电路用于检测驱动电路的电源电压并基于检测电压发送控制信号至另一输出单元的逻辑电路。

30 在本申请实施例的开关量输出模块中，以图 4 中的第一输出单元为例，第一输出单元包括驱动电路 1、回检电路 1、监控电路 1、电源电压检测电路 1 和输出开关 SW1，输出

开关 SW1 的一端耦接+24V，另一端和第二输出单元的输出开关 SW2 的一端串联，输出开关 SW2 的另一端用于输出开关量并和负载耦接。

在本申请实施例中，作为可选实施方式，认为系统的安全状态应该为输出状态为 off，需要输出开关 SW1 和/或 SW2 断开。CPU 单元向驱动电路 1 发送包括开关量信息的控制数据。驱动电路 1 对接收的控制数据进行通信校验，如果校验通过，则根据 CPU 单元发送的控制数据控制输出开关 SW1 断开还是闭合状态。驱动电路 1 还通过回检电路 1 采集输出开关 SW1 的输出状态，以及直接读取输出开关 SW1 反馈的线路状态。输出开关 SW1 自带线路故障诊断功能，在发生失效情况下，可反馈故障信息至驱动电路。CPU 单元从驱动电路 1 中统一读取回检数据，并可根据第一输出单元和第二输出单元的回检数据统一分析。

10 若驱动电路 1 的电源 VCC1 发生过压、欠压等故障，则电源电压检测电路 1 发送 VCC1_Check 故障信号至第二输出单元的逻辑器件 2，逻辑器件 2 接收第二输出单元的 VCC1_Check 故障信号，并控制逻辑门芯片 IC2 关闭驱动电路 2 和 CPU 单元之间的通信，驱动电路 2 因此不会向监控电路 2 发送脉冲信号，监控电路 2 在 1.6s 超时以后，向驱动电路 2 输出低电平信号，使驱动电路 2 关断对应的输出开关 SW2，使模块导向安全。

15 在本申请实施例中，作为可选实施方案，驱动电路一般采用 CPLD 等逻辑芯片进行编程，实现数据校验和输出控制信号至输出开关的功能。监控电路一般采用单稳态触发器电路，触发脉冲时间为 1.6s。

本申请还提出了一种基于上述功能安全的开关量输出模块的诊断处理方法，本实施例的流程示意图如图 5 所示，至少包括基于输出开关故障进行诊断处理，具体包括：

20 S1，根据预设状态周期性控制输出开关 SW1 和输出开关 SW2 的输出状态；
S2，回读回检电路检测的输出状态；
S3，将一个周期内回读的实际回检结果与预设的回检结果进行比较，并基于比较结果判断是否关断输出开关 SW1 和输出开关 SW2 的输出。

25 下面结合图 3 中对本实施例中示出的多个故障诊断处理方法进行分别说明，以便本领域技术人员能够更好地理解本申请的技术方案。

输出开关故障诊断处理：在一些实施例中，输出开关存在开路、短路等失效模式。输出开关故障诊断处理主要针对输出开关 SW1 和输出开关 SW2 可能的开路、短路等失效模式。

30 CPU 单元周期性，按照下表的预设状态，按照 1-4 共 4 种状态循环，顺序地控制输出开关 SW1 和输出开关 SW2 的状态。

预设状态	SW1 状态	SW2 状态	预期回检结果
1	ON	ON	ON
2	ON	OFF	OFF
3	OFF	ON	OFF
4	OFF	OFF	OFF

以一个周期为例，CPU 单元在一个周期的 4 个实际回检结果与 4 个预期结果比较，如果实际回检结果与预期结果不一致，则认为输出开关 SW1 或输出开关 SW2 故障，此时 CPU 单元控制驱动电路 1 和驱动电路 2 同时关断输出开关 SW1 和输出开关 SW2 的输出，导向安全。为了避免负载误动作，诊断的脉宽应该小于负载的响应时间，典型值为 2ms。

通信故障诊断处理：在一些实施例中，CPU 单元与驱动电路之间存在通信故障。以图 4 中的 CPU 单元与驱动电路 1 之间说明通信数据诊断的具体步骤，CPU 单元发送包括控制信息在内的通信信息至驱动电路 1，驱动电路 1 接收通信信息并开始内部的通信数据校验。当数据校验通过时，驱动电路 1 会向监控电路 1 发送一个脉冲信号，维持监控电路 1 的输出状态不变，从而监控电路 1 的输出不影响驱动电路 1 输出至输出开关 SW1 的状态。

当 CPU 与驱动电路 1 之间的通信出现故障时，驱动电路 1 内部的通信数据无法校验通过，驱动电路 1 不会向监控电路 1 发送脉冲信号，监控电路 1 在 1.6s 超时以后，输出状态发生反转，向驱动电路 1 输出低电平信号，强制对应的输出开关 SW1 输出 OFF，使模块导向安全。

CPU 单元内部故障诊断处理：CPU 内部软、硬件有可能出现故障，在一些实施例中，当 CPU 单元内部发生故障以后，往往需要一个外部的独立电路来保证系统处于安全状态。CPU 单元内部发生故障后，发出故障指示信号 ERROR 至逻辑器件 1，逻辑器件 1 接收故障指示信号 ERROR，并控制 IC1 停止工作，从而切断 CPU 单元与驱动电路 1 之间的通信。

同时，由于驱动电路 1 收不到 CPU 单元发送的通信数据，所以不会向监控电路 1 发送脉冲信号，最终监控电路 1 因为超时向驱动电路 1 发出低电平信号，从而驱动电路控制输出开关 SW1 输出 OFF，使模块导向安全的信号。

电源故障诊断处理：在一些实施例中，驱动电路的电源可能发生电压、欠压等故障。为保证系统处于安全状态，以图 4 中所示的第一输出单元为例，当驱动电路 1 的电源 VCC1 出现过压或欠压等故障时，电源电压检测电路 1 会检测到故障，但由于此时的驱动电路 1 已经处于供电异常的状态，无法保证其一定能关断输出，因此电源电压检测电路 1 会向逻辑器件 2 发送信号关闭 IC2，从而关闭 CPU 单元与驱动电路 2 之间的通信，利用正常工作

的驱动电路 2 来关断输出开关 SW2，从而输出导向安全；同理，当驱动电路 2 的电源出现故障时，可以通过正常工作的驱动电路 1 来关断输出开关 SW1 来使模块导向安全。

5 线路故障诊断处理：在一些实施例中，由于输出开关 SW1 和输出开关 SW2 带有负载电流检测功能。当负载电流不满足预设阈值需求，即在线路发生故障短路时大于预设的阈值，或者在线路发生开路时小于预设的阈值时，输出开关 SW1 的芯片的指示引脚的信号发生翻转，CPU 单元可以通过驱动电路 1 将输出开关 SW1 指示的线路故障信息以及输出状态信息一同回读。

10 以上实施例的说明只是用于帮助理解本申请的方法及其核心思想。应当指出，对于本技术领域的普通技术人员来说，在不脱离本申请原理的前提下，还可以对本申请进行若干改进和修饰，这些改进和修饰也落入本申请权利要求的保护范围内。

权利要求书

1. 一种功能安全的开关量输出模块，其特征在于，所述开关量输出模块包括：
CPU 单元，以及，分别与所述 CPU 单元耦接的第一输出单元和第二输出单元；
所述 CPU 单元用于向所述第一输出单元或所述第二输出单元发送通信数据，并基于接收的所述第一输出单元或第二输出单元反馈的诊断数据输出故障信息，从而控制所述第一输出单元或第二输出单元导向安全；
- 5 所述第一输出单元或第二输出单元至少包括依次耦接的逻辑电路、驱动电路、回检电路和输出开关，以及，与所述驱动电路耦接的电源电压检测电路，其中，所述第一输出单元的
输出开关 SW1 和所述第二输出单元的输出开关 SW2 串联；
- 10 所述逻辑电路的输入端输入所述 CPU 单元发送的通信数据，并输出至所述驱动电路，以及，用于接收另一个输出单元的电源电压检测电路输出的故障信号，控制所述 CPU 单元与所述驱动电路之间的通信通断；
- 所述驱动电路用于接收和校验所述 CPU 单元发送的通信数据，并在校验通过后依据所述通信数据信息控制所述输出开关断开或闭合，以及采集所述回检电路的输出状态和所述
15 输出开关的线路诊断信息；
- 所述回检电路用于检测开关输出状态并将其发送至所述驱动电路；
- 所述电源电压检测电路用于检测所述驱动电路的电源电压并基于检测电压发送控制信号至另一输出单元的逻辑电路。
2. 如权利要求 1 所述的开关量输出模块，其特征在于，所述输出单元还包括与所述驱动
20 电路耦接的监控电路，所述监控电路用于接收所述驱动电路数据校验后输出的信号，并输出控制信号控制所述驱动电路输出开通或关断信号，从而控制所述输出开关断开或闭合。
3. 如权利要求 2 所述的开关量输出模块，其特征在于，若所述驱动电路数据校验失败不输出脉冲信号至所述监控电路，从而控制所述监控电路输出低电平信号至所述驱动电路；若所述驱动电路数据校验成功后发送脉冲信号至所述监控电路，从而控制所述监控电路输出
25 状态保持不变。
4. 如权利要求 2 所述的开关量输出模块，其特征在于，所述监控电路包括单稳态触发器电路。
5. 如权利要求 1 所述的开关量输出模块，其特征在于，所述逻辑电路至少包括逻辑门芯片和逻辑器件；所述逻辑门芯片的输入端输入所述 CPU 单元发送的通信数据，输出经所
30 述逻辑门芯片转换后的通信数据至所述驱动电路；
- 所述逻辑器件用于接收另一个输出单元的驱动电路的电源故障信号，从而控制本输出

单元的逻辑门芯片通断。

6. 如权利要求 5 所述的开关量输出模块, 其特征在于, 所述 CPU 单元还用于发出 CPU 单元内部故障信号至所述逻辑器件, 从而通过所述逻辑门芯片控制断开 CPU 单元与所述驱动电路之间的通信。

5 7. 如权利要求 1 所述的开关量输出模块, 其特征在于, 所述输出开关 SW1 和所述输出开关 SW2 为具有负载电流检测功能的开关。

8. 如权利要求 1-7 任一所述的开关量输出模块, 其特征在于, 所述驱动电路包括逻辑芯片 CPLD。

9. 一种基于权利要求 1-8 任一所述的开关量输出模块的诊断处理方法, 其特征在于, 至少包括基于输出开关故障进行诊断处理, 包括:

S1, 根据预设状态周期性控制所述输出开关 SW1 和所述输出开关 SW2 的输出状态;

S2, 回读所述回检电路检测的输出状态;

S3, 将一个周期内回读的实际回检结果与预设的回检结果进行比较, 并基于比较结果判断是否关断所述输出开关 SW1 和所述输出开关 SW2 的输出。

15 10. 如权利要求 9 所述的诊断处理方法, 其特征在于, 所述步骤 S3 包括:

S31, 若所述 CPU 单元的实际回检结果与预设的回检结果相同, 则重复步骤 S1-S3 诊断开关输出状态; S32, 若 CPU 单元的实际回检结果与预设的回检结果不一致, 则所述 CPU 单元控制两个驱动电路同时关断所述输出开关 SW1 和所述输出开关 SW2 的输出。

11. 如权利要求 9 所述的诊断处理方法, 其特征在于, 所述诊断处理方法还包括基于通信故障诊断处理, 包括: 基于所述 CPU 单元与所述驱动电路之间通信数据校验, 并基于检验通过后的通信数据信息控制所述输出开关的输出。

12. 如权利要求 9 所述的诊断处理方法, 其特征在于, 所述诊断处理方法还包括基于所述 CPU 单元内部故障诊断处理, 包括: 基于所述 CPU 单元内部软件或硬件故障发出故障信号至所述逻辑电路, 从而控制通信的通断。

25 13. 如权利要求 9 所述的诊断处理方法, 其特征在于, 所述诊断处理方法还包括基于电源故障诊断处理, 包括: 基于检测的电源故障, 控制另一个输出单元的驱动电路和所述 CPU 单元之间关闭通信, 从而关断所述输出开关的输出以导向安全。

14. 如权利要求 9 所述的诊断处理方法, 其特征在于, 所述诊断处理方法还包括基于线路故障诊断处理, 包括: 所述 CPU 单元回读的所述输出开关检测的负载电流与预设阈值比较, 根据比较结果控制所述输出开关的输出。

15. 如权利要求 9-14 任一所述的诊断处理方法, 其特征在于, 所述一个周期的时间小

于负载的响应时间。