

一种安全与常规控制应用间数据隔离的方法及装置

相关申请

本申请要求 2020 年 12 月 29 日申请的，申请号为 202011590531.2，发明名称为“一种安全与常规控制应用间数据隔离的方法及装置”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

本申请涉及工业过程控制技术领域，特别是涉及一种安全与常规控制应用间数据隔离的方法及装置。

背景技术

为了综合安全控制系统和常规过程控制系统的功能优点，提升控制系统部署和应用拓展的灵活性，降低控制系统的生产和使用成本等，在油气传输、小型关键系统控制等工业应用领域，已越来越多地需要在同一套控制系统中同时支持安全控制功能和常规控制功能。

安全控制功能要求具备高可靠性、高可用性，需遵循功能安全的相关标准开发和实施。安全控制应用中，实施安全控制功能的安全控制应用一般包括安全输入数据（一般指安全输入信号点，比如 DI、AI 等），安全控制算法/功能块、安全输出数据（一般指安全输出信号点，比如 DO 等）。一般情况下，不允许常规数据（包括常规输入/输出信号点，常规中间变量等）直接进入或影响安全应用，以及避免常规控制应用的运行直接影响安全控制应用，否则会降低安全控制功能的安全完整性，即需要保障安全控制应用与常规控制应用的隔离。因此，安全控制应用访问的常规数据是受限的、规模较小的。

在安全混合控制系统中，为保障安全控制应用的功能完整性，一般采用多通道表决的系统架构来提高故障裕度。每个控制器通道均包含相同的安全控制应用和常规控制应用，并独立地运行所有的控制应用。控制系统根据一定的策略，选取一个通道作为主通道，其它通道作为从通道。其中，安全控制应用通过特定的软硬件表决机制对外输出，常规控制应用一般是主通道输出，从通道不输出。

为了保障控制系统的容错性和常规控制功能的可用性，控制系统会将主通道的常规数据冗余同步给各个从通道，这些数据包括常规输入/输出信号点，及与其相关的常规变量。完成一轮冗余同步的周期较长，一般为多个控制周期。控制系统需避免从通道的常规数据

进入安全控制应用后容易导致安全应用输出发生数据回跳的问题，例如当常规数据发生变化时（从数据值 A 变化为数据值 B），各从通道的安全控制应用受该常规数据（数据值 B）影响会立即表决输出（输出数据值 B），此后短时间内各从通道又收到来自主通道变化前的冗余常规数据（数据值 A），此时各从通道受该常规数据影响又会立即表决输出为变化前的数据（数据值 A），此后只有当各从通道收到来自主通道变化后的冗余常规数据时（数据值 B），才会受此影响表决输出为变化后的数据（数据值 B）。

另外，由于实际控制应用场景中，常规数据区、安全数据区、交换数据区中均为结构化数据或多个数据的组合，当有多个异步的任务可能同时读写这些数据区时，需保障任务间读写的互斥，避免一个任务在改写部分结构化数据时，另一个任务在读取该结构数据，
10 则会导致后者读取的数据不完整，甚至错误。

相关技术中有用于执行不安全应用的第一处理器和专用于执行安全应用的第二处理器。其中安全应用中只有一个任务，通过一片全局数据区交换数据，仅是基于微控制器系统，对安全控制、常规控制对存储器的共享访问进行互斥保护。

15 发明内容

本申请的目的在于解决多任务控制、多通道运行的工业控制系统中安全控制应用的功能安全完整性，功能正确性和控制响应特性。提供了一种安全与常规控制应用间数据隔离的方法及装置。

本申请的第一个方面提供了一种安全与常规控制应用间数据隔离的方法，安全控制应用包括安全数据区和若干安全控制任务，所述安全控制任务包括若干安全控制程序；所述
20 常规控制应用包括常规数据区和若干常规控制任务，所述常规控制任务包括若干常规控制程序；所述数据隔离的方法包括：S1、为安全控制应用/常规控制应用中的控制任务分配交换数据区；S2、基于分配的交换数据区，进行安全与常规控制应用间数据隔离交换。

进一步的，步骤 S1 具体包括，为安全控制应用的若干安全控制任务分别分配独立的，
25 并基于第一容量阈值限定大小的安全交换数据区，其中，所述安全交换数据区包括安全交换输入数据区和安全交换输出数据区；为常规控制应用的若干常规控制任务分别分配独立的，并基于第二容量阈值限定大小的常规交换输入数据区。

进一步的，所述安全交换输入数据区用于存储从常规数据区拷贝的所需常规数据，进而被安全控制任务下的安全控制程序读取；所述安全交换输出数据区用于存储被安全控制
30 任务改写的常规数据的交换变量；所述常规交换输入数据区用于从相关的安全控制任务的安全交换数据区拷贝指定的安全数据，进而被常规控制任务下的常规控制程序读取。

进一步的，步骤 S2 中数据隔离交换包括但不限于通过不同的存储器、内存空间划分、访问属性设置，从而限定常规控制任务不能直接读写安全交换输入数据区，但可以读取常规交换输入数据区和安全交换输出数据区，以及，限定安全控制任务不能直接读写常规交换输入数据区，但可以读取安全交换输入数据区和改写安全交换输出数据区。

- 5 进一步的，步骤 S21 具体包括：S211、在安全交换输入数据区，为被安全控制任务读取的常规数据分配对应的交换变量的内存，在安全交换输出数据区，为被安全控制任务改写的常规数据分配对应的交换变量的内存；S212、在常规交换输入数据区，为被常规控制任务读取的安全数据分配对应的交换变量内存。

- 10 进一步的，步骤 S22 具体包括：S221、运行安全控制任务，从常规数据区拷贝需要的常规数据到安全交换输入数据区；和/或，S222、运行常规控制任务，从相关控制任务的安全交换输出数据区拷贝安全数据至常规交换输入数据区；S223、基于运行的安全控制任务/常规控制任务，运行安全控制任务/常规控制程序。

- 15 进一步的，数据隔离的方法还包括基于分别预设常规数据区和安全交换输出数据区的访问冲突解决机制，避免安全控制任务、常规控制任务对常规数据区和安全交换输入数据区、安全交换输出数据区的读写冲突。

进一步的，所述访问冲突解决机制包括但不限于设置控制任务的优先级、任务间的读写锁、数据双缓冲以及 MMU 内存保护。

- 20 本申请的第二个方面提供了一种安全与常规控制应用间数据隔离的装置，至少包括两个多通道架构的系统，其中每个通道均用于运行若干安全控制应用和/或若干常规控制应用，其中，安全控制应用包括安全数据区和若干安全控制任务，常规控制应用包括常规数据区和若干常规控制任务，安全数据区和常规数据区之间相互隔离；常规控制任务不能改写安全数据区，只能读取、不能改写常规数据区的常规交换输入区；安全控制任务不能直接访问常规数据区，只能读取、不能改写安全数据区的安全交换输入数据区。

- 25 进一步的，多通道架构的系统中的一个通道作为主通道，其余通道为从通道，通道间可以传递安全数据和常规数据。

进一步的，所述主通道的安全控制任务用于从常规数据区拷贝所述常规数据至安全控制任务的安全交换输入数据区，并分发至从通道。

进一步的，所述从通道的安全控制任务选取主通道分发的安全交换输入数据，并覆盖从通道的安全控制任务的安全交换输入数据区。

- 30 进一步的，若从通道和主通道无法通讯，则从当前通道的常规数据区拷贝所需的常规数据到安全控制任务的安全交换输入数据区。

本申请的有益技术效果如下：

- 1、可支持多个安全控制任务。
- 2、有效保障安全数据免受常规控制应用的数据、任务/程序的影响，保障安全控制应用的功能安全完整性。
- 5 3、保障多任务运行过程中任务间交换数据的完整性。
- 4、能较好地解决多通道间任务交换数据的同步实时性，保障控制响应实时性。
- 5、不止适用于安全控制应用和常规控制应用，可更广泛地使用于需要实现多任务间交换数据的受控性、完整性或实时性等较高的任何工业控制系统或装置。

10 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 为本申请实施例中安全与常规控制应用间数据隔离的方法的流程示意图。

图 2 为本申请实施例中安全与常规控制应用间数据隔离交换的方法的流程示意图。

15 图 3 为本申请实施例中安全与常规控制应用间数据隔离的装置局部示意图。

图 4 为本申请实施例中单个通道内安全与常规控制应用间数据隔离的局部示意图。

图 5 为本申请实施例中单个通道内安全与常规控制应用的多个任务间数据隔离的局部示意图。

20 具体实施方式

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。

为了方便对本申请的理解，首先对本申请中提到的一些专业术语进行说明。

安全混合控制系统：是指同时包含安全控制应用、常规控制应用的工业控制系统。

25 通道：是功能安全控制系统等具有多重表决架构的系统装置特有的术语。通道是多重化表决系统架构的基本处理单元。一个通道一般包含一个 CPU，相应的存储器，以及相关的微电子设备。每个系统通道独立地运行控制逻辑，与其它通道并行异步工作。一般地，一个安全混合控制系统中，每个通道均包含相同的安全控制应用和常规控制应用，其中安全控制应用通过特定的软硬件表决机制（主、从通道同时参与）对外输出；常规控制应用
30 一般是工作/备用机制：主通道输出，从通道不输出。

安全控制应用：指面向功能安全的控制应用，功能是监视生产装置的运行状况，出现

异常工况时能按既定的安全控制逻辑迅速处理，使危害降到最低，保障人员、装置处于生产安全状态。特点是具备高可靠性，多应用于关键装置和设备的保护与控制、瓦斯与火灾的监测与保护、油气输送过程的安全、蒸汽锅炉监测与保护、机组控制的保护等领域。遵循的标准主要有 IEC 61508，GB/T20438 等。

- 5 安全控制应用不允许随意接入非安全的信号点数据。安全控制应用包含安全数据区和若干安全控制任务，每个安全控制任务包含任务后台控制程序和若干安全控制程序，每个安全控制程序包含若干安全控制回路。每个安全控制回路包含安全的信号输入\输出点，以及安全的控制逻辑。

- 常规控制应用：指面向过程控制的控制应用，应用于常规生产过程的连续测量、常规
10 控制、操作控制管理，保障生产装置的平稳运行。常规控制应用包含常规数据区和若干常规控制任务，每个常规控制任务包含任务后台控制程序和若干常规控制程序，每个常规控制程序包含若干常规控制回路。每个常规控制回路包含常规的信号输入\输出点，以及常规的控制逻辑。

- 安全数据区：指从属于安全控制应用的数据区，一般包含安全输入信号数据、安全输出信号数据、安全内部数据等。数据区里一般都是结构化的数据或有紧密关联的数据组合，
15 需保障控制任务或控制程序在读写数据时能完整地读写整个数据结构或数据组合，而不应出现只读写了部分数据。

- 常规数据区：指从属于常规控制应用的数据区，一般包含常规输入信号数据、常规输出信号数据、常规内部数据等。相同地，数据区里一般都是结构化的数据或有紧密关联的
20 数据组合，需保障控制任务或控制程序在读写数据时能完整地读写整个数据结构或数据组合，而不应出现只读写了部分数据。

 任务：包含若干控制程序、部分数据、以及任务后台控制程序，是控制系统中控制逻辑调度控制的主体对象。任务的执行是异步的、相对独立的，可能存在多个任务同时访问同一数据的场景。

- 25 控制程序：包含若干程序段，一般采用符合 IEC61131-3 标准的编程语言编写控制逻辑。

 控制回路：控制逻辑的基本单元，一般包含输入信号点数据、输出信号点数据、控制算法或功能块等，比如经典的 PID 控制回路。

- 本申请的目的在于解决安全混合控制系统中安全控制应用和常规控制应用间数据隔离的问题，设计了一套安全与常规控制应用间数据隔离的方法和相应的装置，下面结合实
30 施例对本申请的一种安全与常规控制应用间数据隔离的方法和装置进行详细说明，以便本领域技术人员能够更好地理解本申请的技术方案。

如图 1 所示为本申请的一种安全与常规控制应用间数据隔离的方法流程示意图，其中包括以下步骤：

S1、分配交换数据区。为安全控制应用的每一个安全控制任务分配一个独立的、限定大小的安全交换数据区，包括安全交换输入数据区和安全交换输出数据区；为常规控制应用中的每一个常规控制任务分配一个独立的、限定大小的常规交换输入数据区。安全交换输入数据区用于存储从常规数据区拷贝的指定常规数据，进而被安全控制任务下的安全控制程序读取。安全交换输出数据区用于存储被安全控制任务改写的常规数据的交换变量。常规交换输入数据区用于从相关的安全控制任务的安全交换数据区拷贝指定的安全数据，进而被常规控制任务下的常规控制程序读取。

10 S2、基于分配的交换数据区，进行安全与常规控制应用间数据隔离交换。

如图 2 所示，其中，数据交换包括但不限于通过不同的存储器、内存空间划分、访问属性设置，从而限定常规控制任务不能直接读写安全交换输入数据区，但可以读取常规交换输入数据区和安全交换输出数据区，以及，限定安全控制任务不能直接读写常规交换输入数据区，但可以读取安全交换输入数据区和改写安全交换输出数据区。具体包括：

15 S21、分配变量内存；

在安全交换输入数据区中为每一个输入到安全控制任务的常规数据分配对应的交换变量的内存。其中：被安全控制任务读取的常规数据对应的交换变量分配在安全交换输入数据区；被安全控制任务改写的常规数据的交换变量分配在安全交换输出数据区；被常规控制任务读取的安全交换变量对应的常规交换输入变量分配在常规交换输入数据区。

20 S22、更新、读取安全交换输入数据区/常规交换输入数据区。

具体包括，更新、读取安全交换输入数据区，每个安全控制任务运行时，先从常规数据区拷贝指定的部分常规数据到对应的安全交换输入数据区，然后再运行该安全控制任务下属的各安全控制程序。

还包括，更新、读取常规交换输入数据区，每个常规控制任务运行时，先从相关的安全控制任务的安全交换输出数据区拷贝指定的部分数据到常规交换输入数据区，然后再运行该常规控制任务下属的各常规控制程序。

需要说明的是，各个安全控制任务、常规控制任务的运行是相互独立、异步的，步骤更新、读取安全交换输入数据区和更新、读取常规交换输入数据区是可以并发执行。

并且，为了保障安全控制任务读取的常规数据的正确性、完整性，避免安全控制任务、
30 常规控制任务对常规数据区的读写冲突，该装置采用了“设置控制任务的优先级”、“任务间的读写锁”、“数据双缓冲”或“MMU 内存保护”等访问冲突解决机制。

在一些实施方式中，优先保障安全控制任务在读取常规数据区完毕后，才允许常规控制任务改写常规数据区。

下述示出实施例中，如图 3 所示，本申请的一种安全与常规控制应用间数据隔离的装置局部示意图。装置包括至少两个多通道架构的系统，其中每个通道均用于运行若干安全控制应用和/或若干常规控制应用，其中，安全控制应用包括安全数据区和若干安全控制任务，常规控制应用包括常规数据区和若干常规控制任务，安全数据区和常规数据区之间相互隔离。常规控制任务不能改写安全数据区，只能读取、不能改写常规数据区的常规交换输入区；安全控制任务不能直接访问常规数据区，只能读取、不能改写安全数据区的安全交换输入数据区。

图 3 中，装置包括一个主通道和 2 个从通道，各通道间的控制任务及其包含的控制程序均相同。主通道的安全控制任务从主通道的常规数据区拷贝指定的部分常规数据到主通道的安全交换输入数据区，并快速分发到从通道 1#和从通道 2#。所述的快速一般指在一个基本控制周期或者任务周期内，从通道 1#和从通道 2#的安全控制任务选取来自主通道的安全交换输入数据。当从通道与主通道之间断开连接时，则从通道 1#或从通道 2#的安全控制任务从自身对应的常规数据区拷贝指定的部分常规数据到安全控制任务的安全交换输入数据区。

下面通过实际操作实例对上述实施例中示出的安全与常规控制应用间数据隔离的方法和装置进行进一步说明，以便本领域技术人员能够更好地理解本申请的技术方案。

如图 4 所示，为单个通道内的局部示意图，图示中单个通道包括一个常规控制应用和一个安全控制应用，安全控制应用与常规控制应用的数据、程序相对独立，相互隔离。常规控制应用主要包含常规数据区和若干常规控制任务，安全控制应用主要包含安全数据区和若干安全控制任务。

一般地，常规控制任务可直接读取安全数据区中的数据。但是为了有利于常规控制任务执行过程中读取的安全数据的完整性、前后一致性，在本申请中的实施例中，如图 4 所示，可将结构化或前后一致性要求较高的数据赋值到安全交换输出数据区，并经常规交换输入数据区传递给常规控制任务。

每一个安全控制任务分配一片专属的安全交换输入数据区。每个安全控制任务每次运行时，先从常规数据区拷贝指定的部分常规数据到安全交换输入数据区，然后运行该安全控制任务下属的各安全控制程序。该装置通过内存空间划分、访问属性设置等，限定安全控制程序只能读取、不能改写安全交换输入数据区。

如图 4 所示，每一个安全控制任务分配一片专属的安全交换输出数据区，每一个常规控制任务分配一片专属的常规交换输入数据区。该装置通过不同的存储器、内存空间划分、访问属性设置等，限定常规控制任务可直接读取常规交换输入数据区，安全控制任务不能直接访问常规交换输入数据区。类似地，安全控制任务能读写安全交换输出数据区，常规控制任务中的各常规控制程序不能直接访问安全交换输出数据区。

常规控制任务每次运行时，从相关的安全控制任务的安全交换输出数据区拷贝指定的部分数据到常规交换输入数据区，然后再运行该常规控制任务下属的各常规控制程序。为了保障常规控制任务读取的安全交换输出数据的正确性、完整性，避免安全控制任务、常规控制任务对安全交换输出数据区的读写冲突，通过“设置控制任务的优先级”、“任务间的读写锁”、“数据双缓冲”或“MMU 内存保护机制”等访问冲突解决机制，保障安全控制任务在改写安全交换输出数据区完毕后，才允许常规控制任务读取安全交换输出数据区。

如图 5 所示，为多安全控制任务和多常规控制任务间数据隔离的局部示意图，本申请实施例中装置的单个通道内运行一个常规控制应用和一个安全控制应用，安全控制应用包括安全控制任务 1#和安全控制任务 2#；常规控制应用包括常规控制任务 1#和常规控制任务 2#。需要说明的是，安全控制应用和常规控制应用中分别可包括若干个控制任务，各安全控制任务、常规控制任务间均相对独立、异步地运行。本实施例中为了说明清楚，仅示出各包括 2 个控制任务。安全控制任务运行和常规控制任务运行的规则如下：

- 1、安全控制任务 1#和安全控制任务 2#可同时并各自独立的读取常规数据区各自的指定数据，并分别拷贝到安全交换输入数据 1#和安全交换输入数据 2#；
- 20 2、常规控制任务 1#和常规控制任务 2#可同时并各自独立的读取相关的安全任务的安全交换输出数据区 1#和安全交换输出数据区 2#中指定的数据，并分别拷贝到常规交换输入数据区 1#和常规交换输入数据区 2#。

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。以上所述实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

权利要求书

1. 一种安全与常规控制应用间数据隔离的方法，其特征在于，

安全控制应用包括安全数据区和若干安全控制任务，所述安全控制任务包括若干安全控制程序；

5 所述常规控制应用包括常规数据区和若干常规控制任务，所述常规控制任务包括若干常规控制程序；

所述数据隔离的方法包括：

S1、为安全控制应用/常规控制应用中的控制任务分配交换数据区；

S2、基于分配的交换数据区，进行安全与常规控制应用间数据隔离交换。

10 2. 如权利要求 1 所述的数据隔离的方法，其特征在于，步骤 S1 包括：

为所述安全控制应用的若干安全控制任务分别分配独立的，并基于第一容量阈值限定大小的安全交换数据区，其中，所述安全交换数据区包括安全交换输入数据区和安全交换输出数据区；

15 为所述常规控制应用的若干常规控制任务分别分配独立的，并基于第二容量阈值限定大小的常规交换输入数据区。

3. 如权利要求 2 所述的数据隔离的方法，其特征在于，所述安全交换输入数据区用于存储从所述常规数据区拷贝的所需常规数据，进而被所述安全控制任务下的所述安全控制程序读取；

所述安全交换输出数据区用于存储被所述安全控制任务改写的常规数据的交换变量；

20 所述常规交换输入数据区用于从相关的安全控制任务的安全交换数据区拷贝指定的安全数据，进而被所述常规控制任务下的所述常规控制程序读取。

4. 如权利要求 2 所述的数据隔离的方法，其特征在于，步骤 S2 中数据隔离交换包括通过不同的存储器、内存空间划分以及访问属性设置，从而限定所述常规控制任务不能直接读写所述安全交换输入数据区，但可以读取所述常规交换输入数据区和所述安全交换输出数据区，以及，限定所述安全控制任务不能直接读写所述常规交换输入数据区，但可以
25 读取所述安全交换输入数据区和改写所述安全交换输出数据区。

5. 如权利要求 1 所述的数据隔离的方法，其特征在于，步骤 S2 包括：

S21、分配变量内存；

S22、更新、读取所述安全交换输入数据区/所述常规交换输入数据区。

30 6. 如权利要求 5 所述的数据隔离的方法，其特征在于，步骤 S21 包括：

S211、在所述安全交换输入数据区，为被所述安全控制任务读取的常规数据分配对应

的交换变量的内存；在所述安全交换输出数据区，为被所述安全控制任务改写的常规数据分配对应的交换变量的内存；

S212、在所述常规交换输入数据区，为被所述常规控制任务读取的安全数据分配对应的交换变量内存。

5 7. 如权利要求 5 所述的数据隔离的方法，其特征在于，步骤 S22 包括：

S221、运行所述安全控制任务，从所述常规数据区拷贝需要的常规数据到所述安全交换输入数据区；

和/或，S222、运行所述常规控制任务，从相关控制任务的安全交换输出数据区拷贝安全数据至所述常规交换输入数据区；

10 S223、基于运行的安全控制任务/常规控制任务，运行安全控制程序/常规控制程序。

8. 如权利要求 2 所述的数据隔离的方法，其特征在于，所述方法还包括基于分别预设所述常规数据区和所述安全交换输出数据区的访问冲突解决机制，避免所述安全控制任务、所述常规控制任务对所述常规数据区以及所述安全交换输入数据区、所述安全交换输出数据区的读写冲突。

15 9. 如权利要求 8 所述的数据隔离的方法，其特征在于，所述访问冲突解决机制包括设置控制任务的优先级、任务间的读写锁、数据双缓冲以及 MMU 内存保护。

10. 一种安全与常规控制应用间数据隔离的装置，其特征在于，所述装置至少包括两个多通道架构的系统，其中每个通道均用于运行若干安全控制应用和/或若干常规控制应用，其中，所述安全控制应用包括安全数据区和若干安全控制任务，所述常规控制应用包括常
20 规数据区和若干常规控制任务，所述安全数据区和所述常规数据区之间相互隔离；

所述常规控制任务不能改写所述安全数据区，只能读取、不能改写所述常规数据区的常规交换输入区；

所述安全控制任务不能直接访问所述常规数据区，只能读取、不能改写所述安全数据区的安全交换输入数据区。

25 11. 如权利要求 10 所述的数据隔离的装置，其特征在于，所述多通道架构的系统中的一个通道作为主通道，其余通道为从通道，通道间用于传递安全数据和常规数据。

12. 如权利要求 11 所述的数据隔离的装置，其特征在于，所述主通道的安全控制任务用于从所述常规数据区拷贝所述常规数据至所述安全控制任务的安全交换输入数据区，并分发至从通道。

30 13. 如权利要求 11 所述的数据隔离的装置，其特征在于，所述从通道的安全控制任务选取所述主通道分发的安全交换输入数据，并覆盖所述从通道的安全控制任务的安全交换

输入数据区。

14. 如权利要求 11 所述的数据隔离的装置，其特征在于，若所述从通道和所述主通道无法通讯，则从当前通道的常规数据区拷贝所需的常规数据到所述安全控制任务的安全交换输入数据区。