

Description

Method and Device for Data Isolation between Safety and Process Control Applications

Cross-Reference to Related Application

This embodiments of the disclosure claim priority to Chinese patent application No. 202011590531.2 filed on December 29, 2020 and entitled "Method and Device for Data Isolation between Safety and Process Control Applications", the disclosure of which is hereby incorporated by reference in its entirety.

Technical Field

The embodiments of the disclosure relate to the technical field of industrial process control, and in particular to a method and device for data isolation between safety and process control applications.

Background

In order to integrate the functional advantages of a safety control system and a process control system, improve the flexibility of deployment and application expansion of the control system, reduce the production and use costs of the control system, and the like, in the industrial application fields of oil and gas transmission, small critical control system, and the like, there has been an increasing need to support both safety control functions and process control functions in a same control system.

The safety control function is required to have high reliability and high availability, and needs to be developed and implemented according to relevant standards of functional safety. In safety control applications, a safety control application implementing a safety control function generally includes safety input data (generally referring to safety input signal points such as DI, AI, etc.), a safety control algorithm/function block, and safety output data (generally referring to safety output signal points such as DO, etc.). In general, process data (including process input/output signal points, process intermediate variables, and the like) is not allowed to directly enter or affect a safety application, and the running of a process control application is prevented from directly affecting the safety control application, otherwise the safety integrity of the safety control function may be reduced, that is, the isolation between the safety control application and the process control application needs to be guaranteed. Therefore, process data that the safety control application

accesses is restricted and small in size.

In a safety hybrid control system, in order to guarantee the functional integrity of the safety control application, a system architecture of multi-channel voting is generally adopted to improve fault tolerance. Each controller channel contains same safety control application and process control application and runs all control applications independently. The control system selects one channel as a master channel and the other channels as slave channels according to a certain strategy. The safety control application outputs externally through a specific software and hardware voting mechanism, for the process control application, generally, the master channel outputs, and the slave channels do not output.

In order to guarantee fault tolerance of the control system and availability of the process control function, the control system redundantly synchronizes process data of the master channel to the respective slave channels, which data include process input/output signal points and process variables associated therewith. A cycle to complete a round of redundant synchronization is long, which is generally a multiple of control cycle. The control system needs to avoid the problem that process data of the slave channel easily causes data rebound of safety application output after entering the safety control application, for example, when the process data changes (changes from a data value A to a data value B), the safety control application of each slave channel may immediately vote and output (outputs the data value B) due to the influence of the process data (the data value B), and then each slave channel receives the redundant process data (the data value A) before change from the master channel in a short time, and at the moment, each slave channel immediately votes and outputs the data before change (the data value A) due to influences of the process data, and then only when each slave channel receives the redundant process data (the data value B) after change from the master channel, the slave channel votes and outputs the data after change (the data value B) due to the influence.

In addition, since in actual control application scenarios, a process data area, a safety data area and an exchange data area are all structured data or a combination of multiple data, when a plurality of asynchronous tasks are possible to read and write these data areas at the same time, there is a need to guarantee exclusive read and write from task to task, thus avoiding that when one task rewrites part of the structured data, another task reads the structured data, resulting in incomplete or even erroneous data read from the latter.

There is a first processor for executing an unsafely application and a second processor special for executing a safety application in the related art. There is only one task in the safety application, which is to exchange data through a global data area, and mutually exclusive protection is carried

out on shared access to a memory by safety control and process control based only on a microcontroller system.

Summary

An objective of the embodiments of the disclosure is to achieve functional safety integrity, functional correctness, and control response characteristics of safety control applications in a multi-task-control and multi-channel-running industrial control system. A method and device for data isolation between safety and process control applications are provided.

A first aspect of the embodiments of the disclosure provide a method and device for data isolation between safety and process control applications, the safety control application includes a safety data area and a plurality of safety control tasks, and the safety control task includes a plurality of safety control programs; the process control application includes a process data area and a plurality of process control tasks, and the process control task includes a plurality of process control programs; and the method for data isolation includes: S1, an exchange data area is allocated for the control task in the safety control application/process control application; and S2, data isolation exchange between the safety and process control applications is performed on the basis of the allocated exchange data area.

Alternatively, S1 specifically includes: safety exchange data areas of independent and defined size based on a first capacity threshold respectively are allocated for the plurality of safety control tasks of the safety control application, and the safety exchange data areas includes a safety exchange input data area and a safety exchange output data area; and process exchange input data areas of independent and defined size based on a second capacity threshold respectively are allocated for the plurality of process control tasks of the process control application.

Alternatively, the safety exchange input data area is configured to store required process data copied from the process data area, which in turn is read by the safety control program under the safety control task; the safety exchange output data area is configured to store exchange variables of process data rewritten by the safety control task; and the process exchange input data area is configured to copy specified safety data from the safety exchange data area of the relevant safety control task, which in turn is read by the process control program under the process control task.

Alternatively, in S2, data isolation exchange includes, but is not limited to, via different memories, memory space partitions, access attribute settings, defining that the process control task cannot directly read and write the safety exchange input data area, but can read the process exchange input data area and the safety exchange output data area, and defining that the safety

control task cannot directly read and write the process exchange input data area, but can read the safety exchange input data area and rewrite the safety exchange output data area.

Alternatively, S21 specifically includes: S211, in the safety exchange input data area, a memory of corresponding exchange variables is allocated for the process data read by the safety control task, and in the safety exchange output data area, a memory of corresponding exchange variables is allocated for process data overwritten by the safety control task; S212, in the process exchange input data area, a memory of corresponding exchange variables is allocated for the safety data read by the process control task.

Alternatively, S22 specifically includes: S221, the safety control task is run to copy required process data to the safety exchange input data area from the process data area; and/or, S222, the process control task is run to copy the safety data to the process exchange input data area from the safety exchange output data area of the relevant control task; and S223, based on the running safety control task/process control task, the safety control task process control program is run.

Alternatively, the method for data isolation further includes: based on an access conflict resolution mechanism in which the process data area and the safety exchange output data area are preset respectively, read and write conflicts of the safety control task and the process control task on the process data area, the safety exchange input data area and the safety exchange output data area are avoided.

Alternatively, the access conflict resolution mechanism includes, but is not limited to, setting of priority of the control tasks, read and write locks among the tasks, double buffering of the data, and Memory Management Unit (MMU) memory protection.

A second aspect of the embodiments of the disclosure provide a device for data isolation between safety and process control applications, which at least includes two systems having multi-channel architectures, each channel is configured to run a plurality of safety control applications and/or a plurality of process control applications, the safety control application includes a safety data area and a plurality of safety control tasks, and the process control application includes a process data area and a plurality of process control tasks, and the safety data area and the process data area are mutually isolated; the process control task cannot rewrite the safety data area, and can only read and cannot rewrite a process exchange input area; and the safety control task cannot directly access the process data area, and can only read and cannot rewrite a safety exchange input data area of the safety exchange area.

Alternatively, one channel in the system of the multi-channel architecture serves as a master

channel and the other channels are slave channels, and safety data and process data can be transferred between the channels.

Alternatively, the safety control task of the master channel is configured to copy the process data to the safety exchange input data area of the safety control task from the process data area and distribute to the slave channels.

Alternatively, the safety control task of the slave channel selects the safety exchange input data distributed from the master channel and covers the safety exchange input data area of the safety control task of the slave channel.

Alternatively, if the slave channel and the master channels cannot communicate, the required process data is copied to the safety exchange input data area of the safety control task from the process data area of the current channel.

The beneficial technical effects of the invention are as follows.

1. A plurality of safety control tasks can be supported.

2. The safety data is effectively protected from being influenced by data, tasks/programs of the process control application, and the functional safety integrity of the safety control application is guaranteed.

3. The integrity of data exchange among the tasks in a multi-task running process is guaranteed.

4. The simultaneous real-time of data exchange of the tasks among multiple channels can be better solved, and control response real-time is guaranteed.

5. The invention is not only suitable for safety control applications and process control applications, but also more widely used in any industrial control system or device that requires a high degree of controllability, integrity, or real-time of data exchange among multiple tasks.

Brief Description of the Drawings

The drawings described herein serve to provide a further understanding of the embodiments of the disclosure and constitute a part of the embodiments of the disclosure, and the exemplary embodiments of the embodiments of the disclosure and descriptions thereof serve to explain the embodiments of the disclosure and are not to be construed as unduly limiting the embodiments of the disclosure. In the drawings:

Fig. 1 is a schematic flowchart of a method for data isolation between safety and process control applications according to an embodiment of the disclosure.

Fig. 2 is a schematic flowchart of a method for data isolation exchange between safety and process control applications according to an embodiment of the disclosure.

Fig. 3 is a partial schematic diagram of a device for data isolation between safety and process control applications according to an embodiment of the disclosure.

Fig. 4 is a partial schematic diagram of data isolation between safety and process control applications in a single channel according to an embodiment of the disclosure.

Fig. 5 is a partial schematic diagram of data isolation among a plurality of tasks of safety and process control applications in a single channel according to an embodiment of the disclosure.

Detailed Description of the Embodiments

For a further understanding of the embodiments of the disclosure, preferred implementation solutions of the embodiments of the disclosure will now be described in conjunction with embodiments, but it should be understood that these descriptions are only intended to further illustrate the features and advantages of the embodiments of the disclosure and are not intended to limit the claims of the embodiments of the disclosure.

For ease of understanding of the embodiments of the disclosure, some technical terms mentioned in the embodiments of the disclosure will be illustrated first.

Safety hybrid control system: refers to an industrial control system that contains both safety control applications and process control applications.

Channel: is a term specific to a system device with multiple voting architectures such as a functional safety control system. The channel is a basic processing unit of the multiplexed voting system architecture. A channel generally contains a CPU, a corresponding memory, and an associated microelectronic device. Each system channel runs control logic independently, and works asynchronously in parallel with the other channels. Generally, in a safety hybrid control system, each channel includes same safety control application and process control application, the safety control application outputs externally through a specific software and hardware voting mechanism (both the master and slave channels participate in simultaneously); and the process control application is generally a work/standby mechanism: the master channel outputs, and the slave channels do not output.

Safety control application: refers to a control application oriented to functional safety, with the function of monitoring the operating conditions of a production device, in case of abnormal operating conditions, it can promptly deal with according to defined safety control logic, so that hazards are minimized, and personnel and device are in a production safety state. The characteristic is high reliability, with wide use in the field of protection and control of key device and equipment, monitoring and protection of gas and fires, safety of oil and gas delivery processes, steam boiler monitoring and protection, protection of unit controls, etc. Criteria followed are mainly IEC 61508, GB/T20438, etc.

The safety control application does not allow random access of unsafely signal point data. The safety control application includes a safety data area and a plurality of safety control tasks, each safety control task includes a task background control program and a plurality of safety control programs, and each safety control program includes a plurality of safety control loops. Each safety control loop includes safety signal input/output points, and safety control logic.

Process control application: refers to a control application oriented to process control, applied to continuous measurement, process control, operation control management of a process production process, ensuring smooth operation of a production device. The process control application includes a process data area and a plurality of process control tasks, each process control task includes a task background control program and a plurality of process control programs, and each process control program includes a plurality of process control loops. Each process control loop includes process signal input/output points, and process control logic.

Safety data area: refers to a data area subordinate to the safety control application, generally including safety input signal data, safety output signal data, safety internal data, etc. The data area is generally structured data or a closely related data combination, and it needs to be guaranteed that the whole data structure or data combination can be completely read and written when the control task or control program reads or writes data, but not only part of the data is read and written.

Process data area: refers to a data area subordinate to the process control application, generally including process input signal data, process output signal data, process internal data, etc. Similarly, the data area is generally structured data or a closely related data combination, and it needs to be guaranteed that the whole data structure or data combination can be completely read and written when the control task or control program reads or writes data, but not only part of the data is read and written.

Task: contains a plurality of control programs, part of data, and task background control programs, and is subject object of control logic scheduling control in the control system. The

execution of the tasks is asynchronous and relatively independent, and there may be scenarios where multiple tasks access the same data at the same time.

Control program: contains a plurality of program segments, control logic is generally written in a programming language compliant with the IEC61131-3 standard.

Control loop: a basic unit of control logic, generally containing input signal point data, output signal point data, control algorithms or functional blocks, etc., such as a classical PID control loop.

The embodiments of the disclosure aim to solve the problem of data isolation between a safety control application and a process control application in a safety hybrid control system, and design a method and corresponding device for data isolation between safety and process control applications. The method and device for data isolation between safety and process control applications of the embodiments of the disclosure will be described in detail below in conjunction with the embodiments, so that those skilled in the art can better understand the technical solutions of the embodiments of the disclosure.

Fig. 1 is a schematic flowchart of a method for data isolation between safety and process control applications according to an embodiment of the disclosure, which includes the following steps.

S1, exchange data areas are allocated. Safety exchange data areas of independent and defined size are allocated for each safety control task of the safety control application, including a safety exchange input data area and a safety exchange output data area; and a process exchange input data area of independent and defined size is allocated for each process control task of the process control application. The safety exchange input data area is configured to store specified process data copied from the process data area, which is in turn read by the safety control program under the safety control task. The safety exchange output data area is configured to store exchange variables of process data rewritten by the safety control task. The process exchange input data area is configured to copy specified safety data from the safety exchange data area of the relevant safety control task, which in turn is read by the process control program under the process control task.

S2, data isolation exchange between the safety and process control applications is performed on the basis of the allocated exchange data areas.

As shown in Fig. 2, data exchange includes, but is not limited to, via different memories, memory space partitions, access attribute settings, defining that the process control task cannot directly read and write the safety exchange input data area, but can read the process exchange input data area and the safety exchange output data area, and defining that the safety control task

cannot directly read and write the process exchange input data area, but can read the safety exchange input data area and rewrite the safety exchange output data area. The operation specifically includes the following steps.

S21, variable memory is allocated.

In the safety exchange input data area, a memory of corresponding exchange variable is allocated for each process data input to the safety control task. The exchange variable corresponding to process data read by the safety control task is allocated to the safety exchange input data area; the exchange variable of process data rewritten by the safety control task is allocated to the safety exchange output data area; and the process exchange input variable corresponding to the safety exchange variable read by the process control task is allocated to the safety exchange input data area.

S22, the safety exchange input data area/the process exchange input data area is updated and read.

Specifically, the safety exchange input data area is updated and read, when each safety control task is run, the specified part of process data is copied to the corresponding safety exchange input data area from the process data area, and then each safety control program subordinate to the safety control task is run.

Alternatively, the process exchange input data area is updated and read, when each process control task is run, the specified part of data is copied to the process exchange input data area from the safety exchange output data area of the relevant safety control task, and then each process control program subordinate to the process control task is run.

It is to be noted that the operations of the safety control tasks and the process control tasks are independent and asynchronous, and the steps of updating and reading the safety exchange input data area and updating and reading the process exchange input data area can be executed concurrently.

In addition, in order to guarantee the correctness and integrity of the process data read by the safety control task and avoid the read and write conflicts of the safety control task and the process control task to the process data area, the device adopts access conflict solution mechanisms such as setting of priority of the control task, read and write locks among tasks, double buffering of data, or MMU memory protection and the like.

In some implementation modes, it is preferably guaranteed that the process control task is

allowed to rewrite the process data area only after the safety control task reads the process data area.

In the following illustrated embodiments, Fig. 3 is a partial schematic diagram of a device for data isolation between safety and process control applications according to an embodiment of the disclosure. The device at least includes two systems having multi-channel architectures, each channel is configured to run a plurality of safety control applications and/or a plurality of process control applications, the safety control application includes a safety data area and a plurality of safety control tasks, the process control application includes a process data area and a plurality of process control tasks, and the safety data area and the process data area are mutually isolated. The process control task cannot rewrite the safety data area, and can only read and cannot rewrite a process exchange input area; and the safety control task cannot directly access the process data area, and can only read and cannot rewrite a safety exchange input data area of the safety exchange area.

In Fig. 3, the device includes a master channel and two slave channels, and the control tasks among the channels and contained control programs are the same. The safety control task of the master channel is configured to copy part of the specified process data to the safety exchange input data area of the master channel from the process data area of the master channel and rapidly distribute to the slave channels 1# and 2#. Rapidly generally refers to that the safety control tasks of the slave channel 1# and the slave channel 2# select the safety exchange input data from the master channel within a basic control cycle or task cycle. When the slave channel and the master channel is disconnected, the safety control tasks of the slave channel 1# and the channel 2# copy part of specified process data to the safety exchange input data area of the safety control task from corresponding process data areas.

The method and device for data isolation between safety and process control applications illustrated in the above embodiments will be further described below through specific operation examples, so that those skilled in the art can better understand the technical solutions of the embodiments of the disclosure.

Fig. 4 is a partial schematic diagram in a single channel, each channel in the figure includes a process control application and a safety control application, and the data and programs of the safety control application and the process control application are relatively independent and isolated from each other. The process control application includes a process data area and a plurality of process control tasks, and the process control application includes a safety data area and a plurality of safety control tasks.

Generally, the process control tasks can directly read data in the safety data area. However, in order to facilitate integrity and contextual consistency of the safety data read during execution of the process control task, in the embodiments of the disclosure, as shown in Fig. 4, data with higher structural or contextual consistency requirements may be allocated to the safety exchange output data area, and the process exchange input data area passes them to the process control task.

Each safety control task allocates a dedicated safety exchange input data area. When each safety control task is run each time, the part of specified process data is copied to the safety exchange input data area from the process data area, and then each safety control program subordinate to the safety control task is run. The device defines, through memory space partitions, access attribute settings, etc., that the safety control program can only read and cannot rewrite the safety exchange input data area.

As shown in Fig. 4, each safety control task allocates a dedicated safety exchange input data area, and each process control task aligns a dedicated process exchange input data area. The device defines, through different memories, memory space partitions, access attribute settings, etc., that the process control task can directly read the process exchange input data area, and the safety control task cannot directly access the process exchange input data area. Similarly, the safety control task can read and write the safety exchange output data area, and each process control program in the process control task cannot directly access the safety exchange output data area.

When each process control task is run, the specified part of data is copied to the process exchange input data area from the safety exchange output data area of the relevant safety control task, and then each process control program subordinate to the process control task is run. In order to guarantee the correctness and the integrity of the safety exchange output data read by the process control task and avoid the read and write conflicts of the safety control task and the process control task to the safety exchange output data area, through access conflict solution mechanisms such as setting of priority of the control task, read and write locks among the tasks, double buffering of data, or an MMU memory protection mechanism and the like, it is guaranteed that the process control task is allowed to read the safety exchange output data area only after the safety control task rewrites the safety exchange output data area.

Fig. 5 is a partial schematic diagram of data isolation among a plurality of safety control tasks and a plurality of process control tasks, a process control application and a safety control application are run in a single channel of the device of the embodiment of the disclosure, and the safety control application includes a safety control task 1# and a safety control task 2#; and the process control application includes a process control task 1# and a process

control task 2#. It is to be noted that the safety control application and the process control application can include a plurality of control tasks, and the safety control tasks and process control task rare relatively independently and run asynchronously. For illustrative clarity in the embodiment, only two control tasks each are shown. The running rules of the safety control task and the process control task are as follows.

1. The safety control task 1# and safety control task 2# can simultaneously and independently read respective specified data of the process data areas and copy to the safety exchange input data 1# and safety exchange input data 2#, respectively.

2. The process control task 1# and process control task 2# can simultaneously and independently read the specified data in the safety exchange output data area 1# and the safety exchange output data area 2# of the relevant safety task and copy to the process exchange input data area 1# and process exchange input data area 2#, respectively.

The above description of the embodiments is intended only to assist in understanding the method of the embodiments of the disclosure and its core idea. It should be noted that those of ordinary skill in the art can also make several modifications and improvements without departing from the principle of the embodiments of the disclosure, and these modifications and improvements all fall within the scope of protection of the embodiments of the disclosure. The technical features of the above-described embodiments may be randomly combined, and not all possible combinations of the technical features in the above-described embodiments are described for simplicity of description, however, as long as the combinations of the technical features do not contradict each other, they should be considered to be within the scope of the description of the present specification.

Claims

1. A method for data isolation between safety and process control applications, wherein

the safety control application comprises a safety data area and a plurality of safety control tasks,
and the safety control task comprises a plurality of safety control programs;

the process control application comprises a process data area and a plurality of process control
tasks, and the process control task comprises a plurality of process control programs;

the method for data isolation comprises:

S1, allocating an exchange data area for the control task in the safety control application and/or
process control application;

S2, performing data isolation exchange between the safety and process control applications
according to the allocated exchange data area.
2. The method for data isolation as claimed in claim 1, wherein S1 comprises:

allocating safety exchange data areas of independent and defined size based on a first
capacity threshold respectively for the plurality of safety control tasks of the safety control
application, wherein the safety exchange data areas comprise a safety exchange input data
area and a safety exchange output data area;

allocating process exchange input data areas of independent and defined size based on a
second capacity threshold respectively for the plurality of process control tasks of the process
control application.
3. The method for data isolation as claimed in claim 2, wherein the safety exchange input data
area is configured to store required process data copied from the process data area, which in
turn is read by the safety control program under the safety control task;

the safety exchange output data area is configured to store exchange variables of process data
rewritten by the safety control task;

the process exchange input data area is configured to copy specified safety data from the
safety exchange data area of the relevant safety control task, which in turn is read by the
process control program under the process control task.
4. The method for data isolation as claimed in claim 2, wherein in S2, data isolation exchange
comprises, but is not limited to, via different memories, memory space partitions, access
attribute settings, defining that the process control task cannot directly read and write the safety

exchange input data area, but can read the process exchange input data area and the safety exchange output data area, and defining that the safety control task cannot directly read and write the process input data area, but can read the safety exchange input data area and rewrite the safety exchange output data area.

5. The method for data isolation as claimed in claim 1, wherein S2 comprises:

S21, allocating a memory of variables;

S22, updating and reading the safety exchange input data area and/or the process exchange input data area.

6. The method for data isolation as claimed in claim 5, wherein S21 comprises:

S211, in the safety exchange input data area, allocating memory of corresponding exchange variables for process data read by the safety control task; in the safety exchange output data area, allocating a memory of corresponding exchange variables for process data rewritten by the safety control task;

S212, in the process exchange input data area, allocating memory of corresponding exchange variables for safety data read by the process control task.

7. The method for data isolation as claimed in claim 5, wherein S22 comprises:

S221, running the safety control task to copy required process data to the safety exchange input data area from the process data area;

and/or, S222, running the process control task to copy safety data to the process exchange input data area from the safety exchange output data area of the relevant control task;

S223, based on the running safety control task, running the safety control program, or based on the running process control task, running the process control program.

8. The method for data isolation as claimed in claim 2, wherein the method further comprises: based on an access conflict resolution mechanism in which the process data area and the safety exchange output data area are preset, respectively, avoiding read and write conflicts of the safety control task and the process control task on the process data area, the safety exchange input data area and the safety exchange output data area.

9. The method for data isolation as claimed in claim 8, wherein the access conflict resolution mechanism comprises setting of priority of control tasks, read and write locks among tasks, double buffering of data, and MMU memory protection.

10. A device for data isolation between safety and process control applications, at least comprising two systems having multi-channel architectures, wherein each channel is configured to run a plurality of safety control applications and/or a plurality of process control applications, the safety control application comprises a safety data area and a plurality of safety control tasks, the process control application comprises a process data area and a plurality of process control tasks, and the safety data area and the process data area are mutually isolated;
- the process control task cannot rewrite the safety data area, and can only read and cannot rewrite a process exchange input area of the process data area;
- the safety control task cannot directly access the process data area, and can only read and not rewrite the safety exchange input data area of the safety exchange area.
11. The device for data isolation as claimed in claim 10, wherein one channel in the system of the multi-channel architecture serves as a master channel and the other channels are slave channels, and the channels are configured to transfer safety data and process data.
12. The device for data isolation as claimed in claim 11, wherein the safety control task of the master channel is configured to copy the process data to the safety exchange input data area of the safety control task from the process data area and distribute to the slave channels.
13. The device for data isolation as claimed in claim 11, wherein the safety control task of the slave channel selects the safety exchange input data distributed from the master channel and covers the safety exchange input data area of the safety control task of the slave channel.
14. The device for data isolation as claimed in claim 11, wherein if the slave channel and the master channel cannot communicate, the required process data is copied to the safety exchange data area of the safety control task from the process data area of the current channel.