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；

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；

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.

2. The method for data isolation as claimed in claim 1, 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 exchange process input data area, but can read the safety exchange input data area and rewrite the safety exchange output data area.

3. 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.

4. The method for data isolation as claimed in claim 3, 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.

5. The method for data isolation as claimed in claim 3, 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.

6. The method for data isolation as claimed in claim 1, 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.

7. The method for data isolation as claimed in claim 6, 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.

8. 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;

the device is configured to allocate 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;

allocat 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；

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.

9. The device for data isolation as claimed in claim 8, 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.

10. The device for data isolation as claimed in claim 9, 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.

11. The device for data isolation as claimed in claim 9, 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.

12. The device for data isolation as claimed in claim 9, 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.