



Independence Principles Used in the Design of the FPGA-based Safety I&C Platform NicSys8000N



NicSys[®] 8000N

安全级DCS 平台
Safety I&C Platform

Chenghua Liang

Oct. 5th 2016

◆ Presentation Overview

- Introduction
- Standard Requirements for Independence
- Advantages of FPGA technology about independence
- Isolation and independence principles used
in the design of the FPGA-based safety I&C platform
NicSys8000N
- Conclusion



◆ Introduction

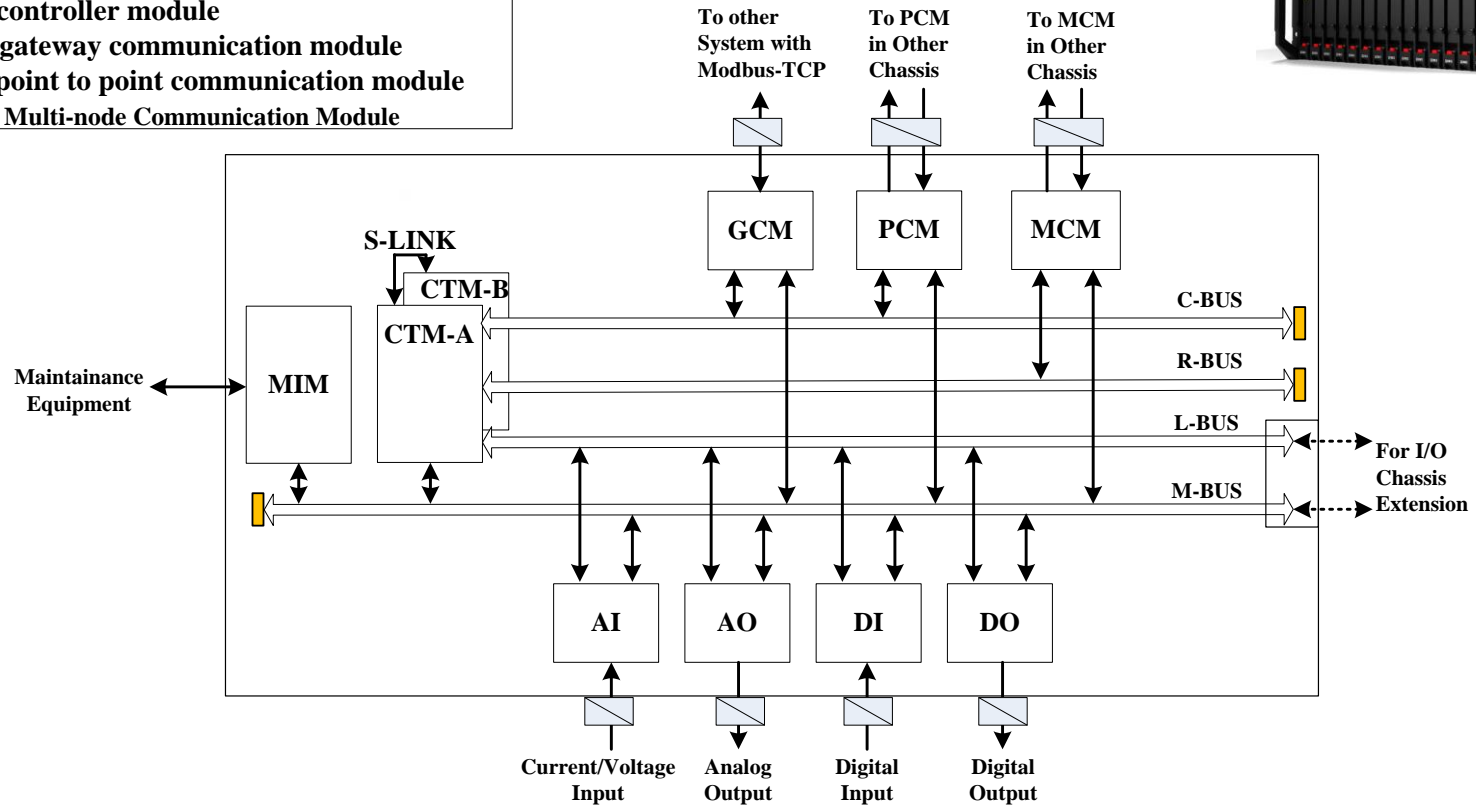
- The NicSys8000N platform is a **hardware-based** architecture system with **high reliability and integrity**.
- The key component in the NicSys8000N platform is the field-programmable gate array (FPGA). The FPGA logic components can be programmed to duplicate the functionality of basic logic gates (such as AND, OR, XOR and NOT). These logic components can be combined into complex combinational functions such as decoder or other math functions.



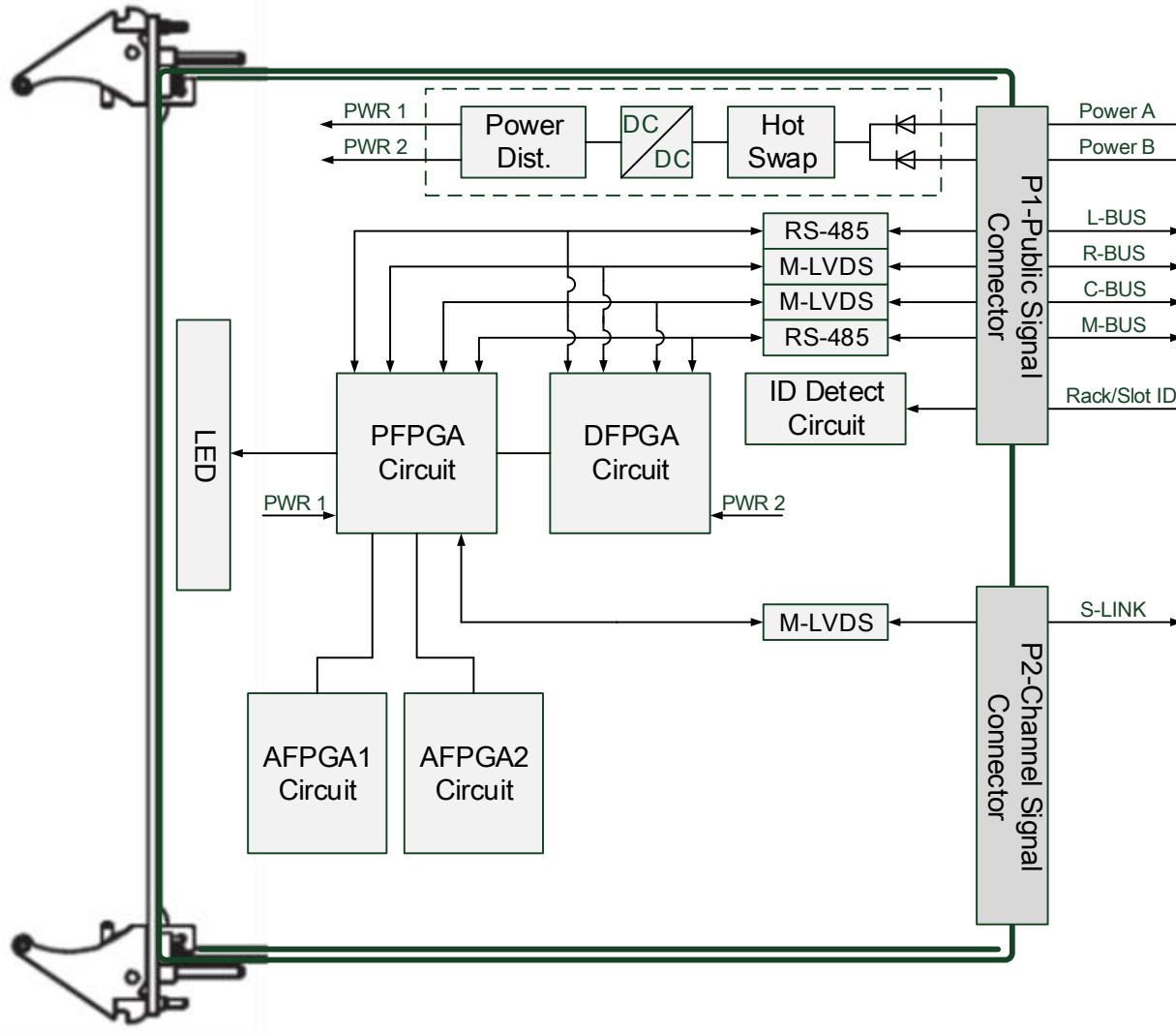
◆ Structure of NicSys8000N platform



MIM: maintenance module
CTM: controller module
GCM: gateway communication module
PCM: point to point communication module
MCM: Multi-node Communication Module



◆ Structure of Controller



◆ Standard Requirements for Independence

RG 1.75 CRITERIA FOR INDEPENDENCE OF ELECTRICAL SAFETY SYSTEM

IEC 61513 Nuclear power plants - instrumentation and control for systems important to safety - General requirements for systems (6.1.2.2.independence)

IEEE 603 Criteria for Safety Systems for Nuclear Power Generating Stations(5.6independence)

PHYSICAL SEPARATION

IEC 60709 Nuclear power plants - instrumentation and control for systems important to safety - Separation

IEEE 384 1E Standard Criteria for independence of Class 1E Equipment and Circuits

NUREG-0800 APPENDIX 7.1-C Guidance for evaluation of conformance to IEEE Std.603 review responsibilities

ELECTRICAL ISOLATION

IEEE 384 Standard Criteria for independence of Class 1E Equipment and Circuits

NUREG-0800 APPENDIX 7.1-C Guidance for evaluation of conformance to IEEE Std.603 review responsibilities

COMMUNICATION INDEPENDENCE

IEEE 7.4.3.2 Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations (Annex E communication independence)

NUREG-0800 APPENDIX 7.1-C Guidance for evaluation of conformance to IEEE Std.603 review responsibilities



◆ The Advantages of FPGA in Independence

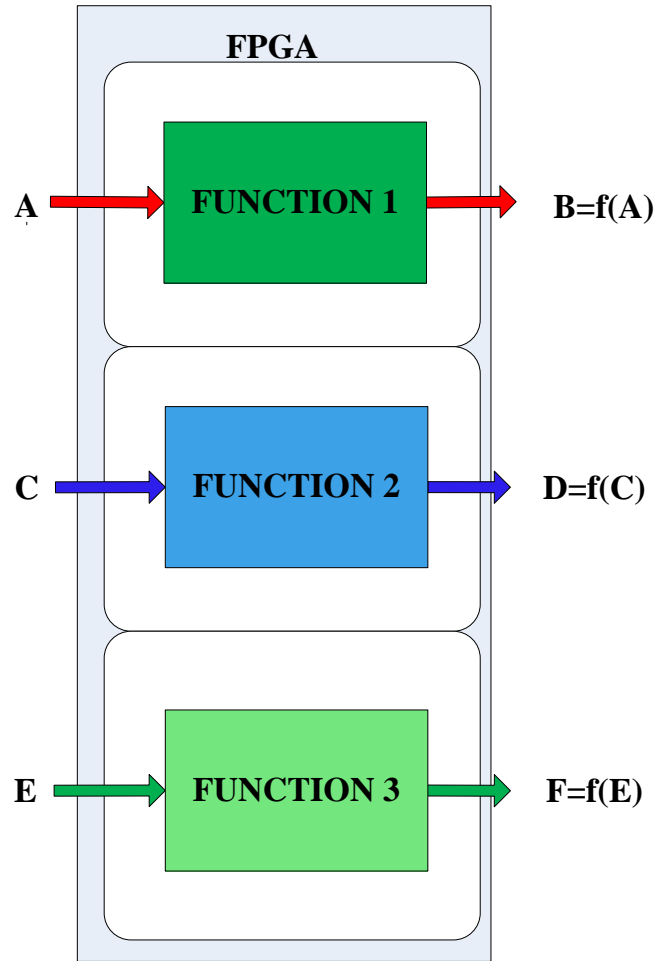
➤ Parallel process

➤ Large and flexible dual port RAM

➤ Physical independence



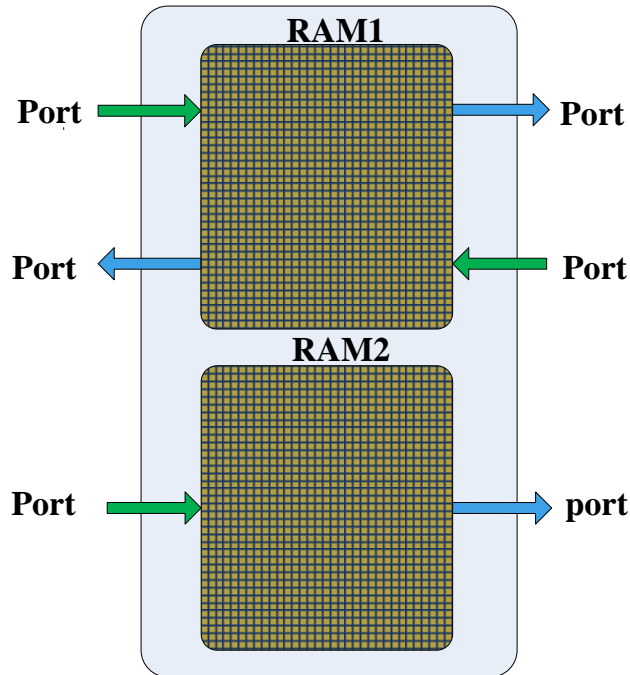
◆ The Advantages of FPGA in Independence



Parallel process

- FUNCTION 1, FUNCTION 2 and FUNCTION 3 can be executed simultaneously and independently.

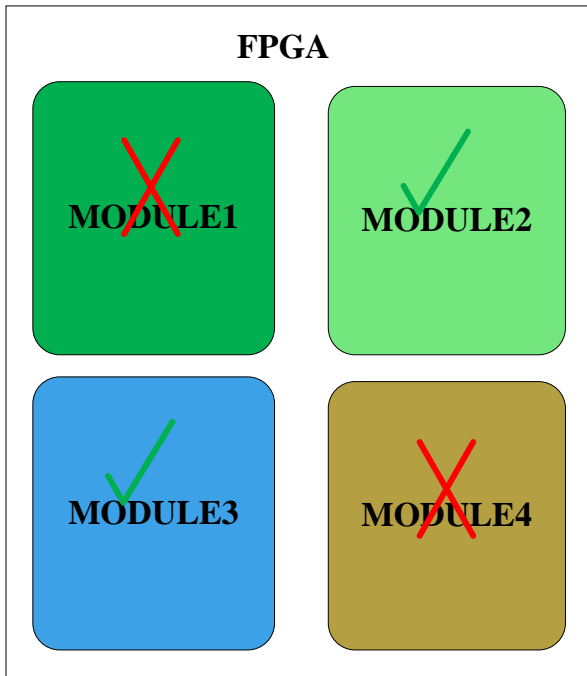
◆ The Advantages of FPGA in Independence



Flexible dual port RAM

- You can design as you want:
 - The memory capacity
 - The number of ports and the type of ports (such as read or write)

◆ The Advantages of FPGA in Independence



Physical independence

- Even there are several modules are failure, the others can be functioned normally.



◆ Independence Principles Used in the Design

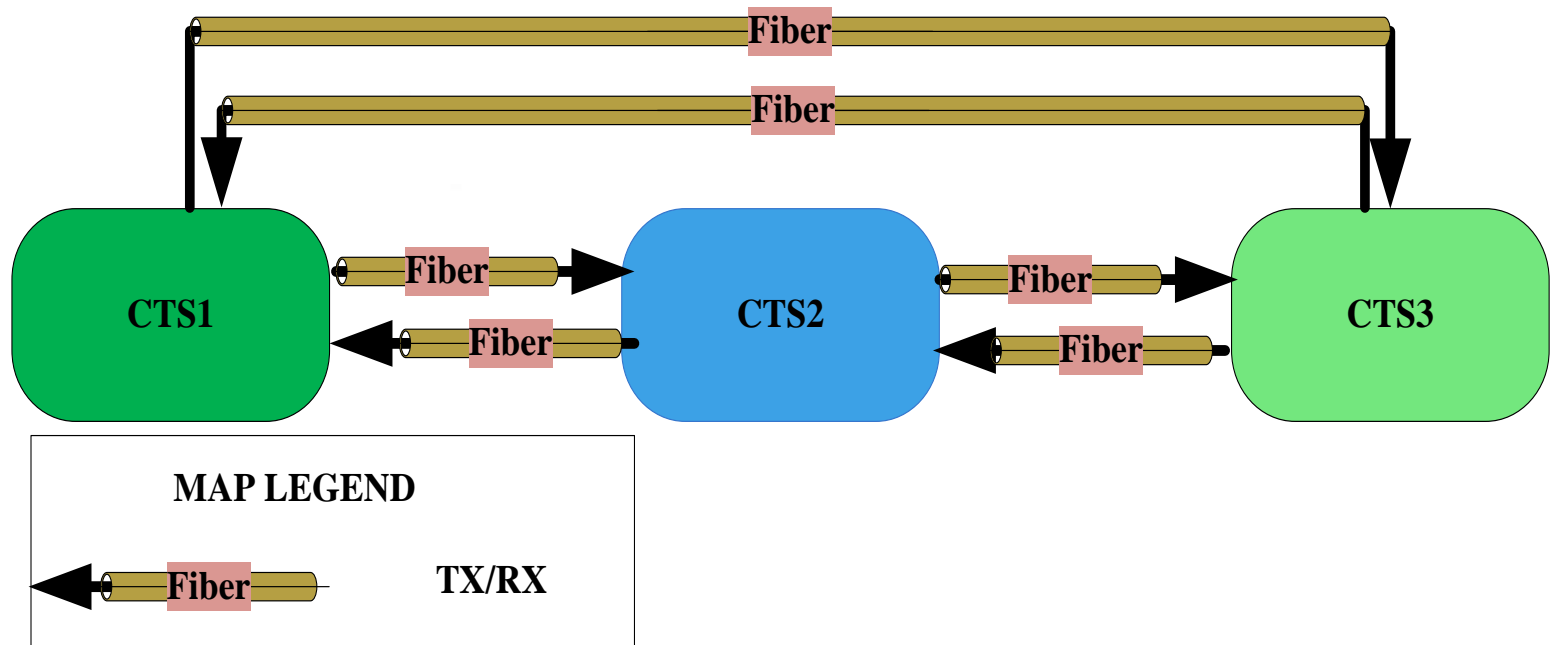
Physical Separation

- Structural design ensure physical separation.
The horizontal distance between the modules in the same chassis is strictly limited . The different chassis keep vertical distance in one cabinet .
- During engineering implementation ,physical separation between each part also be considered.



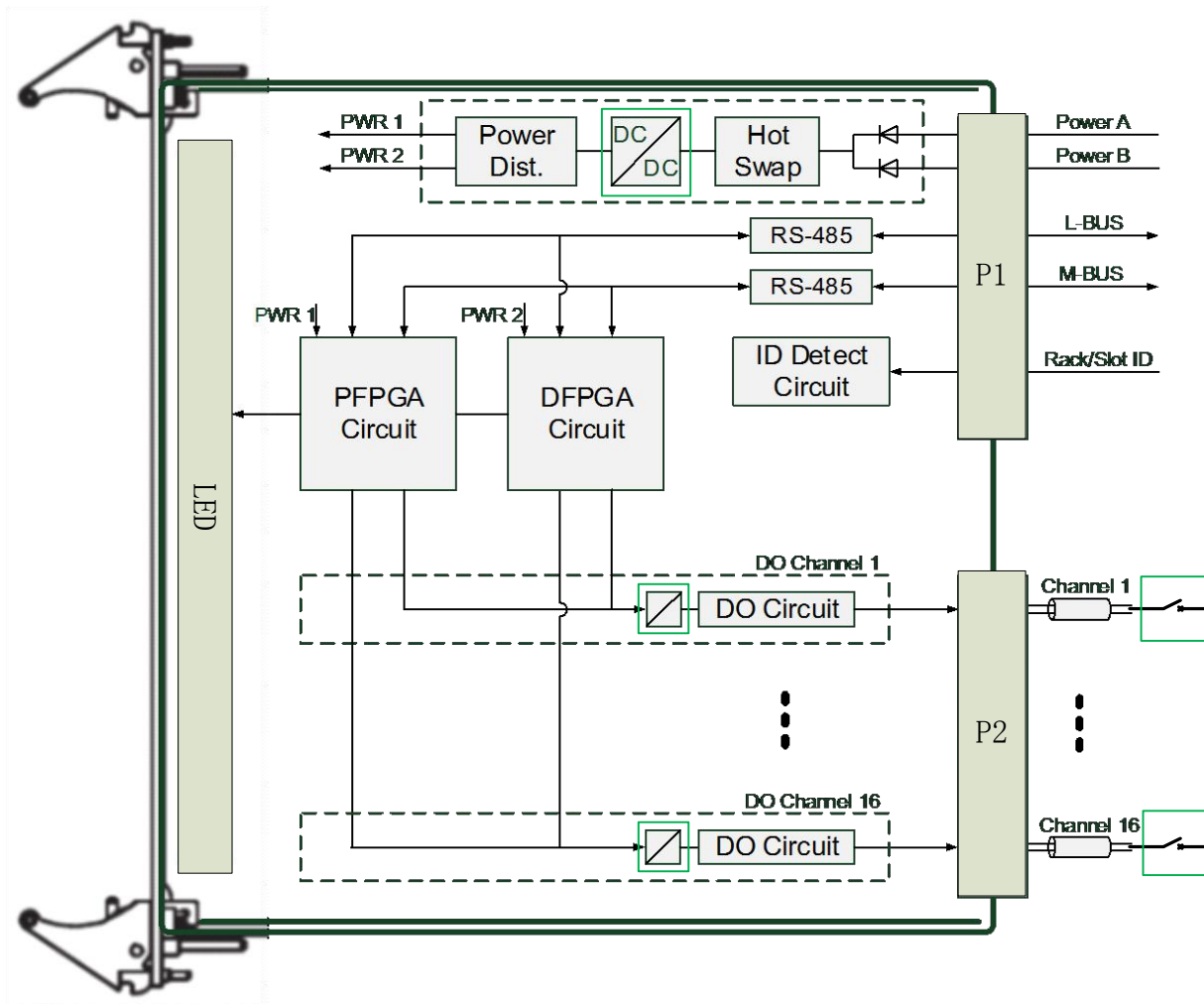
◆ Independence Principles Used in the Design

Electrical Isolation of Communication Module



◆ Independence Principles Used in the Design

Electrical Isolation of I/O Module

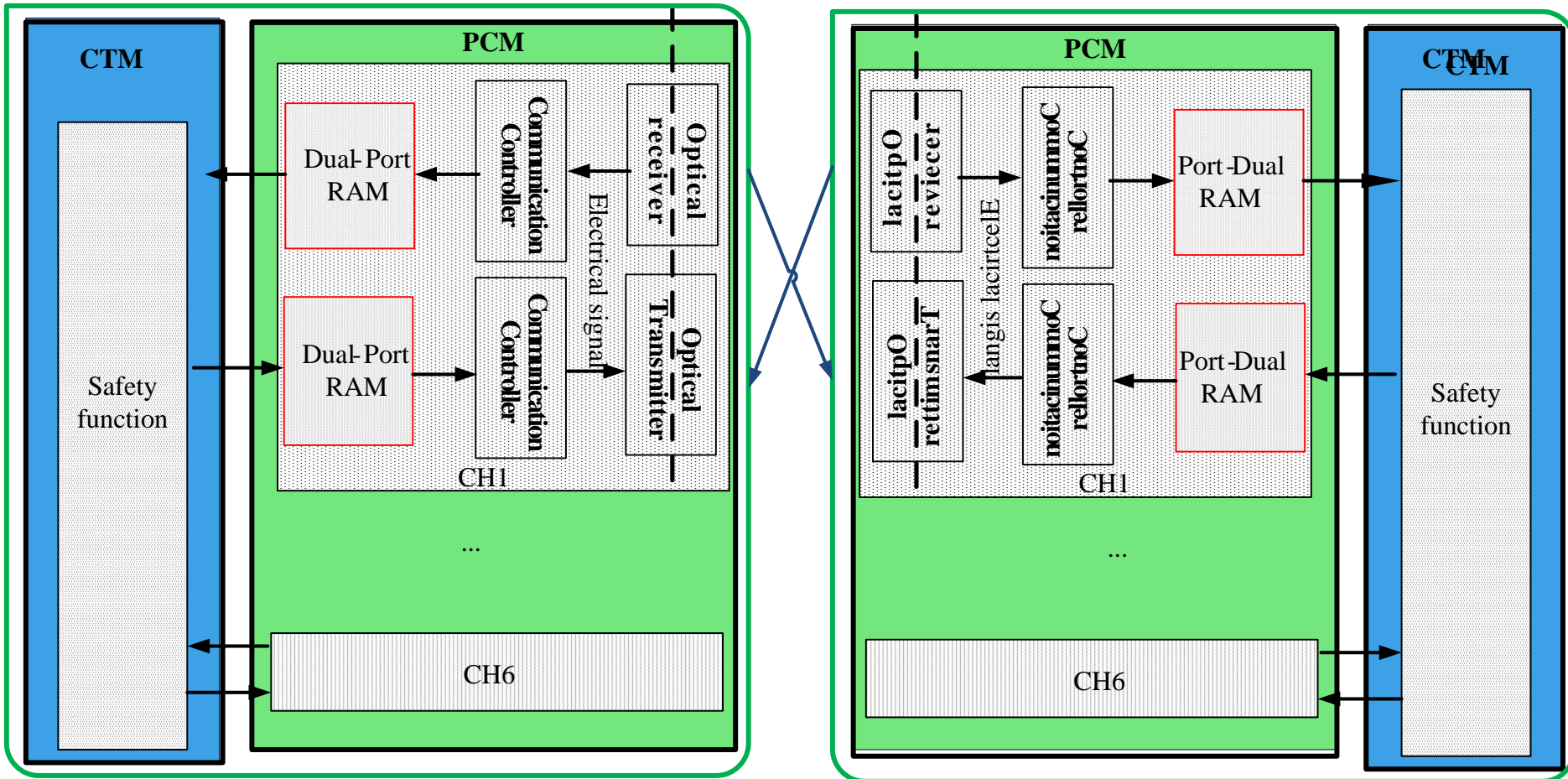


◆ Independence Principles Used in the Design

Communication Independence (Communication and Safety Function)

Station1

Station2



◆ Independence Principles Used in the Design

Communication Independence(Communication and Safety function)

1

- Communication and safety function is independent

2

- Designed up to six TX/RX fiber channels using large and flexible dual port RAM

3

- Six channels work in parallel and independently

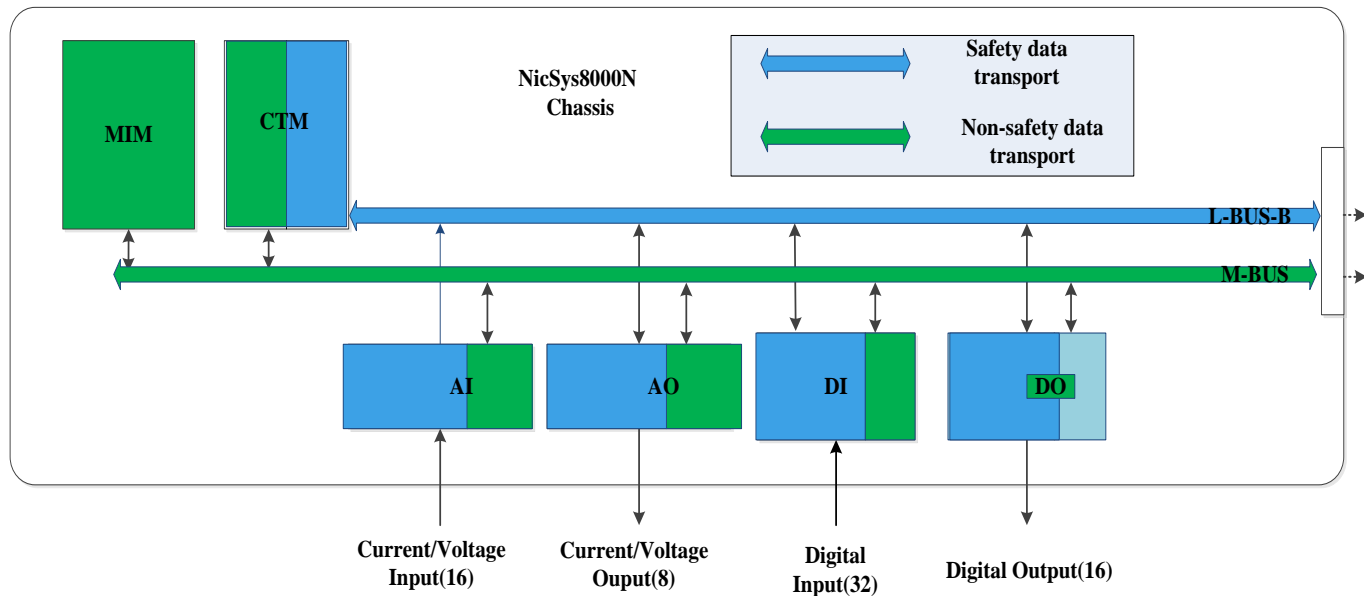
4

- Transport speed up to 100Mbps using pip-line technology



◆ Independence Principles Used in the Design

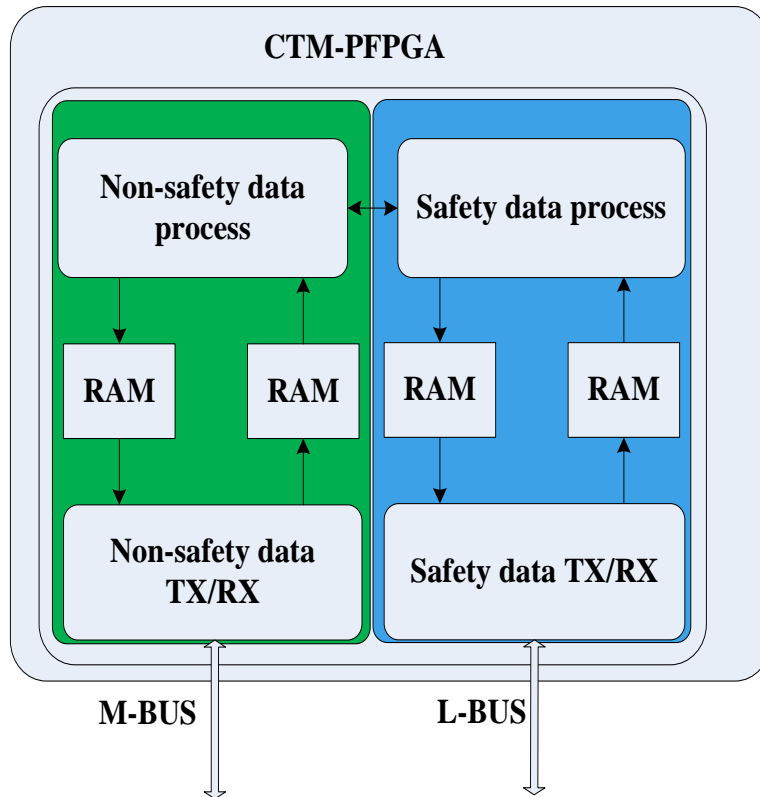
Communication Independence(Safety Data and Non-safety data)



Safety and non-safety communication exchange data through different channels.

◆ Independence Principles Used in the Design

Communication Independence(Safe data and Non-safe data)

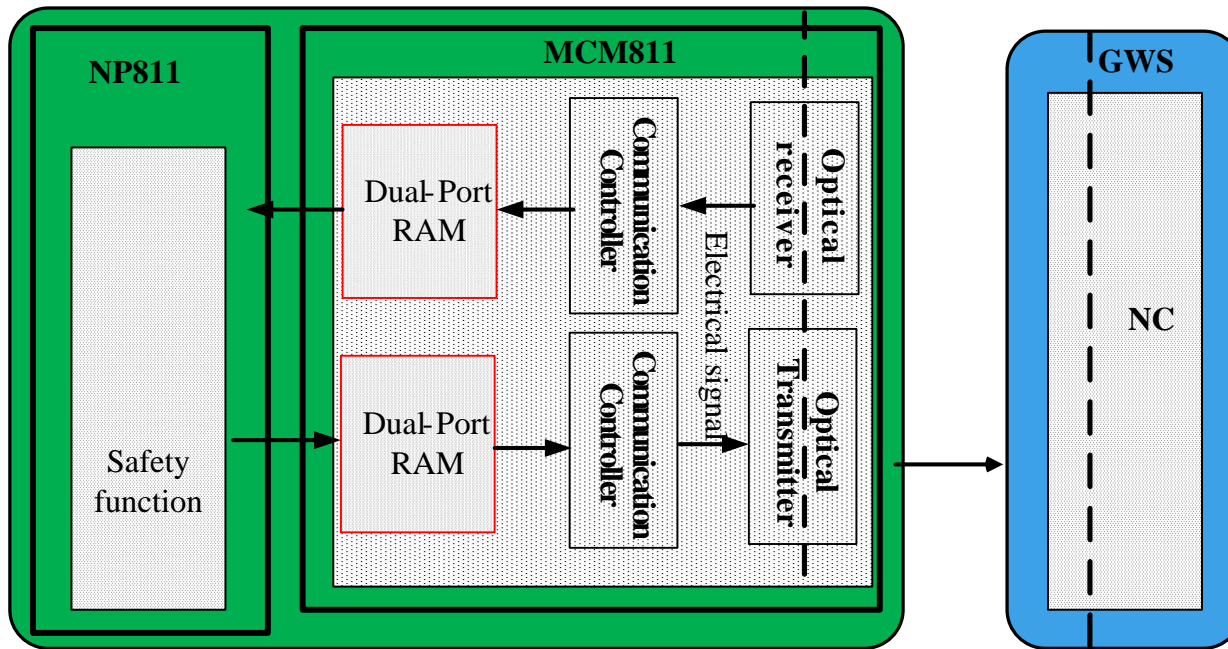


- Constrain Non-safety data process module and safety data process module in different regions
- Non-safety communication and safety communication use IO pins from different bank



◆ Independence Principles Used in the Design

Communication Independence(different systems)



This communication module is used to communication safety system with other non-safety systems.



◆ Conclusion

The design of NicSys8000N platform consider:

Physical separation

Electrical isolation

Communication independence

NicSys8000N platform is a safety instrumentation and control(I&C) system meeting the independence standard



Thank you !

Liang Chenghua

China Nuclear Control System Engineering Co., Ltd (CNCS)

Logic Design Engineer

liangchenghua@cncs.bj.cn

