The Development of Safety DCS Platform - NicSys®8000N Based on FPGA

Liu Zhikai, Hu Yiwu

China Nuclear Control System Engineering Co., Ltd., Beijing 100176, China

INTRODUCTION

This paper describes the safety Nuclear I&C System - NicSys®8000N designed by China Nuclear Control System Engineering Co., Ltd. NicSys®8000N is a general safety distributed control system (DCS) platform and is developed specifically for nuclear applications, the core processing part of the platform is based on field programmable gate array (FPGA) technology. Moreover the modular structure, deterministic response time and testability can be applied to solve plant-wide needs for nuclear safety applications. NicSys®8000N platform complies with China nuclear design codes, guidelines and standards as well as the U.S.Nuclear Regulatory Commission (NRC) guidelines, International Electrotechnical Commission (IEC), International Atomic Energy Agency (IAEA) and Institute of Electrical and Electronics Engineers (IEEE) standards, the platform has been developed using a rigorous safety-related design process that ensures suitable FPGA logic, hardware and software quality and reliability for critical applications such as the reactor protection system or engineered safety features actuation system. The information provided in this paper covers the following topics to fully understand the NicSys®8000N platform: description and development process of NicSys®8000N, architecture and application development tools of NicSys®8000N, technical features of NicSys®8000N, and qualification test of NicSys®8000N.

Platform Composition

NicSys®8000N consists of a series of hardware,[1] programmable logic[2] and software components.

Platform Function

NicSys®8000N is a general safety DCS platform and is developed specifically for nuclear applications. The general functions of NicSys®8000N are as follows.[3]

- Input/output function
- Data communication function
- Logic process function
- Controller redundancy function
- Self-diagnosis function
- Display and operation function

Platform Performance

- Capacity
  - I/O capacity: 1536 binary I/O or 768 analog I/O (single Controller Module (CTM))
  - Display page capacity: 500 pages (single Display Process Module (DPM))
- Accuracy
  - Analog input: ±0.1% full scale
  - Analog output: ±0.1% full scale
- Operation cycle
  - CTM cycle: 15ms fixed
  - DPM cycle: 100ms fixed
- Safety Communication
  - Communication cycle: 7.5ms for Point-to-point Communication Module (PCM), 15~100ms configurable for Multi-node Communication Module (MCM)
  - Communication capacity: 1Kbyte/cycle for PCM, 12Kbyte/cycle for MCM
  - Communication node: up to 64 nodes for MCM
- Self-diagnosis
  - Diagnose Coverage: better than 90% for FPGA based module
- Environment
  - Temperature: 5~35℃
  - Humidity: 10%~80%, non-condensing
  - Air: No salt
  - Atmospheric pressure: 0.086~0.106MPa

Development Lifecycle

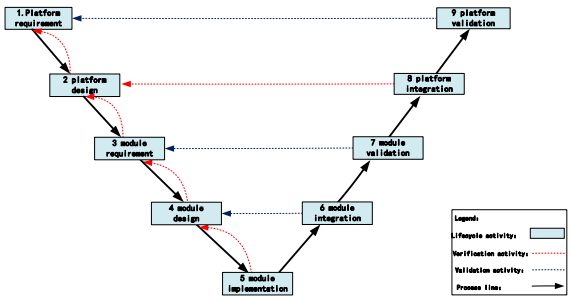

Fig. 1. The Lifecycle of Developing NicSys®8000N

Platform architecture

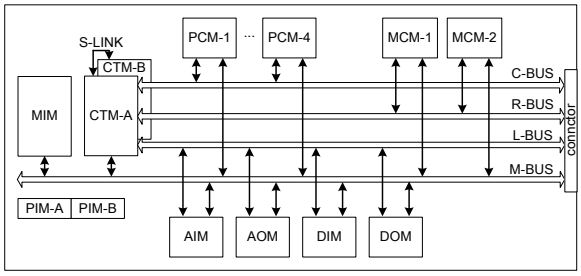

Fig. 2. The Typical Architecture of NicSys®8000N

Technical Features

All FPGA based NicSys®8000N modules have been designed similarly. Fig. 3. shows a generic standard layout of a NicSys®8000N Module.

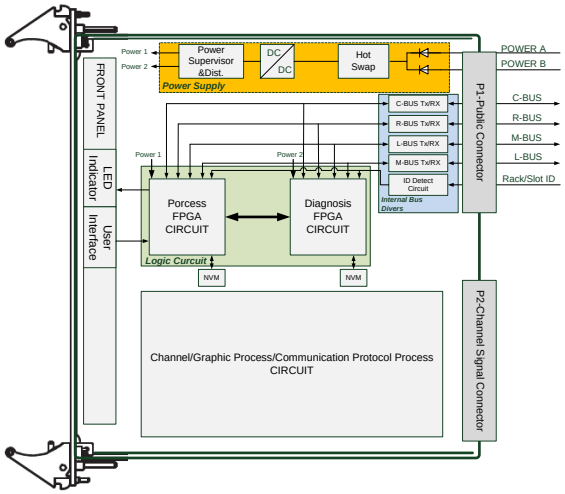

Fig. 3. Common Design of NicSys®8000N Module

The FPGA logic circuit has two on-board FPGAs, the PFPGA and the DFPGA. The dual on-board FPGA structure gives NicSys®8000N FPGA based module superior reliability and diagnostic function. The PFPGA handles system level redundant communication and performs logic executions. The DFPGA is used to diagnosis the integrity of the PFPGA, and perform data verification for each internal system execution.

In particular, the CTM has two algorithm FPGAs (AFPGA1 and AFPGA2) in addition to PFPGA and DFPGA. AFPGA1 and AFPGA2 are algorithm executing units, performing the application logic calculation function with redundancy configuration.

Qualification

Nicsys®8000N qualification process is divided into four stages, the test sequence for the equipment is identified as follows:[4]

- The benchmark test—Equipment compliance inspection, benchmark functional performance test, and caution test.
- Electro Magnetic Compatibility (EMC) test[5] — electromagnetic interference test of conductive (CE, CS) and radiation (RE, RS).
- Environmental test—Testing and/or evaluation of equipment performance over time, including thermal aging, mechanical aging and aging test.
- Seismic test—Tests under conditions of the accident and after the accident.

All the four kinds of test have been conducted during 2017. The test data supports the ability of the NicSys®8000N to operate during and after the corresponding event. The acceptance criterion for these tests includes no loss of safety function, no spurious actuations, performance within the required accuracy and timing, and maintenance of structural integrity (i.e., no broken or loose parts) during and following testing.

RESULTS

The platform uses a rigorous safety-related design process that ensures suitable FPGA logic, hardware and software quality and reliability for critical applications such as the reactor protection system or engineered safety features actuation system. Nuclear Instrumentation System-RNI of Karachi K-2/K-3 project in Pakistan is the first application of NicSys®8000N. The prototype of the system has completed the equipment qualification, and the supply will be completed in 2018.

REFERENCES

1. IEC 61513, "NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL FOR SYSTEMS IMPORTANT TO SAFETY – GENERAL REQUIREMENTS FOR SYSTEMS," International Electrotechnical Commission, first edition (2001).
2. IEC 62566, "Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions," IEC Central Office, 3, rue de Varembé CH-1211 Geneva 20 Switzerland (2012).
3. Feng Wei, He Peng, Liu Feiyang, etc., "FUQING NPP UNITS 5&6 PROJECT RPS SYSTEM REQUIREMENT SPECIFICATION," Nuclear Power Institute of China, Revision F, pp.12-62 (2016).
4. IEC 61508, "Functional safety of electrical/electronic/programmable electronic safety-related systems," IEC Central Office, 3, rue de Varembé CH-1211 Geneva 20 Switzerland. Part1-Part7 (2010).
5. TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," EPRI Working Group on Qualification of Commercially Available Programmable Logic Controllers for Safety Related Applications with S. Levy Incorporated 3425 S. Bascom Avenue Campbell, California 95008 (1996).