Transactions of the Korean Nuclear Society Spring Meeting
Jeju, Korea, May 22, 2009

Performance Testing Methodology for Safety-Critical Programmable Logic Controller

Chang Ho Kim*, Do Young Oh, Ji Hyeon Kim, Sung Ho Kim, Se Do Sohn
Korea Power Engineering Company (KOPEC)
kimch@kopec.co.kr

1. Introduction

The Programmable Logic Controller (PLC) for use in Nuclear Power Plant safety-related applications is being developed and tested first time in Korea. This safety-related PLC is being developed with requirements of regulatory guideline and industry standards for safety system. To test that the quality of the developed PLC is sufficient to be used in safety critical system, document review and various product testings were performed over the development documents for S/W, H/W, and V/V. This paper provides the performance testing methodology and its effectiveness for PLC platform conducted by KOPEC.

2. Basis for Performance testing

For digital I&C systems, the applicant should meet the guidance in Reg. Guide 1.152 [2], which endorses IEEE Std 7-4.3.2 [1], "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations," and set of software engineering standards which describe the software development process. This includes, as a minimum, a conformance to the software engineering regulatory guides (Reg. Guide 1.168 through 1.173).

The performance requirements are selected from IEEE Std 7-4.3.2 and a set of Reg. Guide for safety software developments, Nuclear I&C safety system design experience, software design experience and licensing experience.

The performance testings in the paper are different and diverse methods from the vendor's development and validation testings, which are performed during PLC platform development and testing phase. It also is performed in the view of the application software developer and end user of platform.

3. Performance Testing for Real Time OS

3.1 Test Method

The real time OS testing has three objectives as followings;

- To verify that system timing requirements, calculated and allocated to the digital system, have been satisfied in the safety system with under multi task environments.
- To verify that software operates correctly within time and memory size constraints.
- To verify that the priority of the task under the interrupt with context switching operates as expected.

First, to test the deterministic performance, total five tasks whose cycle times are 50, 250, 500, 2,000, 10,000 msec of the Core Protection Calculator System (CPCS), are allocated. To test memory size constraints, each task has function blocks which have the required number of inputs and outputs classified by type (Boolean, Integer, Real). Function blocks are compiled in the environment of the ANSI C. During test, each task outputs logic zero (0) at starting point of the every odd cycle, and logic one (1) at starting point of the every even cycle. The outputs are monitored by oscilloscope to verify the deterministic characteristic with normal CPU load (51% ~ 54 %).

Second, to test the priority and the interrupt with context switching, each task outputs logic one (1) during a task is running and logic zero (0) during a task finishes its load. This test is performed with CPU load 85~100% to give more severe environment to PLC.

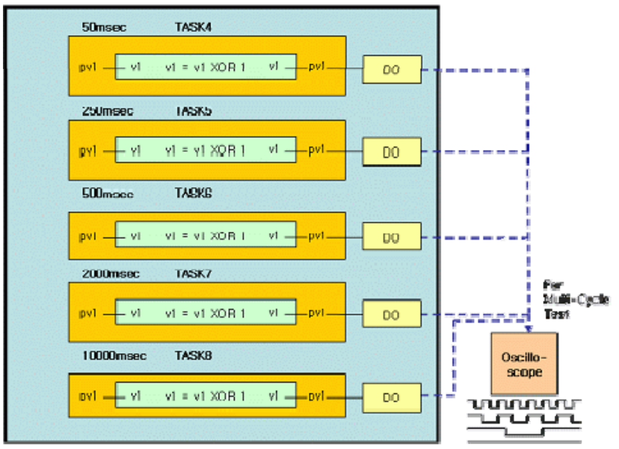

Figure 1. Multi-cycle Time Test Configuration

3.2 Testing Results

In the left part of the figure 2, all tasks are started and stopped at their cycle times exactly. In the right part of the figure 2, the task with higher priority (50 msec) can start within its time tick during lower priority task (250, 500 msec) is running.

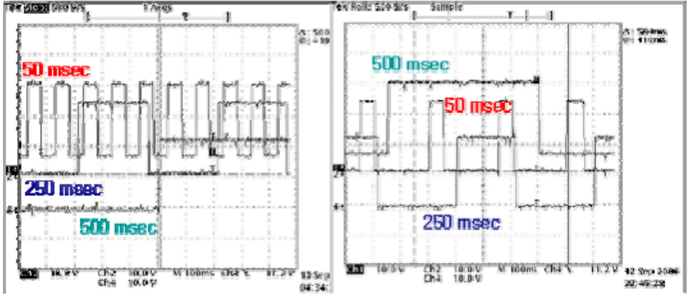

Figure 2. Testing Result for Real Time behaviour

As a result, it is verified that all five tasks are able to finish within predefined cycle times and meet the deterministic performance requirements. It is also verified that the maximum inputs/outputs required by CPCS are accommodated and the priority and the interrupt with context switching operate as expected.

4. Performance Testing for Safety Data Link

4.1 Testing Method

The platform uses the safety data link as the safety-critical data communication. This testing has two objectives as followings;

- To verify that data link is deterministic.
- To verify that data integrity, data rates and data precision are acceptable to requirements.

The test bed in the Figure 3 is prepared using PLC platform to test communication characteristic required by the safety system. In order to monitor the deterministic characteristic of the network, PLC sender continuously sends heartbeat, which is increasing at every cycle, to PLC receiver via ports 1 and 2. Each task 1 through 4 in PLC sender sends a block including the increasing heartbeats via port 1. The task 5 provides 8 blocks including the increasing heartbeats via port 2. PLC receiver receives the twelve blocks including heartbeats with attached CRCs from port 1 and 2. Whenever PLC receiver gets blocks, it is checked that all received values are the same and all the attached CRCs are identical. To give an interrupt to real time OS, the CPU load of task 3 is changed from 30% to 60%.

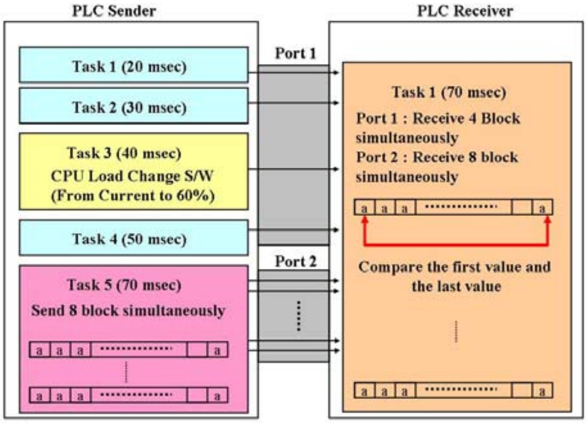

Figure 3. Safety Data Link Test under multi-tasking

4.2 Testing Results

When all 8 blocks arrive, all values and CRCs should be the same in PLC receiver. Using the test results, comments on safety data links are provided to PLC vendor.

5. Performance Testing for Safety-related Network

5.1 Testing Method

The PLC is equipped with the network to give the interface between processors and OM/MTP.

The network testing has two objectives as followings;

- To measure the actual response time of network.
- To verify the network data integrity.

The test bed in the Figure 4 is prepared using PLC platform to test network response time and network data integrity. The 30 units which are maximum size data required by CPCS are broadcasted at every 10 msec from the master via communication module to network. To emulate the actual CPCS, 2 dummy processors which exchange the 30 units per processor are configured. Because response time can be effected by the CPU load, CPU load of slave is changed from 20 to 60 %. As soon as the slave receives all 30 units, this sends 30 feedback indexes to master. When the master receives all feedback indexes from the slave, it investigates the data integrity and records the elapsed time from sending time to feedback time. The data integrity and maximum elapse time are continuously monitored.

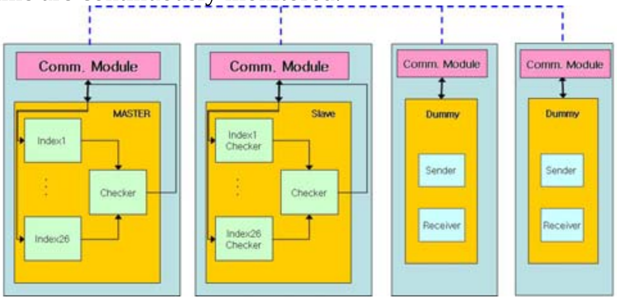

Figure 4. Network testing for integrity and response time

5.2 Testing Results

During testing, the average elapsed time from master-network-slave-network-master is measured. The maximum elapse time is also measured. Network data Integrity is monitored from current CPU load to 60%. Using the test results, comments on safety-related network are provided to PLC vendor.

6. Conclusion

The testing in this paper is performed by system designers and application software developers who are independent of developers. During testing, some valid comments on PLC performance are provided to vendor such as issues related to multi-tasking, safety data link, network, response time, and diagnostics. In addition to testing activities performed in platform development phase by vendor, the testing introduced by independent engineers in this paper is useful and effective to maintain the safety platform quality.

REFERENCES

[1] IEEE Std 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety systems of Nuclear Power Generating Stations”
[2] USNRC Reg. Guide 1.152, “Criteria for Programmable Digital Computers System Software in Safety Related Systems of Nuclear Power Plants”