Digital System Reliability Test for the Evaluation of Safety Critical Software of Digital Reactor Protection System

Hyun-Kook Shin, Sang-Ku Nam, Se-do Sohn , Hang-Bae Kim
I& C Dept., Korea Power Engineering Company, Inc.
150 Deogjin-Dong, Yuseong-Gu, Daejeon, KOREA 305-353

ABSTRACT

A new Digital Reactor Protection System (DRPS) based on VME bus Single Board Computer has been developed by KOPEC to prevent software Common Mode Failure(CMF) inside digital system. The new DRPS has been proved to be an effective digital safety system to prevent CMF by Defense-in-Depth and Diversity (DID&D) analysis. However, for practical use in Nuclear Power Plants, the performance test and the reliability test are essential for the digital system qualification. In this study, a single channel of DRPS prototype has been manufactured for the evaluation of DRPS capabilities. The integrated functional tests are performed and the system reliability is analyzed and tested. The results of reliability test show that the application software of DRPS has a very high reliability compared with the analog reactor protection systems.

Keywords: digital reactor protection system, common mode failure, design diversity, software reliability test, safety critical software.

1. INTRODUCTION

The digital I&C systems compared with the analog I&C systems provide many important technical benefits. They are basically drift-free. The system performance has been improved in terms of accuracy and computational capabilities. Since they have outstanding capabilities of data handling and storage, the plant operating conditions can be effectively measured and displayed when they are adopted in nuclear safety system.

However, the digital systems are vulnerable to Common Mode Failure (CMF) that may cause redundant safety systems to fail in their functions. The avoidance of CMF is of vital importance in the design and operation of digital safety system. In addition, the application of digital safety system to the Nuclear Power Plants (NPPs) needs to establish a very high level of reliability for safety [1].

Korea Power Engineering Company, Inc.(KOPEC) has developed a new Digital Reactor Protection System (DRPS) based on Versa Module Europe(VME) bus Single Board Computer (SBC) in order to prevent CMF inside the digital system. The diversity concept in both hardware and software has been applied to the new DRPS.

In the hardware design, two different types of CPUs are selected for bistable and coincidence logic processors. For software diversity, two types of Real Time Operating System (RTOS) are adopted. The application software uses C language which is highly stable when used for digital class 1E systems in NPPs [2].

In the development stage, new DRPS has been proved to be an effective digital safety system through software Failure Mode and Effect Analysis (FMEA), and Defense-in-Depth and Diversity (DID&D) analysis for CMF [3]. However, for practical use, the integrated system reliability test and functional test are necessary to show that the developed DRPS satisfies the design requirements and the system reliability including software is high enough for specific nuclear application. For this purpose, one channel prototype has been manufactured to evaluate the DRPS performance capability including software quality.

This paper describes the digital system reliability test and the functional test with DRPS prototype. The black-box test method was selected for the reliability test. The black-box test method is a kind of functional test which emphasizes the execution of the required functions and the examination of their input and the output data.

2. DESIGN FEATURES OF DRPS

The DRPS continuously monitors the selected plant safety parameters to assure that the plant safe status is constantly maintained. The DRPS automatically initiates reactor protective action whenever the monitored plant parameter reaches a pre-determined set point level. The reactor trip is provided through an interface with the Reactor Trip Switchgear System (RTSS). The actuation of engineered safety features is achieved through the Digital Engineered Safety Feature Actuation System – Auxiliary Cabinet (DESFAS-AC).

The DRPS consists of four redundant channels (A, B, C and D) as depicted in Figure 1 to satisfy single failure criteria and to improve plant availability. Each channel comprises two Bistable Processors (BPs), two Local Coincidence Logic (LCL) Processors, a System Interface Processor (SIP), initiation logics and a Maintenance/Test Panel (MTP). The system includes four redundant Operator Modules (OM) located on the main control board.

Each BP in the channel receives analog inputs from separate sensors in each channel, and discrete signals from the Core Protection Calculator System (CPCS) for the OPR1000 which stands for Optimized Power Reactor 1000MWe, Korean Standard Nuclear Power Plant. The bistable function determines the trip state by comparing the measured process variable with the predetermined set point value.

Each BP module sends its trip status to the redundant channel LCL processor modules via Serial Data Links (SDL). Each SDL utilizes fiber optic modems and fiber optic cables to provide electrical isolation between the redundant channels.

The LCL processor includes two diversified processor modules and each of them performs two-out-of-four coincidence trip logic for Reactor Trip (RT) and initiation of Engineered Safety Feature Actuation System (ESFAS). The LCL processor produces a trip signal when two or more of four inputs indicate a trip state. If a trip bypass is present, the LCL logic is converted to two-out-of-three coincidence from the two-out-of-four coincidence. The trip channel bypasses are manually initiated in each channel from the MTP.

The initiation signals from two LCLs are provided to the channel's dedicated initiation relays through a hardwired "OR" logic.

The main function of the MTP is to provide a test capability on the DRPS via the human-machine interface. The MTP is also used to monitor DRPS status and to perform DRPS control functions such as the insertion of bistable trip channel bypasses and operating bypasses.

The SIP monitors DRPS channel status and initiates manual and/or automatic surveillance test(s) based on user input via the MTP. The SIP also provides the interfaces to external systems for status indication and surveillance testing.

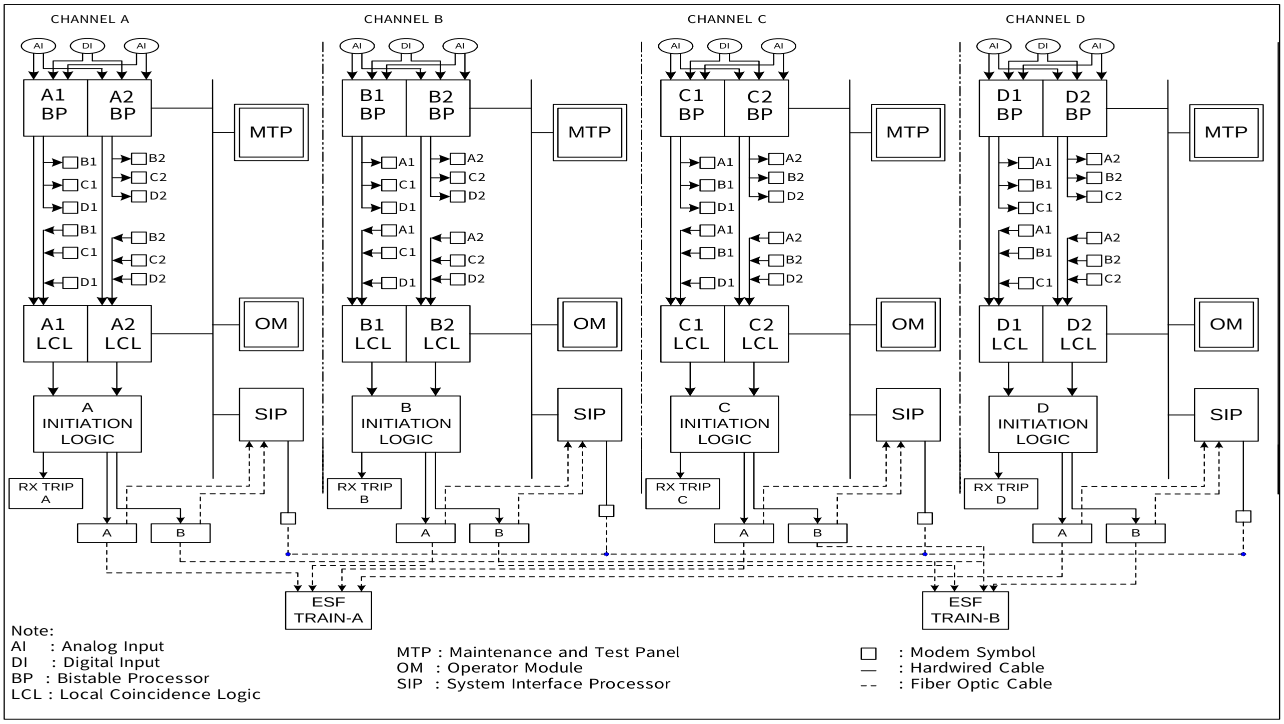


Figure 1. DRPS Block Diagram

3. SYSTEM RELIABILITY ANALYSIS

To evaluate the system reliability of DRPS, a model based evaluation technique is used. A model based evaluation is a cost-effective solution as it allows system evaluation without having to build a system during the conceptual design stage [4].

The Reliability Block Diagram (RBD) method is applied to the system configuration shown in Figure 1. The blocks of the RBD are then connected in series and/or parallel based on the operational dependency between the components as shown in Figure 2. The RBD for the DRPS is further simplified and shown in Figure 3.

In the DRPS reliability evaluation, we assume that the repair time is 2 hours, because spare components have already been prepared in the maintenance shop according to the module-based exchange maintenance method. And system life time is assumed 40 years (350,400 hours). The unavailability of DRPS is calculated using simplified reliability block diagram shown in Figure 3 by Isograph Reliability Software Tool with component failure rates [5, 6]. The pressurizer pressure trip parameter was selected for the evaluation.

The evaluation result shows that the total unavailability of DRPS is approximately 3.6 $\times 10^{-7}$ F/D (Failure/Demand). This reliability is higher than that of the conventional analog reactor protection system. The unavailability of the analog system is known to be ranging from 7.8 $\times 10^{-5}$ to 5.7$\times 10^{-6}$ F/D.

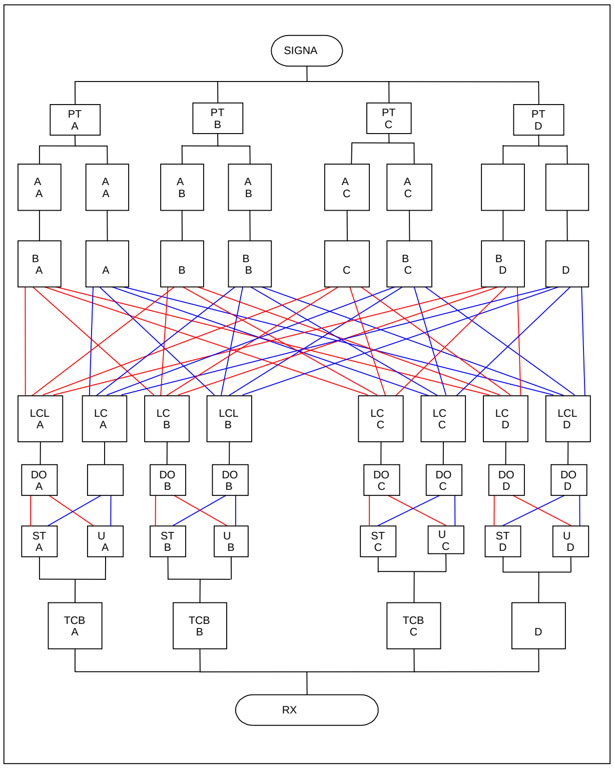


Figure 2. DRPS Reliability Block Diagram

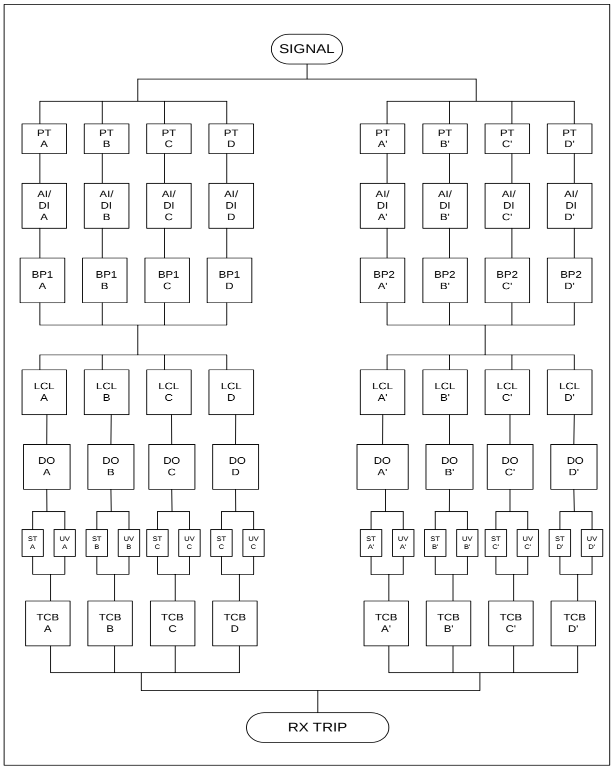


Figure 3. Simplified RBD for DRPS

4. REQUIREMENTS ANALYSIS AND FUNCTIONAL TESTS

4. A. System Requirements Analysis

The detailed functional analysis in the initial stage of software development process is very important to ensure that the software is highly reliable. The scope of DRPS modeling includes process input to Bistable Processor, cross channel communication between the redundant channels, LCL logic and the initiation logic.

Five trip parameters and trip logics with set points are selected for software development of DRPS prototype as shown in Table 1. Modeling the trip algorithms for each trip parameter with various characteristics depends on input signal (analog or digital input), set point method (fixed or variable), bistable logic (falling or rising) and operating bypass function. The above five sample trip parameters cover all types of bistable logic for total seventeen DRPS trip parameters for the OPR1000.

For this functional analysis, the variable overpower trip function is selected. This trip algorithm actuates the reactor trip when the measured neutron flux power increases at a faster rate than preset value or reaches a high preset value as shown in Figure 4. The variable over power trip set point follows process input value with maximum increase rate of 11% power/minute and constant band of 15% power.

Table 1. The Type of Bistable Logic for the Selected Trip Parameters

Trip parameter	Type of set point	Bistable logic	Operating bypass	Trip set point
Low Pressurizer Pressure	Variable set point with manual reset	Falling trip	Yes	1,700 psia 400 psia decrease/reset
Variable over-power trip	Variable set point with automatic rate limit	Rising trip	No	Ceiling : 110 % Band : 15 % Rate : 11%/min
Low S/G Level	Fixed set point	Falling trip	No	45 %
High Containment Pressure	Fixed set point	Rising trip	No	1.9 psig
High Local Power Density	Digital	Discrete	No	Trip = 1

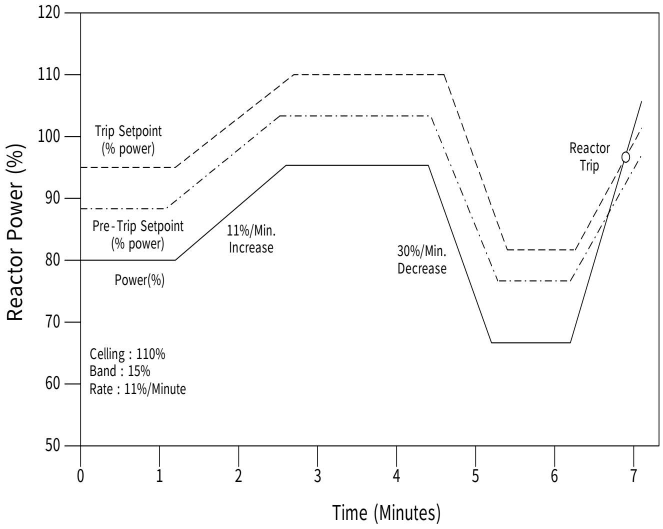


Figure 4. Variable Overpower Trip Function

4. B. DRPS Prototype Configuration

One channel DRPS prototype has been constructed to demonstrate its performance capability as shown in Figure 5. The actual prototype consists of BP rack, LCL processor rack and Maintenance & Test Panel as shown in Figure 6. As described in Section 2, two types of processors are installed in each rack. The Rack 1 uses Motorola CPU for BP and LCL processors, and the other rack (Rack 2) uses Intel CPU for redundant BP and LCL processors. The DRPS adopts two real-time operating systems, i.e., VxWorks for Rack 1 and QNX for Rack 2. The main hardware of two racks is a VME bus based on SBC which is manufactured by the DY4 Systems Inc. in Canada.

4. C. Functional Test

The variable over power trip parameter has variable set point with automatic rate limit and rising trip. In normal operating condition with slow power increase, trip and pre-trip set points track input process value with constant band (15 % power and 9% power, respectively). If increase rate is greater than the pre-determined value (11%/min), the difference between trip set point and process value goes to zero (0). Then bistable logic provides a trip signal to LCL logic. The reactor power will not exceed the ceiling of 110% to keep the reactor from becoming an over powered state.

The result of DRPS prototype functional test for the variable over power trip algorithm is displayed on the MTP as shown in Figure 7. The input signals to analog input module in each rack are generated by simulator. Figure 7 shows the set point and the trip condition during the power increase and decrease. It is shown that trip and pretrip actions are performed correctly as designed. The hysterisis settings also work correctly after trip and before resetting the set point.

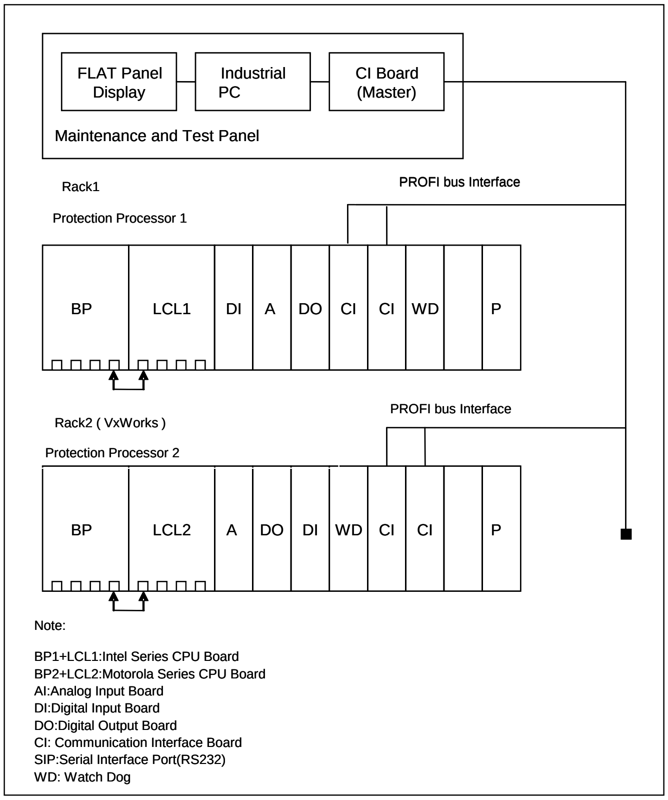


Figure 5. DRPS Prototype Configuration

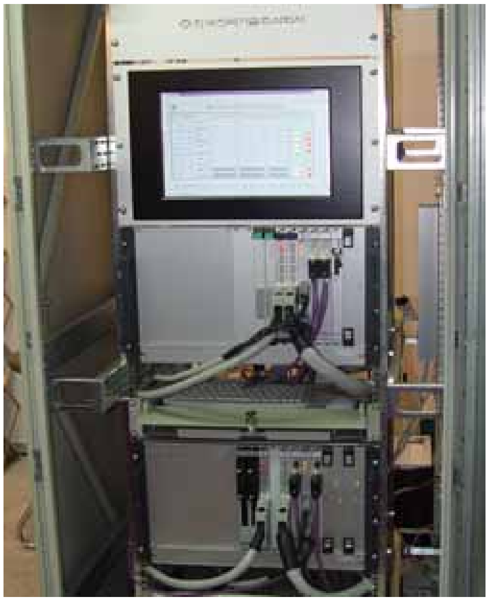


Figure 6. Front Panel of DRPS Prototype

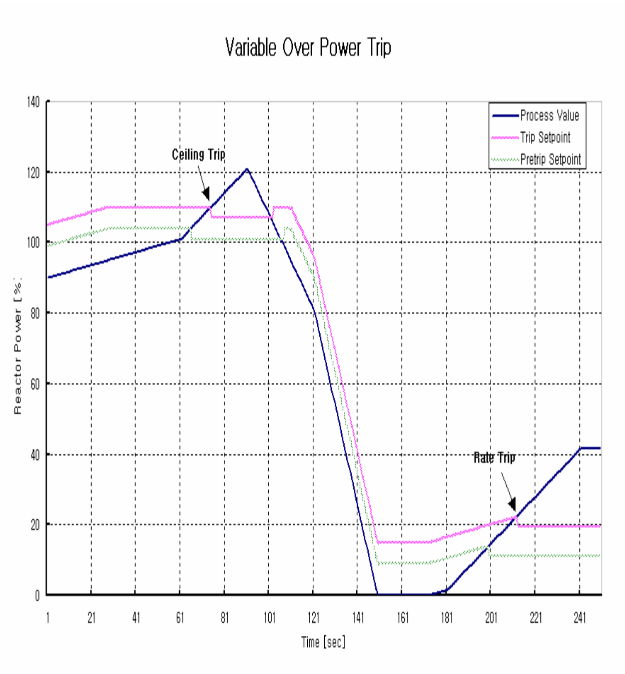


Figure 7. The Functional Test of Variable Over Power Trip

5. DRPS RELIABILITY TEST

The reliability of analog system is simply calculated based on failure rate data of hardware component. In digital system, both hardware and software components should be considered in the reliability calculation. However, the software reliability calculation method is not well established for practical application up to now.

To solve this problem, the error minimized software development process and upgraded Verification and Validation (V&V) method has been established for high quality of DRPS software [7]. The correctness of the functions for DRPS is also checked through the integrated functional tests after software development. Therefore, it is expected that the DRPS software has very high quality based on the CMF preventive system configuration and well organized software production and upgraded V&V method.

However, for practical use in NPPs, it is necessary to prove that DRPS application software has very high reliability. For that purpose, the black-box test method is selected for the reliability test. The black-box test is a kind of functional test method which emphasizes the execution of the functions and the examination of their input and output data.

In the test, a large number of inputs are simulated and the outputs are compared against the specification to validate correctness.

To setup the test, the target number of tests should be determined before test. The system unavailability of 4 channel DRPS is calculated as 3.6×10^{-7} F/D as shown in Section 3. The single channel DRPS unavailability is calculated as 4.5×10^{-4} F/D.

Considering uncertainty margin, the target number is suggested as 10,000 tests. However, it is still large number because one test set consists of 10 variable inputs as shown in Figure 8. Thus individual test input number is one hundred thousand (100,000) tests. To reduce the number of tests, Bernoulli trial equation is used [8]. The number of successes ‘N’ out of n Bernoulli trials is written as follows :

$$N = q \times n \text{ -- } (1)$$

where ‘q’ is the probability of success in a single trial.

The number of tests required to attain a desired confidence level ‘CL’ is obtained from Equation (1) as follows:

$$N = \log (1- CL)/ \log (q) \text{ ------------------------ } (2)$$

According to Equation (2), 6932 tests are required to demonstrate the software reliability (q) of 0.9999 for one channel DRPS with a confidence level of 50%. Therefore, the target number is determined as 7,000 simulation input set for the DRPS reliability test.

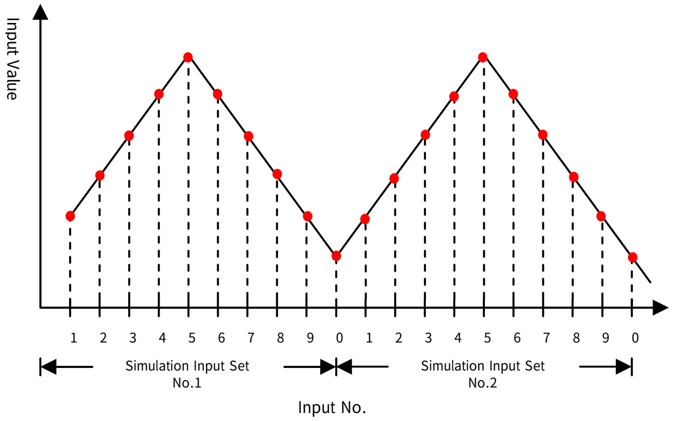


Figure 8. Structure of Test Input Data Set

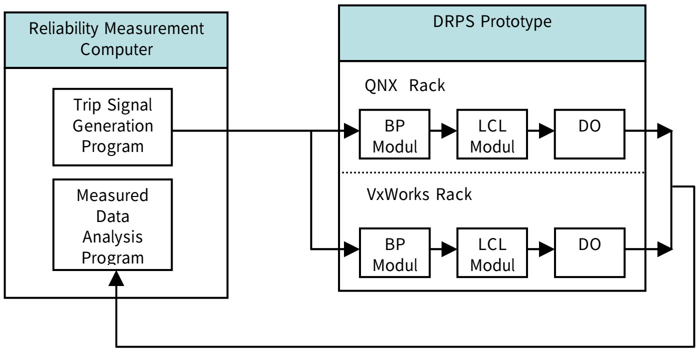


Figure 9. Reliability Test Arrangement with DRPS Prototype and Test Measurement Computer

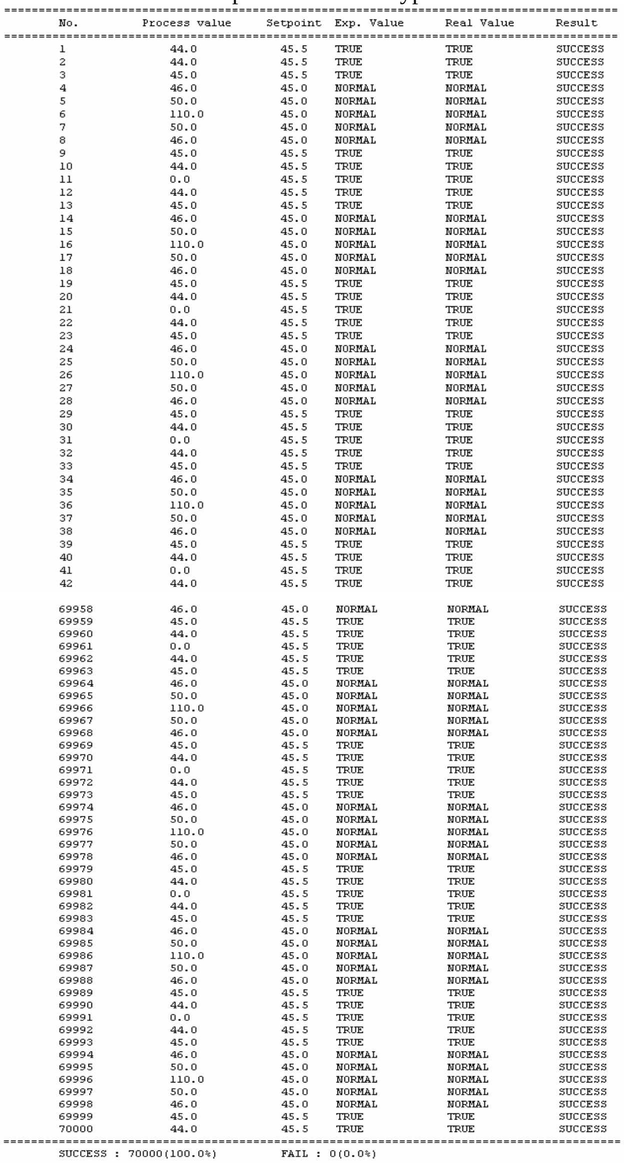
The test method for DRPS software reliability is presented in Figure 9. The simulation input signal is supplied to DRPS prototype from trip generation module in Reliability Measurement Computer (RMC).

In this work, Steam Generator Low Level Trip is selected for sample test. The characteristic of this trip is falling trip. One set of simulation input consists of 10 values around the set point as shown in Figure 8. These input sets are supplied to the input modules of QNX and VxWorks racks in DRPS prototype as shown in Figure 9. The output signal of the DO module in each DRPS sub-rack is sent to data analysis module in RMC for reliability analysis.

The result of reliability test shows that all the measured outputs are consistent with the expected values, as shown in Table 2.

From this test, it is recognized that the system reliability of DRPS is not degraded by the influence of software reliability. Therefore, the reliability of DRPS software is proven for practical use in NPPs.

Table 2.The Result of Reliability Test with Steam Generator Low Level Trip in DRPS Prototype



```
=====================================================================================
       No.         Process value     Setpoint  Exp. Value       Real Value       Result
=====================================================================================
       1               44.0            45.5    TRUE             TRUE             SUCCESS
       2               44.0            45.5    TRUE             TRUE             SUCCESS
       3               45.0            45.5    TRUE             TRUE             SUCCESS
       4               46.0            45.0    NORMAL           NORMAL           SUCCESS
       5               50.0            45.0    NORMAL           NORMAL           SUCCESS
       6               110.0           45.0    NORMAL           NORMAL           SUCCESS
       7               50.0            45.0    NORMAL           NORMAL           SUCCESS
       8               46.0            45.0    NORMAL           NORMAL           SUCCESS
       9               45.0            45.5    TRUE             TRUE             SUCCESS
       10              44.0            45.5    TRUE             TRUE             SUCCESS
       11              0.0             45.5    TRUE             TRUE             SUCCESS
       12              44.0            45.5    TRUE             TRUE             SUCCESS
       13              45.0            45.5    TRUE             TRUE             SUCCESS
       14              46.0            45.0    NORMAL           NORMAL           SUCCESS
       15              50.0            45.0    NORMAL           NORMAL           SUCCESS
       16              110.0           45.0    NORMAL           NORMAL           SUCCESS
       17              50.0            45.0    NORMAL           NORMAL           SUCCESS
       18              46.0            45.0    NORMAL           NORMAL           SUCCESS
       19              45.0            45.5    TRUE             TRUE             SUCCESS
       20              44.0            45.5    TRUE             TRUE             SUCCESS
       21              0.0             45.5    TRUE             TRUE             SUCCESS
       22              44.0            45.5    TRUE             TRUE             SUCCESS
       23              45.0            45.5    TRUE             TRUE             SUCCESS
       24              46.0            45.0    NORMAL           NORMAL           SUCCESS
       25              50.0            45.0    NORMAL           NORMAL           SUCCESS
       26              110.0           45.0    NORMAL           NORMAL           SUCCESS
       27              50.0            45.0    NORMAL           NORMAL           SUCCESS
       28              46.0            45.0    NORMAL           NORMAL           SUCCESS
       29              45.0            45.5    TRUE             TRUE             SUCCESS
       30              44.0            45.5    TRUE             TRUE             SUCCESS
       31              0.0             45.5    TRUE             TRUE             SUCCESS
       32              44.0            45.5    TRUE             TRUE             SUCCESS
       33              45.0            45.5    TRUE             TRUE             SUCCESS
       34              46.0            45.0    NORMAL           NORMAL           SUCCESS
       35              50.0            45.0    NORMAL           NORMAL           SUCCESS
       36              110.0           45.0    NORMAL           NORMAL           SUCCESS
       37              50.0            45.0    NORMAL           NORMAL           SUCCESS
       38              46.0            45.0    NORMAL           NORMAL           SUCCESS
       39              45.0            45.5    TRUE             TRUE             SUCCESS
       40              44.0            45.5    TRUE             TRUE             SUCCESS
       41              0.0             45.5    TRUE             TRUE             SUCCESS
       42              44.0            45.5    TRUE             TRUE             SUCCESS

       69958           46.0            45.0    NORMAL           NORMAL           SUCCESS
       69959           45.0            45.5    TRUE             TRUE             SUCCESS
       69960           44.0            45.5    TRUE             TRUE             SUCCESS
       69961           0.0             45.5    TRUE             TRUE             SUCCESS
       69962           44.0            45.5    TRUE             TRUE             SUCCESS
       69963           45.0            45.5    TRUE             TRUE             SUCCESS
       69964           46.0            45.0    NORMAL           NORMAL           SUCCESS
       69965           50.0            45.0    NORMAL           NORMAL           SUCCESS
       69966           110.0           45.0    NORMAL           NORMAL           SUCCESS
       69967           50.0            45.0    NORMAL           NORMAL           SUCCESS
       69968           46.0            45.0    NORMAL           NORMAL           SUCCESS
       69969           45.0            45.5    TRUE             TRUE             SUCCESS
       69970           44.0            45.5    TRUE             TRUE             SUCCESS
       69971           0.0             45.5    TRUE             TRUE             SUCCESS
       69972           44.0            45.5    TRUE             TRUE             SUCCESS
       69973           45.0            45.5    TRUE             TRUE             SUCCESS
       69974           46.0            45.0    NORMAL           NORMAL           SUCCESS
       69975           50.0            45.0    NORMAL           NORMAL           SUCCESS
       69976           110.0           45.0    NORMAL           NORMAL           SUCCESS
       69977           50.0            45.0    NORMAL           NORMAL           SUCCESS
       69978           46.0            45.0    NORMAL           NORMAL           SUCCESS
       69979           45.0            45.5    TRUE             TRUE             SUCCESS
       69980           44.0            45.5    TRUE             TRUE             SUCCESS
       69981           0.0             45.5    TRUE             TRUE             SUCCESS
       69982           44.0            45.5    TRUE             TRUE             SUCCESS
       69983           45.0            45.5    TRUE             TRUE             SUCCESS
       69984           46.0            45.0    NORMAL           NORMAL           SUCCESS
       69985           50.0            45.0    NORMAL           NORMAL           SUCCESS
       69986           110.0           45.0    NORMAL           NORMAL           SUCCESS
       69987           50.0            45.0    NORMAL           NORMAL           SUCCESS
       69988           46.0            45.0    NORMAL           NORMAL           SUCCESS
       69989           45.0            45.5    TRUE             TRUE             SUCCESS
       69990           44.0            45.5    TRUE             TRUE             SUCCESS
       69991           0.0             45.5    TRUE             TRUE             SUCCESS
       69992           44.0            45.5    TRUE             TRUE             SUCCESS
       69993           45.0            45.5    TRUE             TRUE             SUCCESS
       69994           46.0            45.0    NORMAL           NORMAL           SUCCESS
       69995           50.0            45.0    NORMAL           NORMAL           SUCCESS
       69996           110.0           45.0    NORMAL           NORMAL           SUCCESS
       69997           50.0            45.0    NORMAL           NORMAL           SUCCESS
       69998           46.0            45.0    NORMAL           NORMAL           SUCCESS
       69999           45.0            45.5    TRUE             TRUE             SUCCESS
       70000           44.0            45.5    TRUE             TRUE             SUCCESS
=====================================================================================
       SUCCESS : 70000(100.0%)         FAIL : 0(0.0%)
```

6. CONCLUSIONS

The advanced DRPS has been developed with diverse dual processors. The primary goal of the work is to prevent CMF inside the DRPS. For this purpose, two different types of CPUs, i.e., Motorola and Intel are used. Operating software diversity is achieved by using QNX and VxWorks.

From the qualitative analysis of defense-in-depth and diversity, the design concept of diverse dual processors showed excellent capability in preventing CMF inside the DRPS.

In order to be used in nuclear power plants, the developed digital system is required to prove that it has a high reliability for safety application.

In this work, the reliability and functional test are performed. The functional test of variable over power trip shows good consistency with design functional requirements.

For the reliability test, the black-box test method is used. The result of DRPS reliability test shows that all of the outputs by 70,000 simulated inputs are correct as expected trip states. It strongly indicates that the software of DRPS has no errors.

Therefore, the system unavailability of 3.6×10^{-7} F/D can be satisfied. This reliability is higher than not only the reliability of the analog protection system but also that of currently operating digital protection system in NPPs.

7. ACKNOWLEDGEMENT

The authors would like to express their gratitude to KISTEP (Korea Institute of Science & Technology Evaluation and Planning) and MOST (Ministry of Science and Technology) in Korea for the financial support to this research performed under the National Lab. Project.

8. REFERENCES

[1] DOUGLAS M. CHAPIN et al., Digital Instrumentation and Control Systems in Nuclear Power Plant, Committee on Application of Digital Instrumentation and Control System to Nuclear Power Plant Operations and Safety, National Academy Press, Washington, D.C, pp. 43 ~ 51, 1997.

[2] HYUN KOOK SHIN, SANG KU NAM, et al., Development of an Advanced Digital Reactor Protection System using Diverse Dual processors to prevent Common Mode Failure, pp. 33 ~ 44 of Nuclear Technology, Vol. 141, January 2003.

[3] HYUN KOOK SHIN et al., Digital Reactor Protection System to prevent Software Common Mode Failure, ICAPP’03, Cordoba, Spain, May 4-7, 2003.

[4] R.BILLINGTON et al., Reliability Evaluation of Engineering Systems: Concepts and Techniques, Pitman Advanced Publishing Program, Boston, London, Melbourne, 1983.

[5] ISOGRAPH Limited, Reliability Workbench for Windows version 9.0, Reference Manual, USA, 2001.

[6] DY4 Systems Inc, Harsh Environments COTS Technical Manual, Ottawa, Canada, 2000.

[7] SANG KU NAM, HYUN KOOK SHIN et al., The Software Development Process to Produce Highly Reliable Safety Software for Digital Reactor Protection system, ANS 2004 Embedded Topical Meeting on Operating Nuclear Facility Safety (ONFS), Washington D.C., Nov. 14-18, 2004.

[8] A.PAPOULIS, Probability, Random Variables, and Stochastic Processes, McGraw-Hill, Inc., 1965.