Transactions of the Korean Nuclear Society Spring Meeting
Chuncheon, Korea, May 25-26 2006

Reliability Analysis of Safety Grade PLC(POSAFE-Q) for Nuclear Power Plants

J. Y. Kim,a J. Lyou,a D. Y. Lee,b J. G. Choi,b W. M. Park,b
a Dept. of Electrical and Computer Engineering, Chungnam National University, electron@cnu.ac.kr
b Instrumentation & Control - Human Factors Div., Korea Atomic Energy Research Institute

1. Introduction

The Part Count Method of the military standard MIL-HDK-217F has been used for the reliability prediction of the nuclear field. This handbook determines the Programmable Logic Controller (PLC) failure rate by summing the failure rates of the individual component included in the PLC. Normally it is easily predictable that the components added for the fault detection improve the reliability of the PLC. But the application of this handbook is estimated with poor reliability because of the increased component number for the fault detection. To compensate this discrepancy, the quantitative reliability analysis method is suggested using the functional separation model in this paper. And it is applied to the Reactor Protection System (RPS) being developed in Korea to identify any design weak points from a safety point of view.

2. Hardware reliability analysis modeling

The conventional failure rate prediction model, such as the military handbook MIL-HDBK-217F, is a very conservative method because some failures happened in the PLC modules may not affect the RPS safety if the diagnostic function operates correctly. To consider the effect of the diagnostic function implemented in the PLC, a new failure rate prediction model is proposed. Figure 1 shows the functional block diagram of a typical digital hardware module [1]. The components of the hardware module can be categorized into 4 sub-function groups according to their functions. [2]

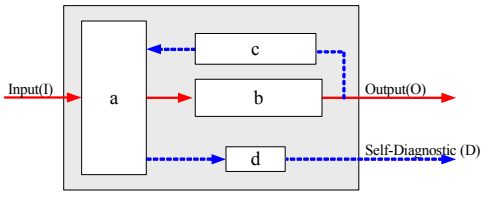

Figure 1. Functional block diagram of a typical digital.

If there is no failure in the module, all the sub-function groups perform their allotted functions correctly, and the PLC module is in the *success state*. If the *b* sub-function group is failed and the other sub-function groups operate properly, the module doesn't make the final output to the external module and the module becomes a *failure state*. But the module immediately generates the error signal to the external module because the self-diagnostic function operates correctly by a loop-back test in the *a* sub-function group. After an error alarm signal, the operator changes the RPS operation mode from the *2*-out-of-*4* to the *2*-out-of-*3*, and starts the maintenance activities immediately. Therefore, the failure case of only the *b* sub-function group is in a so-called *safe failure state*. If the *a* sub-function group is failed, the module doesn't make the transformed signal for the *b* sub-function group. Also the module doesn't conduct the loop-back test. As a result, the module comes to a *failure status*. If all the groups are failed, the module is in a *dangerous failure state*. Therefore the failure case of the *a* sub-function group is in a so-called *dangerous failure state*. The dangerous failure probability of the module can be written as [2,3]:

$$P\{\text{DF of the module}\} = P\left\{\bar{a} + a\bar{b}(\bar{c} + \bar{d})\right\} \approx P(\bar{a}) \quad (1)$$

Therefore, the dangerous failure rate of the module can be approximated by the failure rate of the *a* sub-function group such as follows:

$$\lambda_m \approx \lambda_a \quad (2)$$

3. Failure rate prediction for Safety Grade PLC

The proposed failure model is applied to the PLC modules being developed in Korea. Table 1 shows the failure rates of the digital output (DO) PLC module. From Fig. 1, the functions of the DO module are divided into *a, b, c, and d* sub-function group. The Failure Mode and Effect Analysis (FMEA) method [4] is used to categorize the components in the PLC into the sub-function group according to their functions. The failure rates of the sub-function group in Table 1 are determined by the sum of the individual component failure rates included in the each sub-function group. The failure rates of individual component are determined from MIL-HDBK-217F.

Table 1. Failure rates of the DO PLC module

Sub-function Group	Failure rates ($\times 10^{-6}$ /hr)
a	1.39
b	1.93
c	2.26
d	0.77
Dangerous Failure Rate	1.39
Conventional Failure Rate	6.35

In Table 1, the dangerous failure rate of the DO module can be approximated by the failure rate of the *a* sub-function group from the Eq. 2, and is *1.39E-06*. The conventional failure rate is determined by the sum of the failure rate of all sub-function group, and is *6.35E-06*.

Dangerous failure rate considers the effect of the diagnosis function included in the PLC. The dangerous failure rate of the PLC module can be approximated only by the failure rate of the *a* sub-function group, and is improved than the conventional failure rate. The result of the safety assessment is used as a measure to determine whether the new developed PLC or RPS is applied to the nuclear power plant. If this proposed failure rate model is adopted as a failure rate prediction method by nuclear regulatory body, it can improve the evaluation result for safety assessment without any hazard to the nuclear power plant.

4. Sensitivity analysis

This section describes the result of sensitivity analysis of PLC module which has high failure rate. The object of sensitivity analysis is to determine the weak components in each module from the safety point of view. The results of the sensitivity analysis are used for redesigning the modules such as changing the components, changing the electrical stress, and redesigning the circuits.

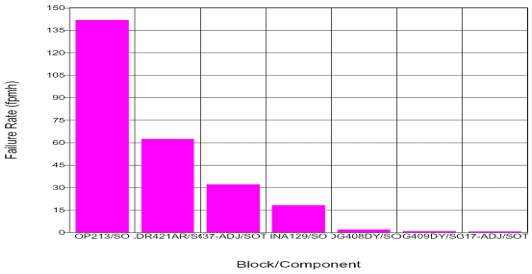

Figure 2. Sensitivity Analysis of analog output module.

Figure 2 shows the results of sensitivity analysis of analog output module. The four components which have high failure rate are DC-DC Converter, OP AMP, Analog Amplifier, and Voltage Regulator. Therefore, if these four components are redesigned or replaced by more high reliable components, the failure rate of the analog output module can be reduced.

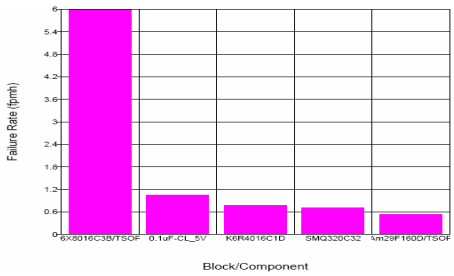

Figure 3. Sensitivity Analysis of CPU

Figure 3 shows the five components which have the high failure rate in CPU module. The five components are Regulator, Microprocessor, Capacitor, and Memory. Therefore, if these five components are replaced by more high reliable components, the failure rate of CPU module can be reduced.

5. Conclusion

The safety grade PLC for the reactor protection system is under development. The PLC has so many kinds of diagnosis functions to detect a fault occurrence in the PLC immediately. The detected failures of the components do not affect the RPS safety directly because the detected failure of the components can be recovered or classified as a *safe failure*. So it is possible to ignore the effects of the detected component failures for the RPS safety assessment. In this paper, a prediction method for the PLC failure rate is suggested to apply it to the nuclear RPS safety assessment. The dangerous failure rate which considers the effect of the diagnosis function included in the PLC is improved than the conventional failure rate. So, if this proposed failure rate model is adopted as a new failure rate prediction method by nuclear regulation body, it will improve the evaluation result for safety assessment without any hazard to the nuclear power plant.

Through the sensitivity analysis of the PLC modules, we identified the components in PLC modules which have high failure rates. We also proposed the redesign of the circuits of PLC modules or replacement of components which have high failure rates.

REFERENCES

[1] KNICS-SED-AR103, Reliability Analysis of PLC Hardware for Safety Systems Application, Korea Atomic Energy Research Institute, 2004.

[2] DY Lee et.al., Safety Assessment Methodology for a Digital Reactor Protection System, IJCAS, Vol. 4, No. 1, pp105-112, 2006.

[3] JY Kim et.al., A Failure Rate Prediction Method for the Probabilistic Safety Assessment, DSN-2005, Supplemental Volume, IEEE Computer Society, 2005.

[4] ANSI/IEEE Std. 352, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems, 1987.