# Failure Models of Software Based I/O Modules

Jong Gyun Choi,[a] Dong Young Lee,[a] Won Man Park,[a] Joon Lyou[b]
*a I&C, Human Factors Division, KAERI, ex-choijg@kaeri.re.kr*
*b Electrical & Computer Engineering Division, College of Engineering, Chungnam National University, jlyou@cnu.ac.kr*

## 1. Introduction

As a part of Korea Nuclear Instrument and Control System (KNICS) Project, we developed failure models and estimated unavailability of software based input and output modules designed for the safety PLC, POSAFE-Q, which is platform of KNICS plant protection system. For the estimation of failure rate of components in the module, the part stress method in MIL-HDBK-217F [1] is employed. The commercial tool, Reliability Workbench [2], provides effective environment for the theoretical failure rate assessment. The MIL-217 estimation routine in this software package is used for estimating the failure rate of hardware electronic components.

## 2. Failure Models

Figure 1 show the typical software based I/O module, the module consists of analog part and digital processing part. The analog input part receives the analog signal from the field, processes analog signal, and convert analog signal to digital signal for digital part. The analog part mainly consists of resistors, transistors, capacitors, diodes. The digital part processes digital signal and gives external module through the back plane bus of PLC. The digital part consists of microprocessor and memory.

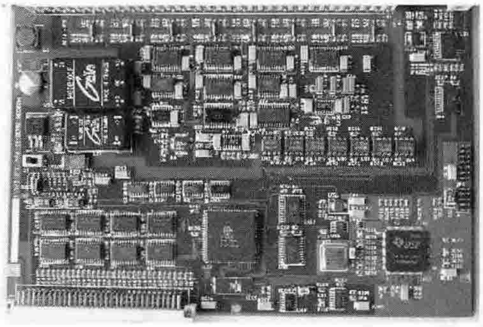

Figure 1. The typical software based I/O module

### 2.1. Functional Group

Figure 2 shows the functional block diagram of typical I/O module. The components of the module can be categorized into 4 sub-function group as follows:

i) The components in ***a*** group receive and transform the input signals. The transformed output signal is given to the ***b*** group. The components in this group also compare feedback signal with the transformed output signal. If the difference between these two signals occurs, error signal is given to interfaced module and user through ***d*** group.

ii) The components in ***b*** group receive and process the transformed signal from ***a*** group. The components in this group also give final output to interfaced module as well as ***c*** group.

iii) The components in ***c*** group transform final output. The transformed final output is given to ***a*** group for comparison.

iv) The components in ***d*** group transport error signal from ***a*** group to interfaced module or user for indicating that the module has failed.

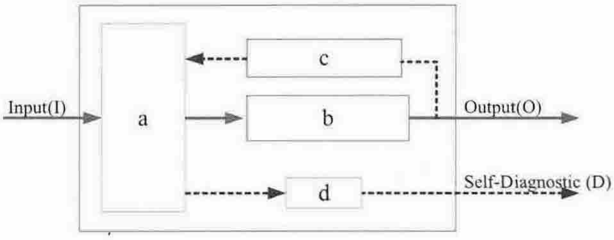

Figure 2. Functional Block Diagram of the I/O Module

### 2.2. Failure Modes

If all the components in a sub-function group have no failure, the sub-function group performs its allotted function correctly. If all sub-function groups in the module perform correctly their function, the function of module is performed successfully and the module is in ***success state***. If the ***b*** sub-function group has failed and the other sub-function groups operate properly, the module has the failed output but can inform the interfaced module or user of its failure because self-diagnostic function operates correctly. The module is in so-called ***safe failure*** state. If all the groups have failed, the module is in ***dangerous (unsafe) failure*** state.

### 2.3. Failure Model and Unavailability

The failure rate of each group is computed as the sum of the component failure rate for all components in the group as follows:

$$\lambda_{Group} = \sum_{i=1}^{n} \lambda_{i,Group} \qquad (1)$$

2.3.1. Conservative Model

The conservative failure rate of module is computed as the sum of the group failure rate in the module as follows:

$$\lambda_{Conservative} = \lambda_a + \lambda_b + \lambda_c + \lambda_d \qquad (2)$$

The unavailability of module is as follows:

$$Q_{Conservative} = \lambda_{Conservative} \cdot \frac{T}{2} \qquad (3)$$

where, T = the periodic test interval in hours

2.3.2. Main Function Model

The main function of the module is performed by the group ***a*** and ***b***. Therefore, the failure rate of module for the main function is computed as the sum of the failure rate of group ***a*** and ***b***.

$$\lambda_{Main} = \lambda_a + \lambda_b \qquad (4)$$

The unavailability of module is as follows:

$$Q_{Main} = \lambda_{Main} \cdot \frac{T}{2} \qquad (5)$$

2.3.3. Dangerous Failure Model

The dangerous failures of the module can be summed as follows:

$$\text{Dangerous Failure of the module} = \bar{a} + \overline{ab}(\bar{c} + \bar{d}) \qquad (6)$$

The dangerous failure probability of the module can be written as:

$$P\{\text{DF of the module}\} = P\{\bar{a} + a\bar{b}(\bar{c} + \bar{d})\} \approx P(\bar{a}) \qquad (2)$$

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

$$\lambda_{DF} \approx \lambda_a \qquad (3)$$

In addition, the unavailability due to dangerous failure of the module can be written as follows:

$$Q_{DF} = \lambda_{DF} \cdot \frac{T}{2} \qquad (4)$$

where, $Q_{DF}$ = the unavailability due to DF
$\lambda_{DF}$ = the failure rate per hour due to DF
T = the periodic test interval in hours

## 3. Conclusion

Through the KNICS project (2001.7.1-2008.6.30), we are developing a digital plant protection system and safety PLC (POSAFE-Q) for the safety critical I&C systems.

The purpose of this work was to develop the failure models for estimating the failure rate and unavailability of the software based I/O modules in the POSAFE-Q. The results of this work will provide fault tree model of digital plant protection system with occurrence probability of some basic events.

Three failure model and unavailability of the software based I/O module was modeled. It is very important to adapt proper failure model for correct estimation of the failure rate and unavailability of the software based I/O modules.

## Acknowledgement

This study has been carried out under the nuclear R&D research program sponsored by MOST

## REFERENCES

[1] MIL-HDBK-217F, "Reliability Prediction of Electric Equipment"

[2] Computer Program, Version 10.0 by ISOGRAPH, Reliability Workbench for Windows 95/98/NT/2000/Me, 2002