Development of Portable Monitoring System for I&C System

Kwang-Il Lee [a*], DongHwa Yoon [a]
[a]*SOOSAN ENS Co. Korea Techno Complex Building, Korea University, Anam-dong, Soungbuk-Gu, Seoul, 02841*
[*]*Corresponding author: lee83t@soosan.co.kr*

1. Introduction

Instrumentation and control system used in places where human access is difficult, such as nuclear power plants, is also difficult to access for maintenance. So basically, it has various self-diagnosis functions. However, due to the increasing threat of cyberattack targeting the industry in recent years, instrumentation and control system is not safe for cyberattack and the reliability of the self-diagnosis function is declining [1].

In this paper, we propose an external system with independent self-diagnosis function and monitoring functions in addition to the self-diagnosis function of Instrumentation and control system according to the cyber security requirement (RS-015) [2]. The main function of the monitoring system is to confirm that the self-diagnosis function of Instrumentation and control system is operating correctly and the other is to diagnose the state of Instrumentation and control system. The development and testing of the monitoring system were based on the POSAFE-Q, a domestic nuclear power Instrumentation and control system applied to Shin Hanul and Shin Kori.

2. Design Methods

In this section describes the development background of the monitoring system and explains the concept of the monitoring system and the structure of hardware and software.

2.1 Background

Unlike past analog systems, digital systems are vulnerable to cyberattack. Examples include Stuxnet and IronGate [3]. Therefore, a method is needed to diagnose even if integrity is violated due to cyberattack of digital Instrumentation and control system. As a solution, this paper proposes a monitoring system.

2.2 POSAFE-Q and Monitoring system

POSAFE-Q is the first nuclear instrumentation control system developed by Korean technology and consists of processor, communication, analog input / output, digital input / output, pulse module and etc. [4]. Also, it has various self-diagnostic functions to meet the requirements of nuclear power plants. The monitoring system proposed in this paper examines these self - diagnosis functions.

2.3 Hardware

The hardware of the monitoring system uses a tablet PC with Windows 10 or higher. The tablet PC communicates with the POSAFE-Q using the serial port(RS-232C) as shown in Fig. 1. It can also be run on PCs that have an environment similar to POSAFE-Q's engineering tool pSET-II.

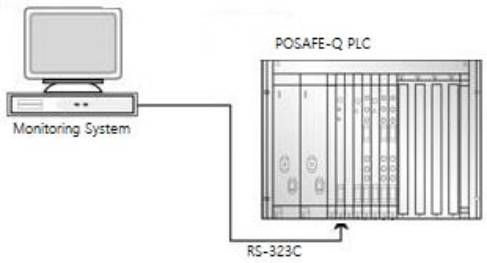

Fig. 1. Communication of monitoring system to processor module

2.4 Software

The functions to be implemented in the monitoring system include basic self-diagnosis function of POSAFE-Q, PLC status check, memory forgery of task and variable area, and modulation diagnosis. These functions are diagnosed by a separate algorithm using original data of POSAFE-Q.

The overall software system architecture is shown in Fig. 2. The back-end consists of a class that manipulate serial communication with the processor module and a class that stores data. The front-end has a visual class that displays the screen, a data control class that performs data operations and processing, and a user interface that handles tablet input.

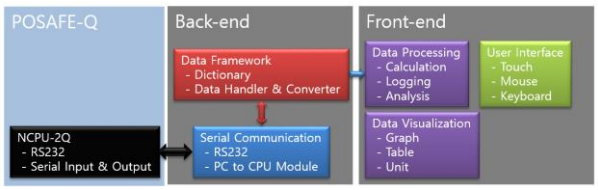

Fig. 2. Structure of monitoring system

Finally, for the security of the monitoring system itself, there are functions such as login, registered hardware management, usage history management, and options. And various information is encrypted and stored.

3. Implementation and Testing

In this section describes how to implement the functions of the monitoring system and shows the test results of those functions.

3.1 Implementation

The functions to be implemented are self-diagnostic functions guaranteed by POSAFE-Q, including CPU utilization, task errors, module status, bus errors, reference clock errors, and memory area errors. Functions other than memory diagnosis are calculated by bringing the items that affect the diagnosis result to the PC. The calculated values are compared with the results of the self-diagnosis function of the existing processor module.

The basic procedure of the memory diagnosis function is shown in Fig. 3. Generally, the memory area where the OS of Instrumentation and control system used in the nuclear power plant and also the task is stored are not easily changed. Based on this point, first, checksum of memory area of processor module which is normally operated is fetched to PC and stored. Next, the PC gets a portion of the memory area to be examined. Computes the checksum for the memory area read and then compares it to the stored checksum. Finally, the algorithm that reads, checks, and compares the next memory area is repeated until the entire memory area is over. When all memory areas are checked, the scan history is saved and the diagnosis is terminated.

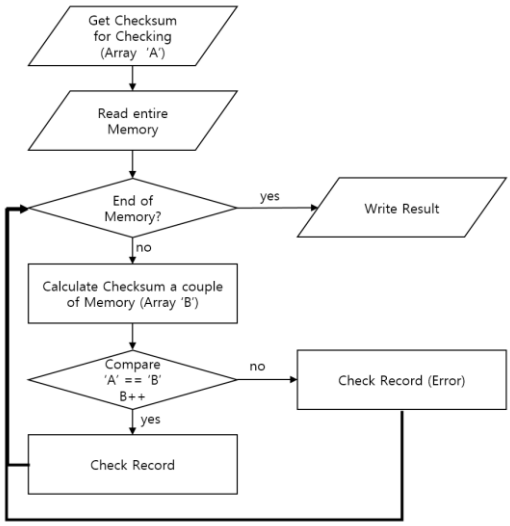

Fig. 3. Flow of memory diagnosis function

The data required for the monitoring system's own security is encrypted using the password-based key derivation function (PBKDF2) [5]. Items to be encrypted include login, hardware registration, checksum, and so on.

3.2 Testing

The hardware configuration consists of a power supply, a processor, and a digital output module. The software consists of one user task that performs simple counting. Test items were CPU utilization, task status diagnosis, bus status diagnosis, module status diagnosis and memory diagnosis function. Most of the functions were tested in the normal state, but the diagnosis of the module status was made by making an error in order to check the error detection function.

Table I: Test result of self-diagnostic functions

Item	POSAFE-Q	Monitoring System
Usage	11%	11%
Task	Normal	Normal
Bus	Normal	Normal
Module	Error (slot 2)	Error (slot 2)
Memory	none	none

As described in the previous section, unlike the basic diagnosis function of the monitoring system, the memory diagnosis function has different inspection methods. In the case of memory diagnosis, it is necessary to perform a long time test because the diagnosis must be performed without affecting the operation of the existing processor module. So, as shown in Fig. 4, the GUI is configured to check the progress. The gray bar at the top represents the total progress, and one green box represents the completion of some diagnostics in the memory area. Diagnostic results can also be found in Table 1, and if errors are found, the green box turns into a red box.

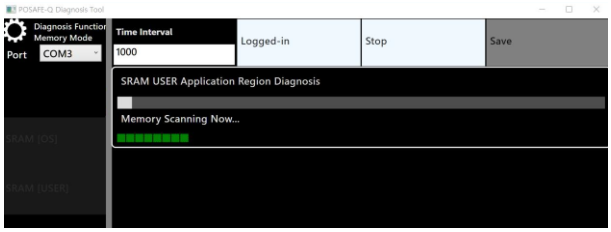

Fig. 4. Memory Diagnosis

4. Conclusions

As a result of testing the functions of the monitoring system, POSAFE-Q was able to perform the performance test of the self-diagnosis function. In addition, it was able to diagnose forged and modulated tasks by external attack. Such a monitoring system is expected to enhance the reliability of Instrumentation and control system exposed to the threat of various cyberattack. However, there is a possibility that the monitoring system will be attacked from the cyber security side. Although the monitoring system proposed in this paper has its own security by the login and device registration, it is vulnerable to external network connection or personal security because it is a general PC. This problem can be treated as a separate rule when

applied to the field, but it is necessary from the viewpoint of personal security to research and develop additional security functions.

ACKNOWLEDGMENT

This work was supported by the Korea Institute of Energy Technology Evaluation and Planning (KETEP) and the Ministry of Trade, Industry & Energy (MOTIE) of the Republic of Korea (No. 20161510101800).

REFERENCES

[1] Kim Tae Hee, Kim Si Won, Kim Hyun Doo and Shin Ik Hyun, 2017, "An Implementation of A Tamper-proof Embedded System with A Diagnostic Device," Proceedings of Symposium of the Korean Institute of communications and Information Sciences, , pp. 1168~1169.
[2] KINAC/RS-015, Cybersecurity Regulation Standard for Nuclear Facilities, Korea Institute of Nuclear Nonproliferation and Control, 2016.
[3] Kushner, David. "The Real Story of Stuxnet". ieee.org. IEEE Spectrum. Retrieved 25 March 2014.
[4] Lee, MyeongKyun, “Development and Application of POSAFE-Q PLC Platform”, 3rd International Conference on NPP Life Management (PLIM) for Long Term Operations (LTO), Salt Lake City, UT, USA, 2012.
[5] Burt Kaliski. "PKCS #5: Password-Based Cryptography Specification Version 2.0". tools.ietf.org. Retrieved 2015.