Asset Analysis Method for the Cyber Security of Man Machine Interface System

Sung Kon Kang, Hun Hee Kim, Yeong Cheol Shin*
Nuclear Engineering & Technology Institute (NETEC), Korea Hydro and Nuclear Power(KHNP)
P.O. Box Youseong-gu Daejeon, Republic of Korea(305-343)
**Corresponding author: sungkon@khnp.co.kr*

1. Introduction

As digital MMIS (Man Machine Interface System) is applied in Nuclear Power Plant (NPP), cyber security is becoming more and more important. Regulatory guide (KINS/GT-N27) requires that implementation plan for cyber security be prepared in NPP [1]. Regulatory guide recommends the following 4 processes: 1) an asset analysis of MMIS, 2) a vulnerability analysis of MMIS, 3) establishment of countermeasures, and 4) establishment of operational guideline for cyber security. Conventional method for the asset analysis is mainly performed with a table form for each asset. Conventional method requires a lot of efforts due to the duplication of information. This paper presents an asset analysis method using object oriented approach for the NPP.

2. Requirement of Asset Analysis

Korean regulatory body requires that an implementation plan and a design for cyber security be established for the operation license of the NPP which has a digital MMIS platform [1]. Also, 10CFR73.54 requires that critical systems, such as digital computers, communication systems, and network performing SSEP (Safety, Security and Emergency Preparedness) functions be protected from cyber attack [2]. Asset analysis is required to identify part of MMIS vulnerable to cyber attacks.

3. Asset Analysis using Object Oriented Method

3.1 Steps of Asset Analysis

In order to represent, using abstraction and inheritance relation, MMIS functions in terms of common technology components. The following steps, as shown in Fig 1, are followed:

- Decomposition of MMIS systems and functions into various levels of technology components
- Identification of common asset objects from the decomposed technology components
- Abstraction structuring using the concept of inheritance of common asset objects

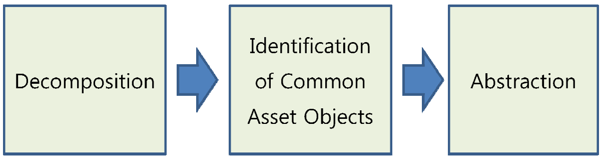

Fig.1. Steps of object oriented asset analysis

3.2 Decomposition and Identification of Common Asset Objects

MMIS includes plant control systems that are implemented based on DCS (Distributed Control System) platform, and plant protection system that is implemented based on PLC (Programmable Logic Controller) platform, turbine control system and other monitoring system. The decomposition is to produce a set of asset objects by identifying technology components used in digital control system such as DCS, network, OS (Operating System), middleware such as GUIMS (graphic user interface management system), hardware and applications.

Next step is to identify common asset objects from the decomposed components. Table 1 shows some of the common asset objects as an example.

Table 1 Common asset objects of DCS and PLC

Ob No	Common asset object	Specification
Ob1	Ovation EWS(Engineering Workstation System)	Dell Optiplex 745 Workstation
Ob2	Ovation OIS(Operator Interface System)	
Ob3	Ovation Server	Dell PowerEdge 840 Server
Ob4	Ovation Controller	Intel Pentium Processor POSIX Real Time Operating System
Ob5	Ovation Data Highway	Intelligent Ethernet Switch(Cisco3550), Ethernet Network Interface Card

3.3 Abstraction

The abstraction is to represent the structure of the asset objects using the relationship between common asset objects and system. Fig 2 shows an example of the abstraction of DCS based control systems. First level in the Fig 2 shows that all second level of the asset objects (EWS, OIS, Sever, and Controller) share the same Ovation data highway. The second level of the Fig 2 shows that Ovation DCS platform share the same asset objects (EWS, OIS, Server and Controller). The third level of the Fig 2 shows that P-CCS (Process-Component Control System), PCS (Power Control System), NPCS (Nuclear Steam Supply System Process Control System) are based on the same asset object (i.e. DCS platform). In case of DPS, only Ovation controller is used to implement.

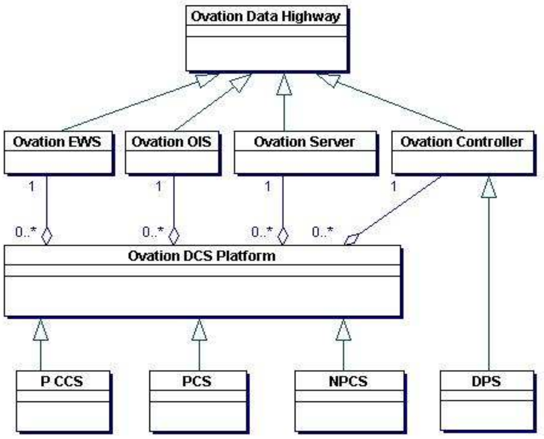

Fig.2. Abstraction of analyzed assets based on the inheritance relationship among DCS components

Systems such as PPS (Plant Protection System), ESF-CCS (Engineered Safety Featured – Component Control System), CPCS (Core Protection Calculator System) are based on the Common-Q PLC platform.

3.5 Expected Benefits

The application of object oriented method to asset analysis for MMIS of NPP is expected to bring the following benefits:

- Asset analysis report shows the relationship between common technology components and plant functions. Hence, it is easy to identify the impact of technology components to the plant functions in the cyber security analysis.
- Information on common components is described in one location in asset analysis. Therefore, it is not necessary to ensure consistencies among duplicated information and it is easy to maintain the asset analysis report when there are changes in MMIS during plant operation.
- Analysis efforts could be saved as compared with the conventional method. In case of DCS based control systems, overall analysis efforts are required in the platform (70%) and system function analysis (30%) considering the structure of system. Using object oriented approach, it is possible to analyze platform only once. Also, additional efforts of 10 % could be considered. Therefore, the analysis efforts could be saved roughly up to 40%.

4. Conclusions

We have applied the object oriented method for the MMIS asset analysis of the nuclear power plant. Based on the experience of the application of the object oriented method to DCS, we found that the analysis efforts could be saved roughly up to 40%. This method has the advantage not only in the reduction of efforts but also in the enhanced traceability of analysis data. We expect that the object oriented method for MMIS asset analysis will be applied to the operating NPPs and the new NPPs.

REFERENCES

[1] “Regulatory Guide on Cyber Security of Instrumentation and Control Systems in Nuclear Facilities (KINS/GT-N27)”, 12/2007, KINS

[2] 10CFR73.54 “Protection of Digital Computer and Communication Systems and Networks, 2009