Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 25-26, 2012

Cyber Security Level Assignment for Research Reactor Digital Instrumentation and Control System Architecture using Concept of Defense–in–Depth

Jinsoo Shin [a], Hanseong Son [b*], Gyunyoung Heo [a], Youngki Kim [c], Jaekwan Park [c]
[a]*Kyung Hee University, Yongin-si, Gyeonggi-do, 446-701, Korea*
[b]*Joongbu Univ., Chubu-myeon, Geumsan-gun, Chungnam, 312-702, Korea*
[c]*Korea Atomic Energy Research Institute, Deokjin-dong, Daejeon, 305-353, Korea*
[*]*Corresponding author: hsson@joongbu.ac.kr*

1. Introduction

Due to recent aging of the analog instrumentation of many nuclear power plants (NPPs) and research reactors, the system reliability decreases while maintenance and testing costs increase. In addition, it is difficult to find the substitutable analog equipments due to obsolescence. Therefore, the instrumentation and control (I&C) systems have changed from analog system to digital system due to these facts [1]. With the introduction of digital systems, research reactors are forced to care for the problem of cyber attacks because I&C systems have been digitalized using networks or communication systems. Especially, it is more issued at research reactors due to the accessibility of human resources. In the real world, an IBM researcher has been successful in controlling the software by penetrating a NPPs network in U.S. on July 2008 and acquiring the control right of nuclear facilities after one week. Moreover, the malignant code called “stuxnet” impaired the nearly 1,000 centrifugal separators in Iran according to an IAEA report. The problem of cyber attacks highlights the important of cyber security, which should be emphasized. Defense–in–depth (DID) is a significant concept for the cyber security to work properly. DID institutes and maintains a hardy program for critical digital asset (CDA) by implementing multiple security boundaries. In this work, we assign cyber security levels to a typical digital I&C system using DID concept. This work is very useful in applying the concept of DID to nuclear industry with respect to cyber security.

2. Methods and Results

In this section, the basic concept of DID and a digital I&C architecture are described. Furthermore, the level assignment of a digital I&C architecture using DID concept and the discussion about this are included.

2.1 Defense–in–Depth

Cyber security program must be designed, applied and maintained by using DID protective strategies to ensure the capability to detect, prevent, respond to, mitigate, and recover about CDA against cyber attacks. DID is a basic concept for safety design of nuclear facilities. DID concept provides enough margin with the design for nuclear facilities by priority. And it maintains the safe state of a system sustainably when it has some problem with its safety. The multi-barriers and multiple levels of protection concept are used in NPPs for DID design [2]. DID concept are also applied for the design of digital I&C system architecture for research reactors.

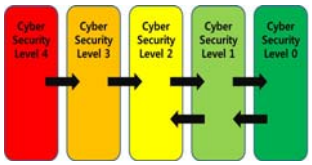

Fig. 1. The architecture of DID in cyber security

DID is an approach in which multiple levels of security and methods are deployed to guard against failure of one component or levels in terms of cyber security. The architecture of DID for cyber security is presented in Fig. 1. This defensive architecture includes the five concentric cyber security defensive levels separated by security boundaries. The systems requiring the greater degree of security are located within a greater number of boundaries. The Fig. 1 shown above does not always correspond directly to the physical location. The rule of this architecture is as follows. The CDAs associated with safety, important to safety and security functions, as well as support systems and equipments which, if compromised, would adversely impact safety, important to safety and security functions, are allocated to Level 4 and are protected from all lower. And only one-way data flow is allowed from level 4 to level 3 and from level 3 to level 2. The initiation of communications from digital assets at lower security levels to digital assets at higher security levels is prohibited. Data only flows from one level to other levels through a device or devices that enforce security policy between each level, by maintaining the capability to detect, prevent, delay, mitigate, and recover from cyber attacks [3].

2.2 Digital I&C Architecture

I&C systems are identified based on the safety and system functions for protecting, controlling and monitoring the facility. [4] The salient I&C systems are presented in the Fig. 2. These systems are Reactor Protection system(RPS), Post-Accident Monitoring System(PAMS), Reactor Regulating System(RRS),

Alternate Protection System(APS), Information Processing System(IPS), Process I&C System(PICS), Automatic Seismic Trip System(ASTS), Radiation Monitoring System(RMS), Main Control Room(MCR) and Supplementary Control Room(SCR).

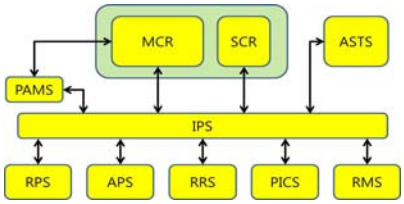

Fig. 2. Architecture of a digital I&C system

2.3 Level Assignment of I&C with DID

The CDAs that provide safety, important-to-safety, security, or control functions are allocated to defensive Level 4 protection and CDAs that provide data acquisition functions are allocated to at least defensive Level 3 protection according to RG- 5.71 [3]. The others can be classified depending on importance and relationship from Level 2 to Level 0. RPS, APS and ASTS are included in cyber security DID Level 4 due to their trip functions for a reactor in case of emergency. The PAMS is placed at DID Level 3 because it provides the necessary information for operators to monitor and take actions, if required, during and after a design basis accident. According to the demands from the operators, this allows the required information at the main control room. If Level 2 is defined as the information processing level acquired from Level 3, IPS is assigned to Level 2. The IPS is designed to provide plant status information to the MCR / SCR for assisting the plant personnel in operating the plant safely. The plant information is derived from other I&C systems such as RPS, RRS and PICS. Level 1 includes MCR, SCR, PICS and RRS. The MCR and SCR control the obtainable information from the IPS. The MCR is the place performed all operational actions related to the control and monitoring of plant process. The SCR is designed very similar to MCR but it is used under situation when the reactor operation in the MCR is not possible. The PICS is a computer based data processing and control system for the process system. It is connected to the IPS through the communication network for information integration in the MCR. The reactor power level is regulated, using control rods, by the RRS which is a computer-based system. The reactor control functions such as the reactor startup and the scheduled shutdown is performed by the RRS. This is achieved by an operator's changing the power levels through keyboard inputs and maintaining the reactor at a steady state. Level 0 is defined as the level to be controlled by Level 1 and, gives and takes the information with Level 1. The RMS is designed to measure, indicate and record the presence and level of radiation. Furthermore, the RMS allows to informing personnel protection and precluding the spread of radiation hazards. Therefore, it is assigned to Level 0.

2.4 Discussion

According to RG-5.71, the CDAs of cyber security DID Level 4 and Level 3 are defined clearly, but the others from Level 2 to Level 0 are not classified clearly until now. In order to apply the DID concept to cyber security for Korean NPPs and/or nuclear research reactors, they have to be defined clearly, though DID levels are assigned by accessibility of operators and safety in this work. Moreover, the digital I&C systems might not be regulated with only one cyber security level due to the complexity of its systems. For example, we consider that the RRS can be assigned from Level 4 to Level 0 because it is a CDA related with safety and at the same time it is controlled by MCR. It is because there are no clear boundaries among all levels for DID and the digital I&C systems are classified by large scale. The levels of security barriers according to DID concept shall be defined clearly and explicitly for cyber security of digital I&C systems.

3. Conclusions

Most of designers and operating organizations in nuclear industry are focusing on replacement of analog I&C systems with digital ones. In this paper, the concepts of DID and multi-barrier levels for the security of the digital I&C systems are explained. This approach can be applied in future studies to implement and evaluate the cyber security systematically. The architecture of digital I&C systems can be designed under this concept.

ACKNOWLEDGEMENT

This work was supported by Advanced Research Center for Nuclear Excellence (ARCNEX) program funded by the Ministry of Education, Science and Technology (Grant Number: 2011-0031773).

REFERENCES

[1] B. Gan, J. H. Brendlen, "Nuclear power plant digital instrumentation and control modifications," Nuclear Science Symp. And Medical Imaging Conf., IEEE Conference Record, Vol. 2, Oct. 25-31, 1992, 730, (1992)
[2] Edward G.wallance, Karl N Fleming, Edward M.Buras, "Next Generation Nuclear Plant Defense-in-Depth Approach", Idago National Laboratory(INL), Dec. 01, 2009
[3] Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, January 2010.
[4] ANSTO Replacement Research Reactor Project Safety Analysis Report Chapter 8 Instrumentation and Control, Nov. 01, 2004