Research on the Methodology of Verification of Vital Digital Assets

Yeeun Byun, Siwon Kim, Kookheui Kwon

Korea Institute of Nuclear Nonproliferation and Control, hibye@kinac.re.kr

INTRODUCTION

As the systems of nuclear power plants(NPP) are getting digitalized, cyber attacks against NPP are increasing. To prevent I&C systems from these cyber attacks, we intend to identify the vital digital assets(VDA) which could be related to the nuclear accidents and apply strengthened security measures for these VDA[1]. So in order to verify whether cyber attacks could cause nuclear accidents including core damage when identified VDA were attacked, this study was conducted. On the abroad, security evaluation environments, which can be represented by simulators or the like, is established for similar reasons and is used to evaluate the security of the I&C system. And also, vulnerability analysis and verification of security technologies are conducted by using these evaluation environments.

On the nuclear power plant, since it is difficult to perform actual penetration testing or assess the impact of accidents, to establish security evaluation environments for practical testing or verification is necessary. So we should study the methodology of establishing environments that can verify the impact of accidents on VDA, and by using these environments, we can build an effective regulatory approach to VDA. So in this study, to establish an environment for verifying VDA, we will analyze the current status of evaluation environments, that is, the current status of simulators, which is a representative facilities of evaluation environments, and identify the methodology for establishing environments of verifying VDA.

ANALYZE CURRENT STATUS

In this section, we will cover the overview of simulators which are representative of evaluation environments for cyber security, and which simulators are currently operating in domestic and abroad.

Overview of Simulators for Cyber Security

Simulators of NPP have been used increasingly for many years, especially for purposes other than operator training on digital systems in the main control room(MCR). Applications such as simulation assisted engineering(SAE) are being used to verify distributed control system(DCS) designs before or during plant commissioning. In addition, simulation software and applications are designed to support engineering groups responsible for the design and verification of digital systems and DCS of new or existing plants by integrating specific functions within the simulation platform to meet these growing trends and requirements of the nuclear industry.

The simulators for training operates in the same operating condition as the target power plants, so that it can easily identify cyber security vulnerability in digital and distributed systems. Also, it could be possible to identify the intrusion into the digital systems by manipulating important operation parameter, and warn the operators of the possibility of cyber attacks by the simulator.

In the US, the NRC defines simulators as essential facilities for operators to be equipped in accordance with 10 CFR 55[2] 'Regulation on Qualification Testing of Operators of Nuclear Power Plants'. The NRC issued several documents on simulator performance requirements and training operators since 10 CFR 55. It is the only document that imposes requirements on the operators as a law, and 55.45(a) covers 13 requirements of operating test. Also, in the R.O.K, RG-N17.08 has been developed by KINS(Korea Institute of Nuclear Safety). It includes all items such as mock coverage of system control and performance test requirements and it is applied for evaluation criteria for simulator of training and license testing of operators.

On the other hand, for cyber security of NPP, the NRC requires licensees to establish cyber security plans for NPP[3], also in the R.O.K, based on the Act on Physical Protection and Radiological Emergency, KINAC(Korea Institute of Nuclear Nonproliferation and Control) requires to establish such plans for NPP. The simulator could describe a cyber security vulnerability caused by the cyber attacks and provide a method for quickly and accurately identifying the cyber attacks.

Current Status of Simulators Operation

In this subsection, we will show the results of an analysis of the current status of simulators operating inside and outside of the Republic of Korea(R.O.K).

Domestic Status of Simulator Operation

In the R.O.K, from the late 1970s to the mid 1980s, a simulator was supplied by Westinghouse and Framatome, which were suppliers of NPP. From the early 1990s, "A plan for localization of a NPP simulation control panel" was established and Kori2, Yeonggwang3 simulator were developed and started to operate. The company participated in the localization of the initial simulator and aimed to enter and expand the business into the nuclear power sector based on this project. So, after dispatching about 20 developers to S3T(changed to GSE) for one year, localized the Kori2 and Yongkwang3 nuclear power plant simulators. In the 2000s, Kori1, Uljin3, Shin-Kori1 and Shin-Wolsung1 were developed by localized technology. There are about 12 simlators operating in the Repulic of Korea, and one for Barakah NPP. Applied software for each simulators will be introduced in the following subsection.

Components of Simulation

Simulation environment software is required to develop the nuclear simulators, and domestic simulation environment software is as follows.

- WSC(USA) 3KEYMASTERS: Apply to APR1400[a] nuclear reactor simulator

- GSE(USA) JADA: Application to OPR1000[b] nuclear reactor simulator

- LS MAPPS(Canada) ROSE: applied to heavy water reactor simulator

The hardware constituting the nuclear power simulator include the followings.

- Simulation computer system that enables real time simulation of software such as nuclear power plant model

- Instructor control panel to control the simulator

- Hardware panel manufactured by simulating the equipment of the reference room

- I/O devices for communication between the process model and the devices installed in the panel

Foreign Status of Simulator Operation

After the Three Miles Island NPP accident in 1979, the NRC strengthened regulations through a multifaceted review of operator education. Six simulators have been developed and operated by four reactor manufacturers (GE, Westinghouse, Combustion Engineering, and Babcock-Wilcox) operating NPP in the United States. NRC's Technical Training Center(TTC) consists of Reactor Technology Training Group, Specialized Technical Training Group and Technical Support Team.

In France, Electricite De France has built a performance-enhanced model or a new control room simulator for NPP throughout France. The simulator will also be used for training of safety engineers and operational team, safety probability testing, as well as nationwide crisis exercises 12 times a year.

METHODOLOGY OF VERIFICATION OF VDA

We have examined the overview of simulators for cyber security and current status of simulator operations inside and outside of the R.O.K. The followings are the verification environments and requirements for verifying whether cyber attacks can be linked to a nuclear accident when real cyber attacks are conducted with VDA targeting. In the first subsection, we will cover the verification environments in which the VDA verification will be applied through the status analysis, and in the next subsection, we will cover what requirements would be needed for such verification environments.

Verification Environments for VDA

In the case of the simulator operated by the domestic NPP as described above, the full scope of the power plant is simulated to implement the operation characteristics of the power plant, and it is operated for various purposes such as education and training. In addition, these simulators are not reflected in the cyber attacks. So it is necessary to derive appropriate cyber security requirements for digital systems and to develop verification environments considering their functions. And for designing the simulators, it can be connected to control the equipment, that is, the hardware.

- For APR 1400, it should be able to connect with equipment such as safety console, PLC of safety system(PPS, QAIS-P, RCOPS) and DCS of non-safety system

- For OPR 1000, it should be able to connect with equipment such as PCS, PMAS, turbine control system and RMS.

So, it would be more effective to utilize the existing simulators (hardware) than to build a new full-scope simulator. In addition, designing a new application (software) to get the more effective results for our purposes will be needed for VDA verification environments. Then through these conclusion, the followings are the requirements of the VDA verification environments.

Requirements for VDA Verification Environments

In this section, we will discuss the requirements for verifying the impact of VDA on cyber attacks. An analysis of target, initiating event, code and scenario should be performed, and details would be followed.

Target

It is necessary to analyze the targets of cyber attacks to be applied to the verification environments, and the probabilistic risk assessment(PRA) model can be applied to identify the VDA which is directly related to the accidents including core damage[1]. After the initiating event, the set of digital assets that could cause accidents is defined to the target sets. And considering the viewpoint of cyber security, it is more effective to prevent accidents by protecting only some of digital assets of target sets, rather than protecting all target sets. So one of the prevention sets can be identified as VDA to prevent accidents due to cyber attacks on all target sets.

Initiating Event

According to the results of the study, there are preliminary initiating events that occur initiating event. The derived initiating events include such as SLOCA(Small Loss Of Coolant Accident), LOFW(Loss Of Feed-Water) and LOCV(Loss of Condenser Vacuum). The target sets and prevention sets that are related to each event will be variously identified. We will focus on how we can prevent core damage when these initiating events occur.

Code

In this paper, code covers all tools for designing verification environments such as MOOSE(Multiphysics Object Oriented Simulation Environment). Most of the simulators currently operating are for training purposes, so they are dealing with the state of normal operation. However, in order to find out the impact of the accidents on the VDA, it is necessary to develop codes which could describe the situation besides normal operation conditions.

Scenario

It is also essential to develop scenarios for the VDA verification environments. In this case, the previously identified

[a]Advanced Power Reactor 1400, developed by the Korea Hydro & Nuclear Power(KHNP), Korea Electric Power Corporation(KEPCO), etc.

[b]Optimized Power Reactor 1000, designated as the Korean Standard Nuclear Power Plant

target, initiating event, etc. could be applied to develop scenarios. Scenarios can be developed to see cyber attacks on VDA can cause nuclear accidents, and if the prevention set is identified, what effects would be when control over this set fails.

Example of Application of VDA Verification Environments

It is assumed that SLOCA has occurred and there are 2 pumps(AF[c]-Pump-01,AF-Pump-02) and 3 valves(CC[d]-Valve-01,CC-Valve-02,CC-Valve-03) connected to some systems which operates to mitigate the SLOCA. And it is assumed that these five equipment must be attacked in order for SLOCA to cause accidents including core damage(all five equipment are digitalized equipment). It is described in Fig. 1.

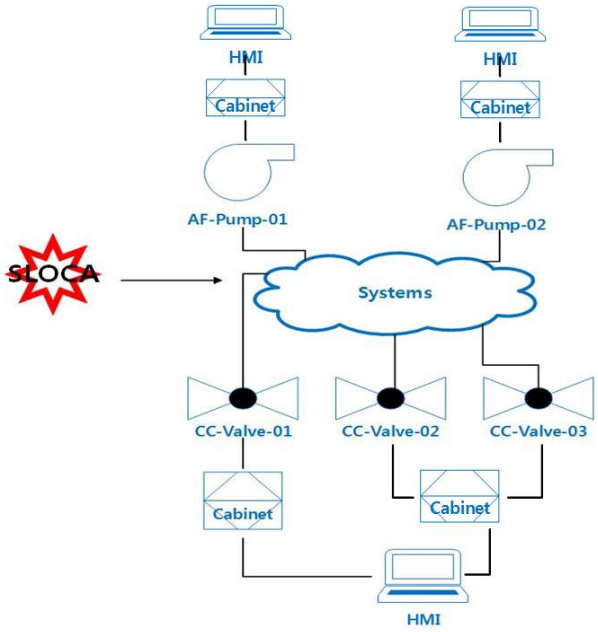

Fig. 1. Example of Accidents

To prevent accidents, at least one of these five equipment must work properly. That is, subsets of five equipment could be defined as prevention set and we could identify one for VDA.

In this case, we could derive 2 scenarios which could be applied to verification e nvironments. One would be able to construct a scenario in which after the SLOCA has occurred, all five equipment are subjected to cyber attacks by malicious code of human machine interface (HMI) and core damage occurs. Another scenario would be to configure the AF-Pump-01 to be properly protected and succeed in mitigating the impact of the accidents caused by cyber attacks. Various scenarios can be constructed, such as modifying prevention sets and combining them into multiple ones, which allows verification of VDA. In addition, many initiating events can be derived through the PRA model, and the target sets and prevention sets also can be derived.

[c]Auxiliary Feedwater
[d]Component Cooling

CONCLUSIONS

In order to investigate the methodology of VDA verification, we reviewed the overview of simulators which are representative facilities of verification environments for cyber security, and the current status of simulator operations inside and outside of the R.O.K. And we examined verifition methodology that can be applied in this study. In addition, we have found that targets, initiating events, codes, and scenarios are required for this verification environments and applied these requirements into example of accidents.

In this study, we used the methodology of VDA identification that was studied previously. It will be possible to identify targets and events through the derived result, and the scenario based on this will be applied to the verification environments to be developed in the future. Then we can reach a goal of this study to describe each of these scenarios in the verification environments and to describe the impact of the target sets when they are attacked and when the protection sets have succeeded in protecting them. Through this, it will be possible to verify the effects of cyber attacks on VDA, and it will be possible to develop ways to more effectively regulate cyber security at nuclear power plants.

ACKNOWLEDGMENTS

This work was supported by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety(KoFONS) using the financial resource granted by the Nuclear Safety and Security Commission(NSSC) of the Republic of Korea. (No. 1605007)

REFERENCES

1. K.KWON, “Research on Vital Digital Assets for Nuclear Cyber Security,” *ANS 2017 International Topical Meeting on Probablistic Safety Assessment and Analysis* (2017).
2. U.S.NRC, *Operators’ Licenses*, U.S. Nuclear Regulatory Commission (2017).
3. U.S.NRC, *Protection of digital computer and communication systems and networks*, U.S. Nuclear Regulatory Commission (2015).