An Analysis of Cyber-Attack on NPP Considering Physical Impact

In Hyo Lee[a], Han Seong Son[b*], Hyun Gook Kang[a]
[a] *Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology, 291 Daehak-ro, Yuseong-gu, Daejeon, South Korea*
[b] *Computer and Game Science, Joongbu Univ., 201 Daehak-ro, Geumsan-gun, Chungnam, South Korea*
**Corresponding author: hsson@joongbu.ac.kr*

1. Introduction

As NPP I&C systems are digitalized, cyber threats on NPP are also increasing. So, the necessity of research on cyber security for critical infrastructures like NPP becomes bigger. Some research teams performed related works on cyber-physical system which is a system that cyber-attack can lead to serious consequences including product loss, damage, injury and death when it is attacked [1], [2]. They investigated the physical impact on cyber-physical system due to the cyber-attack. But it is hard to find the research about NPP cyber security considering the physical impact or safety. In this paper, to investigate the relationship between physical impact and cyber-attack, level 1 PSA results are utilized in chapter 2 and cyber-attack analysis is performed in chapter 3.

2. PSA result analysis

In this section, accident sequence and components which are directly related to accident sequence and cyber-attack are analyzed. Also, digitalized control systems which are directly related to accident sequence and cyber-attack are analyzed. Target sequence is ATWS core damage sequence #27 in OPR 1000 event tree [3] and target accident is LOFW accident.

2.1. Accident sequence analysis

The initiating event LOFW can occur due to closure of FW control valve or closure of MSIV or MFIV or pump stop such as FW pump or condensate pump [4]. If these systems are failed by cyber-attack, initiating event will happen. It is modeled in Fig. 1.

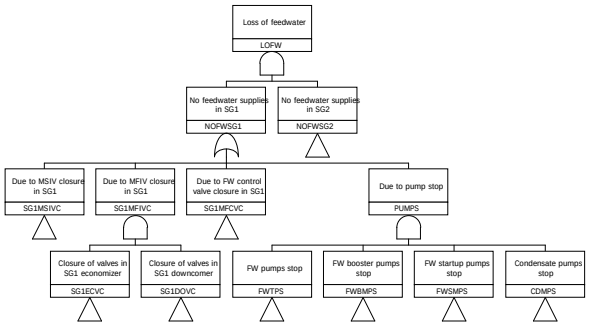

Fig. 1 Fault tree model of LOFW

After the initiating event happens, RPS and DPS tries to trip the NPP. If reactor trip fails due to cyber-attack, it goes to so called ATWS accident. Then, other mitigation measures are actuated such as heat removal by secondary side. In this situation, core is automatically cooled by AFWS. If this system also fails by cyber-attack, water will be directly injected in reactor vessel by HPSIS after operator successfully depressurizes RCS. If HPSIS doesn't work due to cyber-attack, core must be damaged. These are the ATWS core damage sequence #27.

2.2. Components & control systems analysis

Event tree well describes mitigation measures and those are shown in heading with fault tree. From the fault tree and P&ID diagram, components which are related to the accident mitigation, components which are controlled by digital I&C systems and digital I&C systems can be analyzed. Fig. 2 is a fault tree of failure of delivering auxiliary feedwater. In this fault tree, basic events which are not related to cyber-attack can be removed as shown in Fig. 2. In case of valve, check valve or manual valve failure is removed because they are not active system. Also remaining valves such as MOVs, SOVs, AOVs and E/H valves are analyzed based on P&ID diagram to link with digital I&C systems. In case of motor driven pumps, they can be failed directly by cyber-attack or failed due to pump room cooling related systems such as CCWS, ESWS failure. However, turbine driven pumps only can be failed when steam supplying systems are failed by cyber-attack. Because mitigation system failure in considering redundancy is modeled in fault tree, only analysis results on individual components are summarized in Table.1, 2 and 3. And related digital control systems are in Table.4 with their functions. The digital control systems are assumed that they are same as in APR 1400.

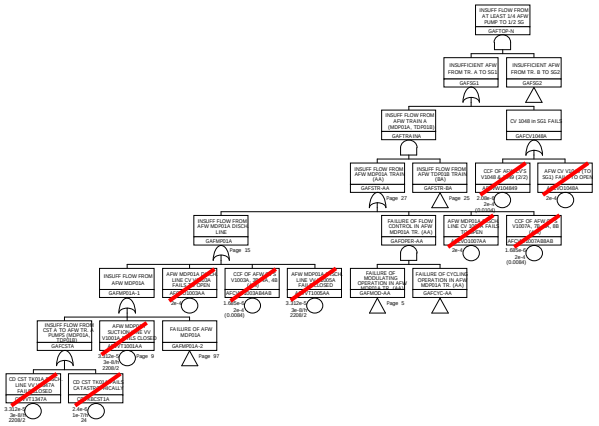

Fig. 2 Example of fault tree reduction (AFWS)

Table.1 Components related to accident mitigation (control signal: AFWS)

Component	Description	State (Normal)	State (AFAS)
1/2-521-V-109/110	AFW turbine steam supply valve	Close	Open
1/2-527-V-009/010	AFW turbine steam isolation valve	Close	Open
1/2-542-M-PP02A/PP02B	AFW motor driven pump	Standby	Start
1/2-542-V-035/036/037/038	AFW modulating valve	Open	Close/modulating
1/2-542-V-043/044	AFW isolation valve	Open	Open
1/2-542-V-045/046	AFW isolation valve	Close	Open

Table.2 Components related to accident mitigation (control signal: HPSIS)

Component	Description	State (Normal)	State (SIAS)
1/2-441-M-PP02A/PP02B	HPSI pump	Standby	Start
1/2-441-V-616/626/636/646	HPSI line isolation valve	Close	Open
1/2-441-V-617/627/637/647	HPSI line isolation valve	Close	Open
1/2-461-M-PP01A/PP01B/PP02A/PP02B	CCW pump	Start	Start
1/2-462-M-PP01A/PP01B/PP02A/PP02B	ESW pump	Start	Start

Table.3 Components related to keep steady state (control signal: MSIS)

Component	Description	State (Normal)	State (MSIS)
1/2-521-V-151/152/153/154	Main steam isolation valve	Open	Close
1/2-541-V-121/123/131/133	MFW isolation valve	Open	Close
1/2-541-V-122/124/132/134	MFW isolation valve	Open	Close
1/2-541-M-PP01/PP02/PP03	MFW pump	Start	Stop
1/2-541-M-PP04/PP05/PP06	MFW booster pump	Start	Stop
1/2-541-M-PP07	Startup FW pump	Start	Stop

Table.4 Digital control systems and their physical function

Type	Function	Control signal	Digital control system
Maintaining steady state of NPP	Supplement FW	FW control signal, MSIS	FWCS, RPS, ESF-CCS
Mitigation of accident	Reactor trip	Trip signal	RPS, DPS, ESF-CCS
	Supplement AFW	AFAS	RPS, DPS, ESF-CCS
	Safety injection	SIAS	RPS, DPS, ESF-CCS

3. Cyber security analysis on VDA

3.1. Attack type analysis

From the results in Table.1, Table.2, Table.3 and Table.4, there are five signals related to core damage sequence. FW control signal, AFAS, SIAS, trip signal and MSIS are them. When considering physical impacts on NPP by these signals, they are categorized into three ways. (1) FW control signal: this is not a safety signal. This signal keeps a NPP in steady state by controlling FW control valves and FW pumps. (2) AFAS, SIAS and trip signal: these are safety signals. These signals actuate plant safety functions such as heat removal and reactor trip. (3) MSIS: this is safety signal but different in (2). Signals in (2) actuate safety functions. However if MSIS is generated, it blocks the water passage and flow in FW line. So if it is generated in normal operation, NPP can be in transient. If consider the characteristics of control signals and actual components states, attack types are categorized as fallows. (a) An attack which blocks a control signal (AFAS, SIAS, trip signal): if components perform their safety function when they received actuate signal and they can't perform their function when they didn't receive actuation signal, hacker can implement this attack type. (b) An attack which makes a fake control signal (individual component control signal, FW control signal, MSIS): if components are working during normal state and type (a) attack can't work, hacker can implement this attack type to make plant in undesirable state such as valve closure or pump stop.

3.2. Vulnerability analysis and attack implementation

Vulnerabilities of digital control systems are used to attack digital I&C systems in ways described in 3.1. As shown in Table.4, some digital control systems are related to keep NPP in safety condition. Because their actual platform is DCS, PLC and industrial PC, vulnerabilities of them are investigated. All information is investigated in National Vulnerability Database (NVD) which is the U.S. government repository of standards based on vulnerability management data

Table.5 PLC vulnerability and cyber-attack impact

Vulnerability	Impact type
Stack-based buffer overflows	Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Privilege escalation	Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

Table.6 DCS vulnerability and cyber-attack impact

Vulnerability	Impact type
Stack-based buffer overflow	Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Heap-based buffer overflow	Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

Table.7 QNX Neutrino vulnerability and cyber-attack impact

Vulnerability	Impact type
Privilege escalation	Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Crafted packets to TCP port	Denial of service
Format string vulnerability	Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Stack-based buffer overflow	Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
World-writable permissions	Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Crttrap command	Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

represented [5]. In APR 1400, private OS is operated in PLC and vulnerability data depends on the source which is provided by vendor. And cabinet operated module in RPS and ESF-CCS are industrial PC which operated by QNX Neutrino OS. So, PLC, DCS and QNX Neutrino are used as keyword to search vulnerabilities. The results are given in Table.5 to Table.7. Using these vulnerabilities, hacker can implement attack like in 3.1. For example, if hacker connects engineering workstation (EWS) and PLC during overhaul period and attacks on PLC by stack-based buffer overflow attack using EWS, he can make unauthorized modification of PLC code. If the target is RPS BP and hacker modifies the BP logic to block the trip signal or ESFAS, hacker can implement the things that are described in 3.1.

4. Conclusion

The cyber security issue on NPP is inevitable issue. Unlike general cyber security, cyber-physical system like NPP can induce serious consequences such as core damage by cyber-attack. So in this paper, to find how hacker can attack the NPP, (1) PSA results were utilized to find the relationship between physical system and cyber-attack and (2) vulnerabilities on digital control systems were investigated to find how hacker can implement the possible attack. It is expected that these steps are utilized when establishing penetration test plans or cyber security drill plans.

REFERENCES

[1] Sandia national laboratories, Modeling and simulation for cyber-physical system security research, development and applications, SAND2010-0568, 2010
[2] D.Kundur, X.Feng, S.Liu, T.Zourntos, Towards a framework for cyber attack impact analysis of the electric smart grid, Smart Grid communications, 2010 First IEEE International Conference, 4-6 Oct.2010
[3] OPR 1000 PSA model, KAERI
[4] KAERI, Procedure for conducting Probabilistic Safety Assessment –Level 1 full power internal event analysis-, KAERI/TR-2548/2003, 2003
[5] National Vulnerability Database, https://nvd.nist.gov/home.cfm