Risk Assessment of Cyber-attacks on Nuclear Power Plants

Jong-Woo Park and Seung Jun Lee

Affiliation Information: 50, UNIST-gil , Ulsan, Republic of Korea, 44919, jonwoo822@unist.ac.kr

A cyber-attack is one of the new threats introduced by adopting digital technology to nuclear power plants. Though the cyber security against the cyber-attack is a serious issue in safety critical infrastructures, it is difficult to assess and model the cyber security because of lack of information, especially in nuclear power plants. The cyber security of a nuclear power plant has a different aspect from that of other industries because a strategy to defense only known attacks is not allowable for a nuclear power plant. A risk is defined as the product of frequency and consequence. Since a cyber-attack is an intended attack, it is not possible to estimate the frequency. Therefore, we focused on the consequence of a cyber-attack already occurred. In this work, the risk of cyber-attacks is assessed based on a probabilistic safety assessment (PSA) model. While an attack causing a serious consequence should be carefully considered in development of a cyber security strategy, attacks having negligible consequence does not have to be considered seriously. Based on the risk-information of cyber-attacks, it is possible to design an efficient defense strategy.

I. Introduction

Digitalized instrumentation and control (I&C) systems in nuclear power plants (NPPs) provide advantages for improving safety. High calculation speed and fault-tolerant techniques are the examples of the positive features. However, there are also negative effects such as newly introduced threats. A cyber-attack is a typical example. Recently, the cyber security of NPPs has been highlighted as one of the serious issues after the cyber-attack by 'Stuxnet' in an Iran's nuclear facility in 2007.

After 911, US, which has the most developed cyber security technology and database in the world, defined NPPs as the top important national facilities. US government has been making efforts to improve cyber security of NPPs through the research such as national test-bad. And US NRC published regulatory guideline about cyber security. In the report, US NRC provided which problems should be solved to protect software installed in an NPP, and what should be considered for improving cyber security. However, the research of cyber security or cyber-attack risk assessment is not mature.

The cyber security of an NPP has a different aspect from that of other industries. Generally, a vaccine is programmed to detect already known types of virus. When a new virus is observed, the vaccine is updated using the information of the new virus. In other word, unknown virus is not detectable. However, it is not allowable to detect only known attacks or prepare a vaccine after attacks for an NPP. A strategy to defense only known attacks is not allowable for highly safety-critical systems.

In this work, a method to assess the risk of cyber-attacks based on a probabilistic safety assessment (PSA) was proposed. Based on the risk-information of cyber-attacks, it is possible to design an efficient defense strategy. For example, while an attack causing a serious consequence should be carefully considered in development of a cyber security strategy, attacks having negligible consequence does not have to be considered seriously.

II. Methods

From the viewpoint of safety, the risk of a cyber-attack can be expressed as following equation.

*Risk of a cyber-attack = P(cyber-attack) * P(event | cyber-attack) * C(event).*

P(cyber-attack) indicates a probability of a cyber-attack, *P(event | cyber-attack)* means the probability of an event caused by the cyber-attack, and *C(event)* represents the consequence due to the event. However, a cyber-attack is an intended

attack, so it is meaningless to estimate the probability of a cyber-attack. Therefore, in this work, we analyzed the consequence of possible cyber-attack.

There have been no widely accepted risk assessment model for cyber-attacks. This work utilizes a PSA model to estimate the risk of a cyber-attack and to identify dangerous scenarios. Core damage frequency (CDF), which is evaluated in level 1 PSA, is one of the measures to estimate an NPP safety. The ET/FT (Event Tree and Fault Tree) method is popular one to build a CDF estimation model. Lots of basic events including component failures and human error are considered in an ET/FT model. If an NPP is infected by a virus, the effect of the virus can be represented by a component failure or by a human error. That means, it is possible to represent the effect of a cyber-attack on the CDF by setting the failure probability of a component or a human action as a hundred percent.

In this work, the PSA model was used, which was developed for a digitalized NPP having digitalized RPS (Reactor Protection System) and ESFAS (Engineered Safety Features Actuation System). To evaluate the effect of a cyber-attack, the minimal cutsets (MSCs) were analyzed. Among MCSs, important MCSs were selected and the basic events in them were analyzed. Some basic events could be failed by a cyber-attack directly or indirectly, and some does not have any relation with a cyber-attack. Then, the CDF was recalculated by setting the failure probabilities of the related basic events as 1 to observe the effect of a cyber-attack.

III. Result

1. Analysis of Contribution to CDF

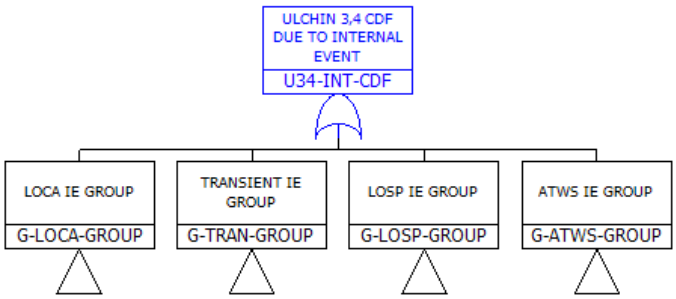

Fig. 1. A part of PSA model

As shown in Fig. 1, the CDF is evaluated with consideration of possible initiating events such as LOCA, LOSP, ATWS and so on. First, as mentioned in the previous section, MCSs were analyzed as shown in Fig. 2. Among thousands MCSs, 500 MSCs, which occupy about 85% of the CDF, were analyzed.

Table 1. The part of CDF table of NPP model in AIMS.

NO	VALUE	F-V	ACC	EVENT#1	#2	#3	#4	#5
1	3.72E-07	0.061037	0.061037	%ILOOP-SBO	EGDGW01ABET	NR-AC11HR		
2	3.52E-07	0.057836	0.118873	%ILOOP	EDBYW125DC	FLAG-ID-LOOP-025		
3	3.07E-07	0.050359	0.169232	%ISL	FLAG-ID-NR-AC8HR	HSMVW67576		
4	2.66E-07	0.043705	0.212938	%IRVR				
5	1.59E-07	0.026116	0.239054	%IML	FLAG-ID-REC-HSMV6756	HSOPHHLCLR		
6	1.59E-07	0.026116	0.265171	%ILL	FLAG-ID-REC-HSMV6756	HSOPHHLCLR		
7	1.50E-07	0.024646	0.289817	%ISL	FLAG-ID-NR-AC8HR	HSSPPSUMP		
8	1.49E-07	0.024446	0.314262	%ILOOP	AFOPHALTWT	EGDGK01ABET	FLAG-ID-NR-AC18HR	
9	1.46E-07	0.024034	0.338297	%ILOOP	AFTPW01B2A	EGDGK01ABET	FLAG-ID-LOOP-025	
10	1.46E-07	0.02394	0.362237	%ILOOP	AFOPHPPSTART	EGDGK01ABET	FLAG-ID-NR-AC18HR	
344	1.35E-09	0.000222	0.830948	%ILODC	DPSKAPLC2	FLAG-ID-NR-AC1HR	FSQPFCLP2A	SDOPHEARLY
345	1.35E-09	0.000222	0.83117	%ILODC	DPSKAPLC1	FLAG-ID-NR-AC1HR	FSQPFCLV1A	SDOPHEARLY
346	1.35E-09	0.000222	0.831393	%ILODC	DPSKAPLC1	FLAG-ID-NR-AC1HR	FSQPFCLP2A	SDOPHEARLY
347	1.35E-09	0.000222	0.831615	%ILODC	DPSKAPLC1	FLAG-ID-NR-AC1HR	FSQPFCLP1A	SDOPHEARLY
348	1.35E-09	0.000222	0.831837	%ILODC	DPSKAPLC2	FLAG-ID-NR-AC1HR	FSQPFCLP1A	SDOPHEARLY
349	1.35E-09	0.000222	0.832059	%ILODC	DPSKAPLC2	FLAG-ID-NR-AC1HR	FSQPFCLV2A	SDOPHEARLY
350	1.35E-09	0.000222	0.832281	%ILODC	DPSKAPLC1	FLAG-ID-NR-AC1HR	FSQPFCLV2A	SDOPHEARLY
351	1.35E-09	0.000222	0.832503	%ILODC	DPSKAPLC2	FLAG-ID-NR-AC1HR	FSQPFCLV1A	SDOPHEARLY

The basic events related to digital I&C systems should have top priority in the analysis because they might be the first target of an attack. However, the other basic events could be affected by a cyber-attack. For example, while a cyber-attack cannot directly cause an operator error, it is possible to make a human error indirectly by providing wrong information via infected monitoring systems. If an EDG is controlled by digital system, the failure on demand of the EDG should be considered in cyber-attack analysis.

Therefore, we analyzed three cases. The first case is the attack on digital I&C systems, the second case is the attack on digital control system for EDGs, and the last case is the attack on monitoring systems for main control room operators. In Table 1, blue, yellow, and red basic events represent human errors, failures related to EDG (Emergency Diesel Generator), and failures in digital I&C systems respectively.

Table 2. Basic events directly related to cyber-attack

Basic event	Detail
DPSKAPLC1	FAILURE OF DPS CH.1 SIGNAL PROCESSOR (PLC1)
DPSKAPLC2	FAILURE OF DPS CH.2 SIGNAL PROCESSOR (PLC2)
DPTCAMG2	TRIP CONTACTOR FOR MG SET-2 (DPS-2) FAILS TO ACTUATE (OPEN)
DPTCAMG1	TRIP CONTACTOR FOR MG SET-1 (DPS-1) FAILS TO ACTUATE (OPEN)
FSQPFCLP2A	DO FOR CL-P2A FAILS TO PROVIDE OUTPUT
FSQPFCLP1A	DO FOR CL-P1A FAILS TO PROVIDE OUTPUT
FSQPFCLV1A	DO FOR CL-V1A FAILS TO PROVIDE OUTPUT
FSQPFCLV2A	DO FOR CL-V2A FAILS TO PROVIDE OUTPUT
RPOMWCP	CCF ALL DIGITAL OUTPUT MODULES
RPPMWBP	CCF ALL BISTABLE PROCESS MODULES
RPWDJBPCCF	BP WDT FAILS TO DETECT CCF

When the basic events of digital I&C systems are considered, their contribution to the CDF is only 0.266%. While the CDFs when cyber-attacks on EDG and monitoring system are contributed 33.8% and 38.3%.

2. RAW Analysis

RAW (Risk Achievement Worth) is one of the importance measures to observe total system failure probability when the failure probability of a component is set to one. As mentioned previously, the effect of a cyber-attack can be evaluated by assuming the failure rate of the corresponding basic events as one. Therefore, RAW was used to evaluate the possible risk of a cyber-attack.

Table 3. A part of RAW chart of NPP only possible to cyber-attacks

#	EVENT	PROB	F-V	RRW	RAW	BIRNBAUM	# OF MCS
52	HSOPHHLCLR	9.35E-04	0.052233	1.055112	56.812	0.00034	2
63	RPOMWCP	2.63E-05	0.000888	1.000889	34.741	0.000205	54
69	AFOPHALTWT	1.45E-03	0.041334	1.043116	29.465	0.000173	575
85	AFOPHPPSTART	1.42E-03	0.037818	1.039304	27.594	0.000162	439
109	RPRYWIR	8.51E-07	0.000012	1.000012	14.81	0.000084	2
116	RPPMWBP	1.27E-04	0.00143	1.001432	12.285	0.000069	69
136	AFOPUV1015BB	3.75E-04	0.001865	1.001868	5.971	0.00003	86
137	AFCVO1003BB	2.25E-04	0.001096	1.001097	5.863	0.00003	65
138	AFCVO1007BB	2.25E-04	0.001096	1.001097	5.863	0.00003	65
139	AFCVO1012BB	2.25E-04	0.001096	1.001097	5.863	0.00003	65
151	FSQPKQPALL	9.53E-05	0.000385	1.000385	5.037	0.000025	17
152	FSFRKFORALL	9.94E-05	0.000401	1.000401	5.037	0.000025	17
153	FSFTKFOTALL	9.94E-05	0.000401	1.000401	5.037	0.000025	17
157	RPIMWAIBP	6.47E-05	0.000242	1.000242	4.747	0.000023	14
161	FSDPKDPALL	2.03E-05	0.000072	1.000072	4.541	0.000022	7

Table 3 shows a part of RAW list. Red and black basic events represent digital I&C and operator failure respectively. For example, RPOMWCP is one of the basic events for RPS. If RPOMWCP is assumed as failed, then the CDF increases about 35 times. In the same way, HSOPHHLCLR is the one of operator failure basic events. If HSOPHHLCLR is assumed as failed, then CDF will increase about 57times.

As mentioned, the analyzed NPP in this work has digital RPS, ESFAS, and DPS (Diverse Protection System). If a cyber-attack makes a failure of a component but a system, for example, the whole RPS is unavailable by a cyber-attack, then the effect of the attack will be much serious. In the analysis results, it was observed that the CDF increases about 450 times by unavailable RPS by a cyber-attack Table 4 shows the analysis results at system level. As shown in the table, attacked ESFAS increases CDF about 200 times, and attacked DPS makes increase of CDF by 9 times ESFAS is attacked through cyber-attacks, then CDF is increased 200 times. And DPS is attacked, then CDF is increased 9 times. For the worst case, if it is assumed that all PCS card are failed by a cyber-attack, then the CDF increases 25521 times.

Table 4. The result table of other system is cyber-attacked

RP_ATT	FS_ATT
About 450 times increased	About 200 times increased
DP_ATT	**CX_ATT**
About 9 times increased	About 25521 times increased

IV. CONCLUSIONS

In this work, the risk assessment of cyber-attacks was performed based on the plant PSA model. This method is to estimate the cyber-attack risk by identifying the influenced factors in the plant PSA model. It is not necessary to develop a new model for the cyber security. In the proposed method, cyber-attacks are represented as basic events in a plant PSA model, and the change of CDF is analyzed for the assumed attacks. Only some cases were analyzed in this work, so more various scenarios should be analyzed. Further study should be conducted to identify possible cyber-attacks not considered in this work for the accurate and reliable assessment.

REFERENCES

1. Do-Yeon Kim, Cyber security issues imposed on nuclear power plants, Annals of Nuclear Energy (2013)
2. JaeKwan Park, YongSuk Suh, Cheol Park, Implementation of cyber security for safety systems of nuclear facilities, Annals of Nuclear Energy (2015)
3. P.A.S. Ralstona, J.H. Grahamb, J.L. Hiebb, Cyber security risk assessment for SCADA and DCS networks, Science Direct (2007)