# Cyber Threat Scenario Development Process Reflecting DBT Attributes and CDA Characteristics

Seungmin Kim [a, b], Gyunyoung Heo [b], Kookheui Kwon [c]
[a c] *Korea Institute of Nuclear Nonproliferation and Control, Yuseong-daero, Yuseong-gu, Daejeon 34057, Korea*
[a b] *Kyung Hee Univ., Deogyeong-daero, Giheung-gu, Yongin-si, Gyeongi-do 17104, Korea*
[*] *Corresponding author: viavacita@kinac.re.kr*

***Keywords : Cybersecurity, Nuclear Facility, Cyber-attack Scenario, Design Basis Threat**

## 1. Introduction

According to the Act on Physical Protection and Radiological Emergency, the licensees of nuclear facilities should assess cyber threats every three years to comply with physical protection policies and set Design Basis Threat(DBT) that serve as criteria for designing physical protection systems [1]. Nuclear licensees develop cyber threat scenarios and corresponding response scenarios to demonstrate the capability to protect against cyber threats within the DBTs. However, due to the lack of detailed methods for developing cyber threat and response scenarios, some scenarios can't demonstrate the capability to protect against threats within the DBTs. Therefore, this paper presents a process for developing cyber threat scenarios.

## 2. Process for Developing Cyber Threat Scenario

DBT represents the maximum threats that nuclear licensees should protect against. Fig. 1 shows the overview of DBT and the responsibility of nuclear licensees. Licensees develop cyber threat and response scenarios to demonstrate that physical protection systems of nuclear facilities have been established against newly identified threats from new DBTs. This paper presents the process for developing cyber threat scenarios, which are part of the threat and response scenarios. The process includes determining general information from DBT attributes, classification of types of CDAs, determining attack vectors for CDAs, matching attack techniques, and evaluating the impact on nuclear facilities.

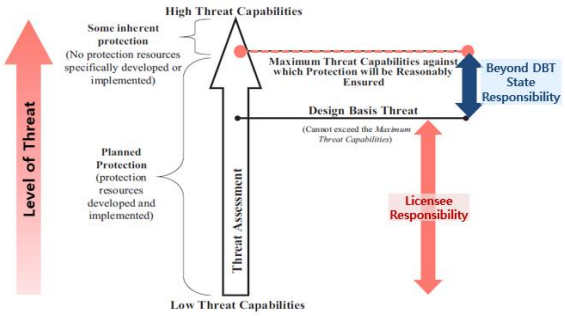


Fig. 1. Overview of DBT and responsibility of licensee

The process and overview diagram for developing cyber threat scenarios are shown in Fig. 2.

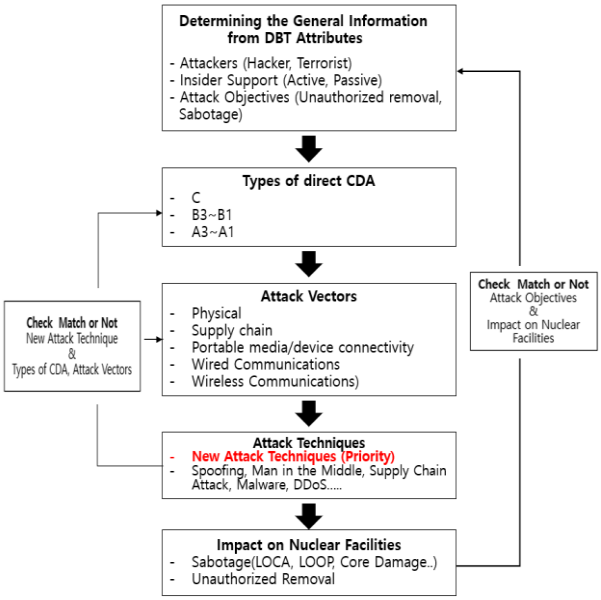


Fig. 2. Progress of Developing Cyber Threat Scenarios

### 2.1 Determining the General Information from DBT Attributes

The first step in the development process of the cyber threat scenario is to determine the general information to be used in the cyber threat scenario, and DBT attributes are utilized to select the general information.

DBT attributes may vary depending on the DBT level set by each country and are usually managed as classified documents. Therefore, this paper refers to the Appendix of IAEA Nuclear Security Series (NSS) No. 10 (Rev.1), "National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements." The Korea Institute of Nuclear Nonproliferation and Control (KINAC)/RS-011, "Cyber-security Exercise for Nuclear Facilities," selected the common points presented in both documents as general information [2,3].

As a result, general information is defined as types of attackers (hackers, terrorists), insider support (active,

passive), and attack objectives (unauthorized removal, sabotage).

### *2.2 Classification of types of direct CDAs*

The second step is to classify the types of CDAs. To develop cyber threat scenarios, cyber threat targets must be selected. Cyber threat targets consist of CDAs possessed by nuclear facilities. CDAs perform safety-related, important-to-safety, security, and emergency preparedness functions and are digital devices that nuclear licensees must protect against cyber threats. CDAs can be classified as non-direct CDAs and direct CDAs. Non-direct CDAs do not critically affect atomic facility safety and security, so they are excluded from the scope of this paper. Direct CDAs can be classified based on hardware characteristics and functionalities, as shown in Table 1.

Table 1: Type classification based on CDA characteristics

| Types of CDA | Description |
|---|---|
| C | PC type |
| B3 | Not classified as type C but have communication ports excluding RS-232, 422, 485 ports or support storage devices through USB/memory card connection ports |
| B2 | Not classified as type C or B3 but can change internal programs through communication functions |
| B1 | Not classified as type C or B3 and cannot change internal programs through communication functions |
| A3 | Not classified as type C or B1~B3 but can change internal settings (excluding operating variables) through HMI devices |
| A2 | Not classified as type C, B1~B3, or A3 but can change operating variables through HMI devices such as built-in buttons |
| A1 | Not classified as type C, B1~B3, or A3 and cannot change operating variables through HMI devices such as built-in buttons |

### *2.3 Determining Attack Vectors for CDAs*

The third step is to determine attack vectors for CDAs. Attack vectors can be identified based on the classification results of CDAs. Attack vectors can be classified as pathways for accessing cyber threat targets. This paper adopts the classification criteria provided by the Nuclear Energy Institute (NEI) in NEI 08-09 "Cyber Security Plan for Nuclear Power Reactors," which was developed to comply with the U.S. Nuclear Regulatory Commission's Regulatory Guide 5.71(R.G.5.71) for cyber security implementation and regulatory guidelines for U.S. nuclear facilities. The classification criteria provided in NEI 08-09 are physical access to the CDA, supply chain access to the CDA, portable media/device connectivity to the CDA, wired communications with the CDA, and wireless communications with the CDA [4].

The attack vectors identified based on the classification of CDAs by hardware characteristics and functionalities can be matched. For example, C-type assets correspond to all five attack vectors, while A1 assets, which do not have communication ports and functionalities, correspond to physical and supply chain access.

### *2.4 Matching Attack techniques and evaluating the Impact on Nuclear Facilities*

The fourth step matches attack techniques within the DBT based on the analysis results of the second and third processes. The characteristics of CDAs and attack vectors limit attack techniques. For example, the C-type CDA can be subjected to most attack techniques because all five attack vectors are possible, while the A1-type CDA is unable to perform network-related attack methods such as Spoofing due to the absence of data communication. However, if a new attack technique is set in DBT, licensees should prioritize the new attack technique. The attack vector and CDA type shall be reviewed for validity if a new attack technique is selected. If the review shows that the attack vector and CDA type are invalid, the attack vector and CDA type shall be re-selected.

The last step is to assess the impact on nuclear facilities. When the selected attack techniques succeed against the chosen target systems, it is necessary to predict what impact may occur, which should be consistent with the attack objectives mentioned in the general information.

## 3. Example of Cyber Threat Scenario Development Process

This section provides an example of the process for developing threat scenarios described in section 2. In the first step, general information defines the types of attackers as hacker groups, insider support as passive support(providing information about target systems), and the attack objective as sabotage. In the second and third steps, it is assumed that there are C-type CDAs in the Engineered Safety Features-Component Control Systems(ESF-CCS). C-type CDAs are susceptible to all five attack vectors, but supply chain access to the CDA is selected. In the fourth step, it is assumed that the supply chain attack is newly set as a threat in DBT. The

new attack technique should be validated for types of CDA(C type) and attack vectors (supply chain) and can be validated.

The fifth step evaluates the impact of cyber intrusions on nuclear facilities and shows that the ESF-CCS, whose logic has been altered by a supply chain attack, is susceptible to sabotage by failing to operate normally during a plant emergency such as a LOCA(Loss of Coolant Accident). This is also consistent with the attack objective set in the general information.

The cyber threat scenario is summarized as follows: A hacker group obtains information about the target system (ESF-CCS) through insider support and manipulates the logic of a newly introduced ESF-CCS CDA (C type). The manipulated CDA does not function properly in the event of an emergency, such as a LOCA, which affects the sabotage objective.

## 4. Conclusions

This paper presents the process of developing cyber threat scenarios by determining general information from DBT attributes, classifying types of CDAs, determining attack vectors for CDAs, matching attack techniques, and evaluating the impact on nuclear facilities. The cyber threat scenario process presented in this paper can be utilized for physical protection system integrity verification through DBT reconfiguration and for developing threat scenarios for cyber security exercises. However, preliminary impact analysis is required to accurately determine whether the selected cyber threat targets(CDAs) are affected by cyber intrusions such as Unauthorized removal or sabotage. Preliminary impact analysis should utilize risk-informed decision-making results such as PSA (Probabilistic Safety Assessment), and the validation of the attack objectives through preliminary impact analysis will be supplemented in future research.

## REFERENCES

[1] NSSC, Act on Physical Protection and Radiological Emergency, NSSC, 2022.
[2] IAEA, Nuclear Security Series (NSS) No. 10 (Rev.1), National Nuclear Security Threat Assessment Design Basis Threats and Representative Threat Statements, IAEA, 2021.
[3] KINAC, Regulatory Standard 011, Cyber-security Exercise for Nuclear Facilities, KINAC, 2020.
[4] NEI 08-09, Cyber Security Plan for Nuclear Power Reactors, NEI, 2010.