Development of Cyber Threat Information Model

Kwang-Seop Son *, Jae-Gu Song, Jung-Woon Lee
Security R&D Team, Korea Atomic Energy Research Institute, 111 Daedeok-daero 989 beon-gil, Yuseong-gu, Daejeon, South Korea
**Corresponding author: ksson78@kaeri.re.kr*

1. Introduction

As a part of Development of Nuclear Safety Regulatory Technologies project, we research a quantitative risk assessment for cyber attacks to Nuclear Power Plants (NPPs). In order to assess a cyber risk, it is necessary to develop the cyber threat information model (CTIM) for target system. The CTIM is a series of process to analyze and identify the representative features of adversarial threats such as threat sources, attack vectors, threat events, threat scenarios, and so on. If the CTIMs are well established, the cyber threats and the consequences of adversary impacts on the target system could be systematically analyzed and identified. In this study, we propose the CTIM applicable to the NPPs.

2. Cyber Threat Information Model

The NPPs have many systems according to the functions or missions, which also consist of various equipment to perform the functions or missions. It is therefore effective to develop the CTIM configured as the system-level and component-level CTIM. The key object of the system-level CTIM is to identify the threat scenarios and the main object of the component-level is to identify the threat events and attack vectors organizing the threat scenarios identified in the system-level CTIM.

2.1 System-level CTIM

In order to identify the threat scenarios for the target system, the following information have to be included in the system-level CTIM:

- System ID
- Installation location
- Main functions
- Security functions and status of cyber security plans (CSPs)
- Components
- Internal and external interface
- Method to test and repair
- Identification of threat
- Identification of threat scenarios

For the establishment of systematic threat scenarios, we use the System Theoretic Process Analysis (STPA) method. The differences between the STPA and the proposed method in this study are as follows:

Table I: Differences between the STPA and the proposed method

	The STPA	The proposed method
Risk assessment	Safety risk	Cyber security risk
Structure model	Control structure based on components	Threat structure based on Critical Digital Assets (CDAs), which should be protected from cyber threat (As define RG 5.71[1])
Unsafety Control Actions (UCAs)	Using the control structure, unsafe behaviors are identified based on control actions and feedbacks between controllers and controlled process	The exploitable threats are identified through analyzing the attack vectors and threat events of CDAs
Scenarios	The loss scenarios are identified through analyzing the causal factors leading UCAs or hazard in the point of view of control	The threat scenarios are identified based on the attack vectors and threat events of CDAs in the point of view of cyber security

The procedures of identifying the threat scenarios are shown in Fig. 1.

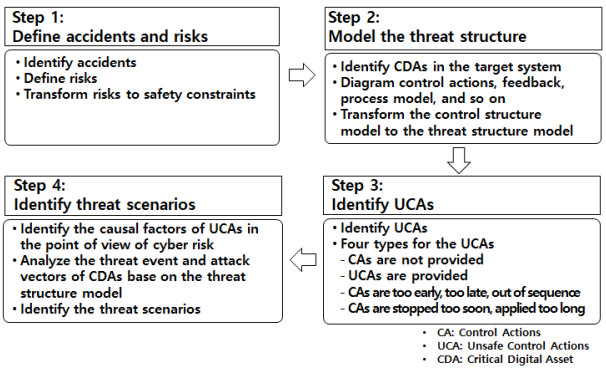

Fig. 1. The procedures of cyber threat scenarios based on the STPA [2]

There are the following approaches to analyze the causal factors of the UCAs in Fig. 1:

1) Unsafe control behavior in the controller (Problems in the controller itself)
2) Inadequate feedback or information to the controller (Problems in the controller input)
3) Inadequate control actions from actuator to the controlled process (Problems in the controller output)
4) Inadequate input or output to/from the controlled process (Problems in the controlled process)

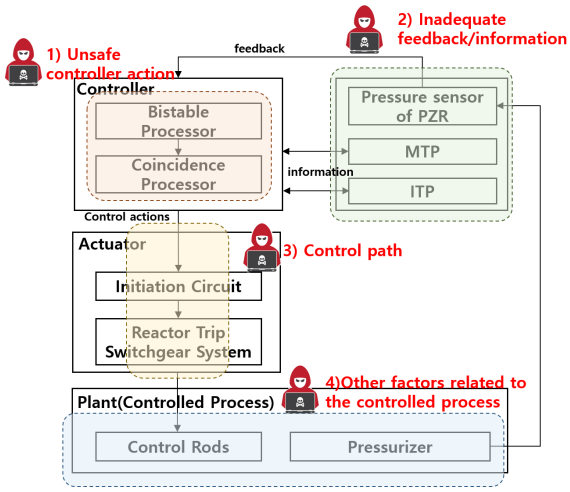

Fig. 2. Approaches to identify the cyber threat in the case of Reactor Protection System (RPS)

2.2 Component (CDA)-level CTIM

In order to identify the threat events and attack vectors, the component-level CTIM includes the following information:

- CDA ID
- CDA Type
- OS version and customized/commercialized
- CDA class based on NEI 13-10
- Security level
- Physical interface
- Communication protocol
- Objects accessible to CDA
- Status of CSPs
- Main functions
- Critical Data
- Input/Output signals
- Threat events
- Attack vectors

The threat events and attack vectors in component-level CTIM organize the threat scenarios identified in the system-level CTIM. The possible threat events in the CDAs are as shown in Table II.

Table II: Possible threat events in the component (CDA)-level [3]

Threat Events	Description
Denial of Control Action	Control systems operation disrupted by delaying or blocking the flow of information, thereby denying availability of networks to control system operator
Control Devices Reprogrammed	Unauthorized changes made to programmed instructions in Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Distributed Control System (DCS), or SCADA (Supervisory Control, And Data Acquisition) controllers, alarm thresholds changed, or unauthorized command issued to control equipment
Spoofed Status Information	False information sent to control system operators either to disguise unauthorized changes or to initiate inappropriate action by system operators
Control Logic Manipulation	Control system software or configuration settings modified, producing unpredictable results
Safety functions modified	Safety functions are manipulated such that they either do not perform when needed or perform incorrect control actions that damage the ICS
Malware on Control devices	Malicious software introduced into the devices

The attack vectors in the CDAs are as follows [4]:

- Direct network connectivity
- Wireless network capability
- Portable media and equipment
- Supply chain
- Direct physical access

From the threat events and attack vectors, the threat identification model for CDA can be expressed in Fig. 3.

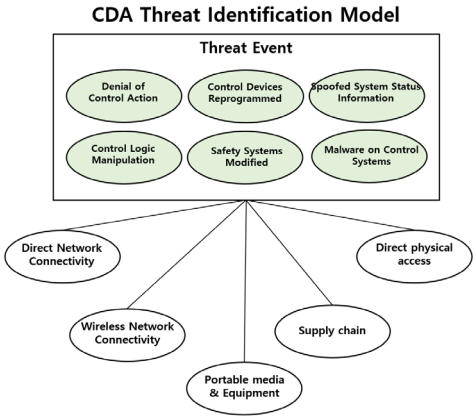

Fig. 3. Threat identification model for CDA

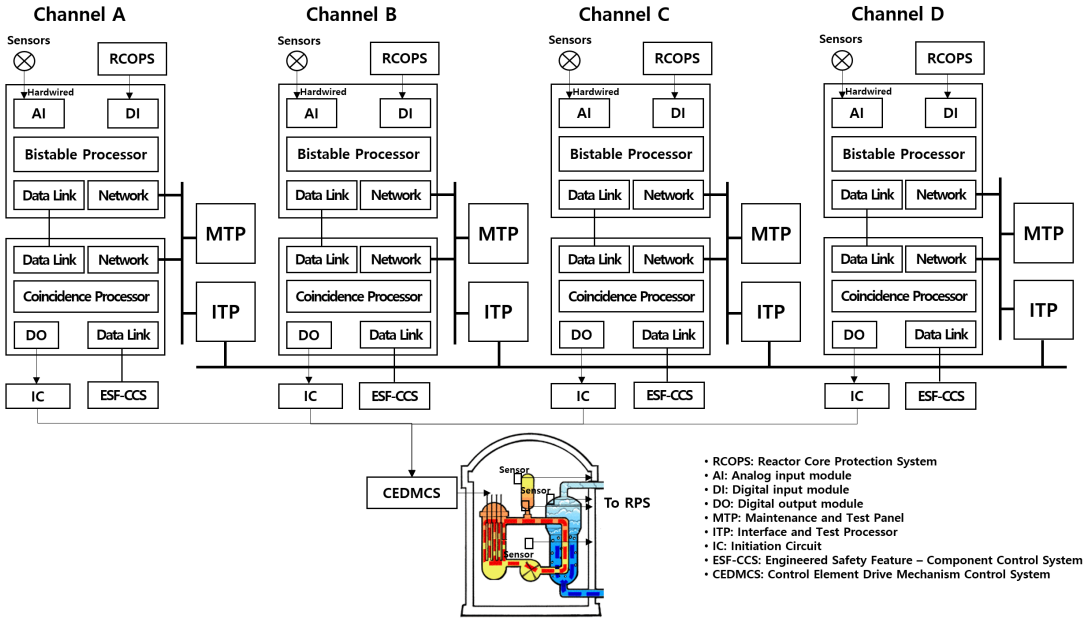

Fig. 4. Typical structure of RPS

2.3 Case study: Reactor Protection System (RPS)

The main object of CTIM is to identify the threat scenarios in the system-level, the threat events and attack vectors in component-level. Therefore, in this section, we focus on the identification of threat scenarios in the RPS. The RPS is one of safety systems, which continue to monitor the safety variables and generates Reactor Trip (RT) and Engineered Safety Feature (ESF) initiation signals when the safety variables are out of normal range. Typical structure of RPS is shown in Fig. 4. The functions of key components of RPS are as follows:

- Bistable Processor (BP): RT signals generations except for the Local Power Density (LPD) and the Departure Nucleate Boiling Ratio (DBNR)
- Coincidence Processor (CP): Determination of channel trip through 2/4 voting for four BPs
- Initiation Circuit (IC): Delivering the channel trip signal to Control Element Drive Mechanism Control System (CEDMCS)
- Maintenance and Test Panel (MTP): Local panel for the RPS test and maintenance
- Interface and Test Processor (ITP): Testing the RPS and interfacing with the other ITPs in each channel

The systems interfacing with the RPS are Reactor Core Protection System (RCOPS), Engineered Safety Feature – Component Control System (ESF-CCS), and CEDMCS, of which functions are as follows:

- RCOPS: RT signals generation of the LPD and the DBNR in the reactor core
- ESF-CCS: According to the ESF initiation of RPS, related pumps and valves operate.
- CEDMCS: By performing selective 2/4 voting logic for four channel trip signals, all control rods are inserted into the reactor core.

In order to identify the threat scenarios, accidents and risks of target system should be defined and be transformed to the safety constraints (SCs) in the same way of the STPA. Generally, the safety systems in NPPs are designed and implemented through Quality Assurance (QA) and Validation & Verification activities. The functional requirements (FRs) in the target system requirements (SRs) are defined from conceptual design phase, and then the detailed hardware and software are designed and implemented based on the FRs. The FRs could be therefore safety constraints (SCs). Based on the STPA, the system loss, hazard and SC of RPS are summarized in Table III.

Table III: System loss, hazard and SC of RPS

System loss	System hazard	Safety constraint [5]
• L1: Human injury • L2: Environmental pollution • L3: System damage • L4: Unavailable electrical power	• H1: Release of radioactive materials • H2: Temperature and pressure of Reactor Coolant System (RCS) too high • H3: Equipment operated beyond normal range	• SC1: Reactor Trip (RT) • SC2: ESF initiation • SC3: Bypass • SC4: Control rod withdrawal prohibit • SC5: Monitoring and displaying system status

	· H4: Plant shutdown	· SC6: Test and diagnosis · SC7: Interlocks

Using the CDA threat identification model in Fig. 3, we can model the threat structure based on the control structure. Fig. 5 shows the control and threat structure of the RPS, which are only for one channel for the simplification.

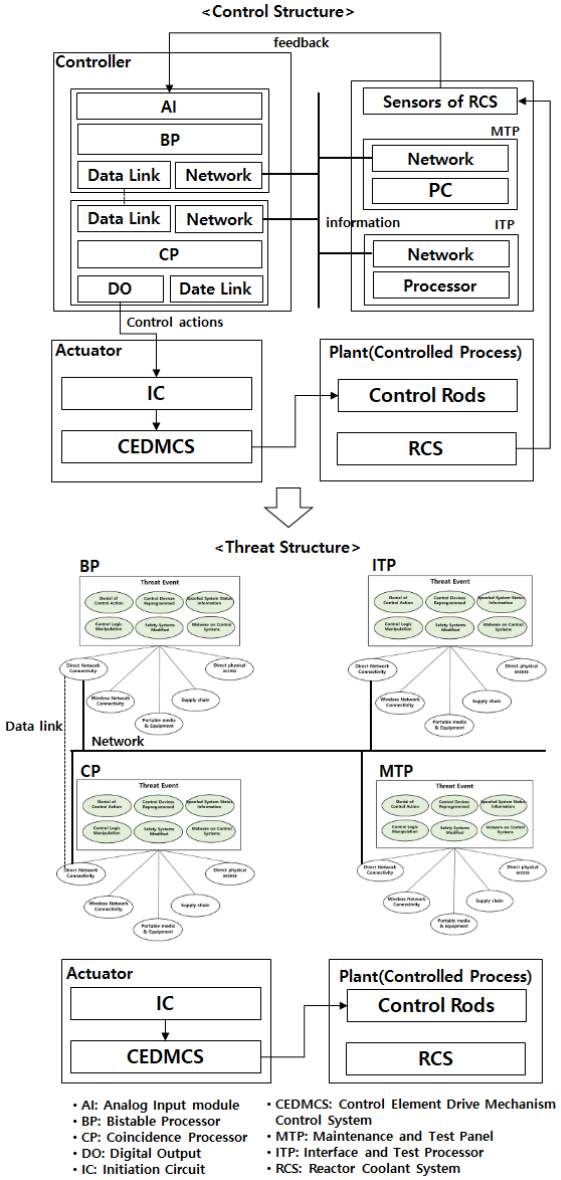

Fig. 5. Control and threat structure of RPS

In order to identify the UCAs of RPS, we consider the RT function by high pressure of the pressurizer, which is one function of SC 1 as described in Table III. The UCA of this control action is analyzed as Table IV.

Table IV: UCAs of RT function – High pressure of PZR

Control Action	RT for high pressure of pressurizer (PZR)		
Not providing causes hazard	Yes (H1, H2, H3, H4)	UCA 1-1	Pressure of PZR is beyond the set point, however failed to generate the RT signal
Providing causes hazard	No		N/A
Too late/Too soon/out of sequence	Yes (Too late) (H1, H2, H3, H4)	UCA 1-2	Pressure of PZR is beyond the set point, however RT signal is generated too late
		UCA 1-3	Pressure of PZR is below the setpoint, RT signal is generated
Stopped too soon/Applied too long	Yes (Stopped too soon) (H1, H2, H3, H4)	UCA 1-4	The generation of RT signal stopped too soon before the CEDMCS receives the RT signal

Based on Table IV, we identify the threat scenario for UCA 1-1 as shown in Table V.

Table V: Threat scenario for UCA 1-1

SC/UCA	Description
SC -1	Trip signal is generated when the pressure of PZR is beyond the setpoint
UCA 1-1	The pressure of PZR is beyond the setpoint, however the trip signal fails to be generated
Casual factors	Unsafe control action [1) in Fig.2]
Possible causes in cyber risk	Inadequate control logic (Threat logic) installation
Related CDAs	BP, CP
Threat events in CDA	Control device reprogrammed (in Fig. 3)
Attack vectors	Portable media & Equipment
Threat scenario 1-1-1	1) Access to BP/CP cabinet 2) Connection EWS to BP/CP 3) Installation inadequate control logic on BP/CP 4) Rotating the rotary switch on BP/CP to change mode

Fig. 6 shows the hierarchical structure among the SRs, UCSs, threat scenarios and threat structure. The threat events and attack vectors organizing each threat scenario 1-1-1 in Table V are as follows:

· Threat scenario 1-1-1: BP (Portable media & Equipment/Control device reprogrammed)

3. Conclusions

In order to assess the cyber risk in NPPs, we propose the CTIM, which constitutes the system-level and component-level CTIM. In the system-level CTIM, the

threat scenarios are identified based on the STPA. In the component-level CTIM, the threat events and attack vectors are identified, which organize the threat scenarios. For the links between the threat scenarios and the threat events, we propose the threat structure and threat identification model for the component (CDA). The proposed model is useful for identifying the threat scenarios of target system in NPPs.

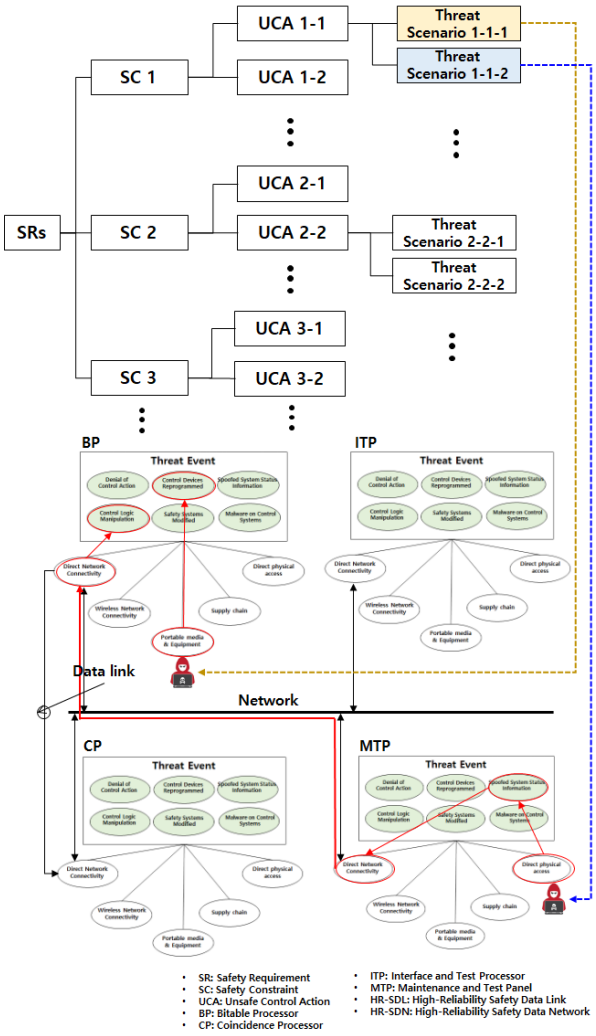

Fig. 6. Hierarchical structure among SRs, SCs UCAs and threat structure of RPS

REFERENCES

[1] U.S. Nuclear Regulatory Commission, Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, January 2010.
[2] Nancy G. Leveson, John P. Thomas, STPA Handbook, March 2018.
[3] Keith Stouffer, Victoria Pillitteri, Marshall Abrams, Adam Hahn, Guide to Industrial Control Systems (ICS) Security, NIST SP 800-82, Rev. 2, May 2015.
[4] NEI, Addressing Cyber Security Controls for Nuclear Power Reactors, NEI 10-09, Rev. 0, 2011.
[5] Dong-Hoon Kim, System Requirements for Reactor Protection System, NTIP-RPS-SR101, Rev.1, KAERI Design Report, 2015.