공학석사학위논문

Development of a System Dynamics Model for the Assessment of Nuclear Security Culture at a Nuclear Power Plant

원자력발전소 내 핵안보 문화 평가를 위한

시스템 다이내믹스 모델 개발

2016 년 8 월

서울대학교 대학원

에너지시스템공학부

이건희

Development of a System Dynamics Model for the Assessment of Nuclear Security Culture at a Nuclear Power Plant

지도 교수 황 일 순

이 논문을 공학석사 학위논문으로 제출함
2016 년 6 월

서울대학교 대학원
에너지시스템공학부
이 건 희

이건희의 공학석사 학위논문을 인준함
2016 년 7 월

위 원 장 심 형 진 (인)

부위원장 황 일 순 (인)

위 원 전 봉 근 (인)

Abstract

Development of a System Dynamics Model for the Assessment of Nuclear Security Culture at a Nuclear Power Plant

Keon Hee Lee

Department of Energy Systems Engineering

The Graduate School

Seoul National University

Nuclear security is one of pillars to build the sustainability of the peaceful use of nuclear energy. The Nuclear Security Summits have identified nuclear security culture as a crucial leverage to enhance organizational capacities in the nuclear security. Since 'nuclear security culture' was defined as one of the twelve fundamental principles of physical protection of nuclear material and nuclear facilities endorsed by the IAEA Board of Governors in 2001, there have been active research around world. The concept and indicators of the nuclear security culture are described by IAEA as its implementing guide under the Nuclear Security Series No. 7. They also published a draft of self-assessment method for nuclear security culture in organizations as a mechanism for identifying ways to strengthen the culture. Nevertheless, there are many obstacles to conceptualize and to assess the culture, because its intriguing, intertwined and dynamic characteristics are difficult to be understood thoroughly.

The safety culture, in general, has been studied for a relatively long period of time. Several assessment methodologies are developed using data collected from interviews, surveys, document review, behavior observation, etc. One of methods for dealing with data is System Dynamics (SD), as an approach to understanding the nonlinear behavior of complex systems over time. In the case of security culture, the majority of past studies have focused on information security culture and employed SD models to describe the system characteristics and their evolutions as well. From the survey of literature of methodologies for assessing the organizational culture, System Dynamics is expected to be suitable for assessing nuclear security culture taking into account its structural complexity and dynamic characteristics. Therefore, this thesis aims to developing a SD model for the assessment of nuclear security culture at a nuclear power plant and for making policy recommendations towards the enhancement of the culture.

A SD model is consisted of Casual Loop Diagram (CLD) and Stock Flow Diagram (SFD). A CLD is developed as a logic flow chart of the elements of nuclear security culture to show their interactions. From IAEA indicators suggested in Nuclear Security Series the twenty elements of the culture are drawn by considering their measurability in this thesis. Their inter-relationship is deduced with the descriptive knowledge regarding the real world phenomenon. The diagram shows several feedback loops including 'Policy level-Work environment', 'Workload-Stress' and 'Learning'. Based on the structure of the CLD, a SFD is developed to demonstrate the dynamic nature of the main elements in terms of stocks and flows processes.

To investigate the inter-relationships postulated in the developed SD model, two sets of survey questionnaires are developed, targeting the personnel at NPPs and their regulator. Each survey set is made of 39 and 6 questions which are designed to evaluate awareness of nuclear security culture and relevant infrastructure, respectively. The data sets are collected from 846 workers at NPPs and 10 experts in physical protection. Regression analysis are applied to verify their statistical significance as well as reliability and validity. As a result of statistical analysis, it turns out that two separate SD models can be built using responses from security-worker and non-security-worker as distinguished by the ratio of total security execution time to total working hours and better reflect the real world phenomenon. 0.2 is the most appropriate ratio for showing the differences. To simulate a base scenario, the assumption that security knowledge and periodic model behavior in one year do not carry forward to the next year is made. Under the assumption, the SFD is segregated into two models and simulated in the base scenario.

To ensure the reliability of the current (2015) survey data, the correlation equations used as inputs in the model are compared with the date of previous year (2014). Based on the 2014 and 2015 data, two relationships among ‘Security policy level of facility’, ‘Clear organization structure of facility’ and ‘Security rule and procedure’ are compared. To check the model reliability, an uncertainty caused by the input data uncertainties is evaluated using stochastic sampling method. Applying the latter method to the models by sampling with many different sets of input according to their distribution, the uncertainty with 500 samplings after 5 years for 95% confidence interval is estimated.

Based on the simulation result from the base scenario, sensitivity analysis is performed to determine the effect of each parameter on the culture. By changing input variables by 10% respectively, these effects are measured by percentage changes in the level of security consciousness and action. The magnitude of changes compared to the levels simulated in the base scenario is defined as their sensitivity. For both security-worker and non-security-worker, their consciousness and actions are very sensitive to the changes of 'Security education and training', 'Security education and training cycle' and 'Half-life of knowledge decay'.

Finally, policy recommendations are made in the thesis. Six strategies are suggested from the sensitivity study result: 1) Raising the policy level, 2) Expanding investment in education and training, 3) Shortening the cycle of education and training, 4) Raising the quality of education and training, 5) Raising the frequency of regulations, 6) Increasing allocation of security resource. By comparing their effectiveness, a strategy to prevent security knowledge from becoming forgotten is the most effective, especially for non-security-worker. For security-worker, a strategy to raise the policy level or the frequency of regulations is highly recommended.

This thesis emphasizes the assessment of nuclear security culture as an instrumental vehicle to improve security readiness at Korean nuclear power plant effectively. To capture the dynamic and complex characteristics of the culture, the approach involving SD model, large-scale surveys and sensitivity analysis is shown to be highly useful. Policy recommendations derived from the SD models for the enhancement of nuclear security culture are expected to be effective in improving

security consciousness and action. On this ground, the developed SD model is recommended as a quantitative analysis tool for reliable estimates of the cultural effects of relevant policy decisions in commercial nuclear facilities in Korean settings.

Keywords: Nuclear security culture, Assessment of organizational culture, System Dynamics, Survey, Sensitivity Analysis, Uncertainty, Decision making tool

Student Number: 2014-22722

Table of Contents

List of Figures

List of Tables

1. Introduction

Nuclear security is one of pillars to build the sustainability of the peaceful use of nuclear energy. After the September 11 attacks and Fukushima accident, the issues about the malicious acts by non-state actors and the vulnerability of nuclear facilities have surfaced. A number of countries using nuclear energy recognize that the nuclear security incidents must be carefully handled to pursue their own security. The Nuclear Security Summits (NSSs), which have become a platform to create initiatives for strengthening nuclear nonproliferation and nuclear security, reaffirm the responsibility of each country for performing the concrete measures of nuclear security. International cooperation, such as sharing their best practices, is also highlighted to build a robust nuclear security system. But the measures relevant to physical protection and national security strategy make them share the limited amount of information with each other. Instead, the attitudes and behavior of individuals, organizations and governments which consider nuclear security as a priority, can be internationally investigated as a crucial leverage to enhance organizational capacities in the nuclear security. This is the starting point of the discussion about nuclear security culture.

Since ‘nuclear security culture’ was defined as one of the twelve fundamental principles of physical protection of nuclear material and nuclear facilities endorsed by the IAEA Board of Governors in 2001, there have been active research around world. The concept and indicators of the culture are described by IAEA as its implementing guide under the Nuclear Security Series No. 7 as follows [2].

The assembly of characteristics, attitudes and behaviour of individuals, organizations and institutions which serves as a means to support and enhance nuclear security

IAEA also suggests that well-developed management systems and adequate behavior are important to support and enhance nuclear security as shown in Figure 1.1. They also published a draft of self-assessment method for nuclear security culture in organizations as a mechanism for identifying ways to strengthen the culture [3]. Nevertheless, there are many obstacles to conceptualize and to assess the culture, because its intriguing, intertwined and dynamic characteristics are difficult to be understood thoroughly.

The safety culture, in general, has been studied for a relatively long period of time. Several assessment methodologies are developed using data collected from interviews, surveys, document review, behavior observation, etc. IAEA develops the Independent Safety Culture Self-Assessment (ISCA) as a comprehensive analysis of six ways; Interviews, Surveys, Target group interview, Document review, Observation, Operational Safety Review Team (OSART) materials. Nuclear Energy Institute (NEI) and Korea Hydro & Nuclear Power Co. (KHNP) adopt safety culture principles from the Institute of Nuclear Power Operations (INPO) and the Edgar Schein 3-tier model respectively to assess nuclear safety culture. The results from these methodologies represent the certain snapshots of the culture based on the data collected at the time. Another method for dealing with data is System Dynamics (SD), as an approach to understanding the nonlinear behavior of complex systems over time. This method provide a quantitative analysis model to capture the dynamic nature of the systems and to revisit the decision on a periodic basis.

In the case of security culture, the majority of past studies have focused on information security culture and employed SD models to describe the system characteristics and their evolutions as well. From the survey of literature of methodologies for assessing the organizational culture, System Dynamics is expected to be suitable for assessing nuclear security culture taking into account its structural complexity and dynamic characteristics.

Therefore, this thesis aims to developing a SD model for the assessment of nuclear security culture at a nuclear power plant and for making policy recommendations towards the enhancement of the culture.

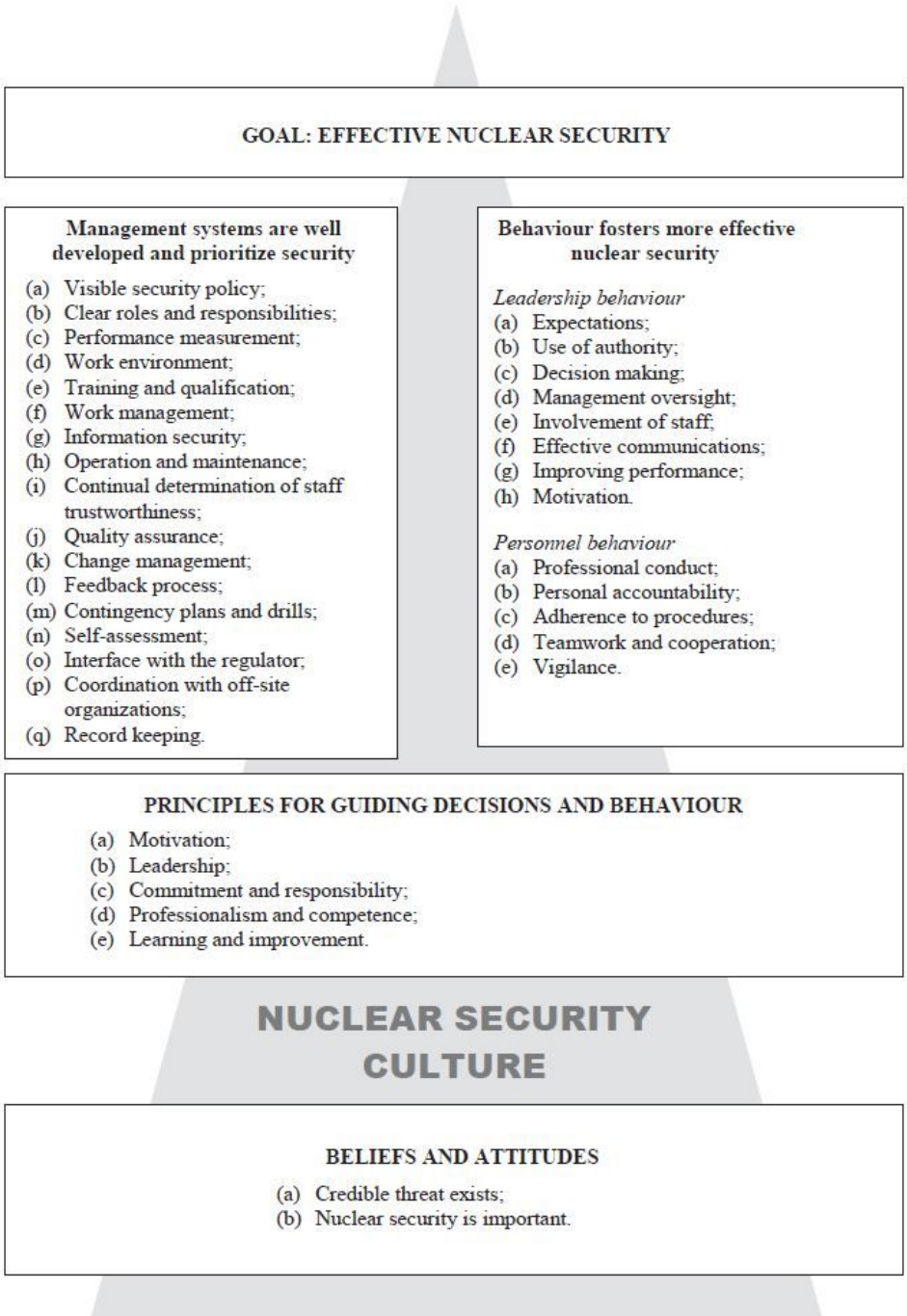


Figure 1.1 The characteristics of nuclear security culture [2]

2. Literature Review

2.1 Nuclear Security Culture

Nuclear security culture is recognized as a main contributing factor to nuclear security. There have been some accidents caused by a lack of the culture in nuclear facilities. For example, Pelindaba, which is the Nuclear Research Complex in South Africa, had a break-in on November 8, 2007. Four armed men disabled several layers of security on fences before cutting their way in, then attacked and shot a security officer. They seem to have had prior knowledge of the security measures.[1] In 2007, an anonymous person sent a letter to the NRC complaining of security guards sleeping at Peach Bottom NPP. After months of NRC inactivity, he videotaped the inattentive guards and sent the tape to a local TV station for media exposure.[2] In 2014, anti-nuclear activists launched a cyber-attack on KHNP, releasing employee information and technical documents, which were leaked from the emails of former/current employees and computers of subcontractors.[3]

To ensure the security of nuclear facilities such as NPPs, in-depth understanding of the culture is required. Under the threat of terrorism, many countries actively seek ways to develop the concept of the culture and its assessment methodology.

---

[1] "IAEA concludes lessons of Pelindaba break-in", World Nuclear News, 28 January, 2008.
[2] "Exelon Terminates Wackenhut Security Contract at Peach Bottom Nuclear Power Plant", NEI Nuclear Notes, 24 September, 2007.
[3] "Activists hack KHNP's computer systems", World Nuclear News, 22 December, 2014.

2.1.1 Concept of Nuclear Security Culture

Among the twelve fundamental principles of physical protection of nuclear material and nuclear facilities, the fundamental principle F proposes the importance of security culture and recommend its implementation and its maintenance in the concerned organizations as follows [1].

Security Culture: All organizations involved in implementing physical protection should give due priority to the security culture; to its development and maintenance necessary to ensure its effective implementation in the entire organization.

I. Khripunov et al (2004) suggest the concept of security culture to contribute to the effective protection of nuclear material by managing the three distinct but interacting sets of inputs: Principles and Values, External Factors, and the Security Culture Mechanism [4]. Based on the concept, the model of the culture is developed as shown in Figure 2.1. M. Brière and D. Winter (2005) present three general components of nuclear security culture: Policy at the State Level, Framework within Organizations, Attitudes of Managers and Individuals [5]. They also make some comments on each components. The comments at the state level covers the definition and evaluation of the threat and the distribution of the responsibilities. For organizations, the comments about commitments, management structures, resources and vigilance are made. The comments on individuals particularly are divided into two types depending on whether individuals are directly implied in security or not.

IAEA (2008) published the implementing guide containing the definition of the

culture and their characteristics [2]. The beliefs and attitudes, which are the basis of the culture, are derived from recognizing the existence of threat and its importance. The characteristics of management systems and behavior are described as follows.

· *The characteristics of Management Systems*

Visible security policy; Clear roles and responsibilities; Work environment; Performance measurement; Training and qualification; Work management; Information security; Operations and maintenance; Contingency plans and drills; Quality assurance; Feedback process; Determination of staff trustworthiness; Change management; Self-assessment; Coordination with off-site organizations; Interface with the regulator.

· *The characteristics of Behavior*

- *Leadership Behavior: Expectations; Use of authority; Decision making; Management oversight; Involvement of staff; Effective communications; Improving performance.*
- *Personnel Behavior: Professional conduct; Personal accountability; Adherence to procedures; Teamwork and cooperation; Vigilance.*

2.1.2 Assessment of Nuclear Security Culture

As a part of the culture itself, a study to assess nuclear security culture has begun based on the preceding concepts and characteristics. This assessment process is emphasized as an effective strategy to improve the culture and alert the concerned organization and individuals to the credible threat. Especially, security

incidents are infrequent as compared with safety ones. This feature can cause the negligence issues. In this context, the assessment of nuclear security culture is important as much as the culture itself.

IAEA (2014) published a draft of self-assessment method for nuclear security culture in organizations as a mechanism for identifying ways to strengthen the culture [3]. They suggest the six stage process of self-assessment of the culture as shown in Figure 2.2. The process starts with establishing a self-assessment team. The team collects the data from survey, interview, document review, and observation and consolidate the result. Next, the color-code scheme is applied as the three-tiered outcome model on the average score. Red is a sign of weakness when the score is under the median and yellow is ground for concern. Green is a sign of strength that should be preserved. After assigning the color-code, the result is discussed to submit the final report containing a follow-up action plan. The whole scheme of data processing is shown in Figure 2.3.

H. Yoo and J. Lee (2015) evaluate the awareness of the culture of personnel at nuclear facilities by conducting a survey [6]. The survey is made up of questions asking their beliefs and attitude, operating systems, leadership behaviors and staff behaviors. The result shows that the scores increase as the service period lengthens and the personnel gets older until their 50s. The differences between managers and staffs are significant. Generally, managers better recognize the importance of the culture than staffs.

These assessments show the static level of the culture at a certain time. However, the items which are considered in the process have interaction and even causality among themselves. The method to capture the dynamic nature of the culture is necessary to investigate its characteristics more specifically and assess it in terms of medium and long term.

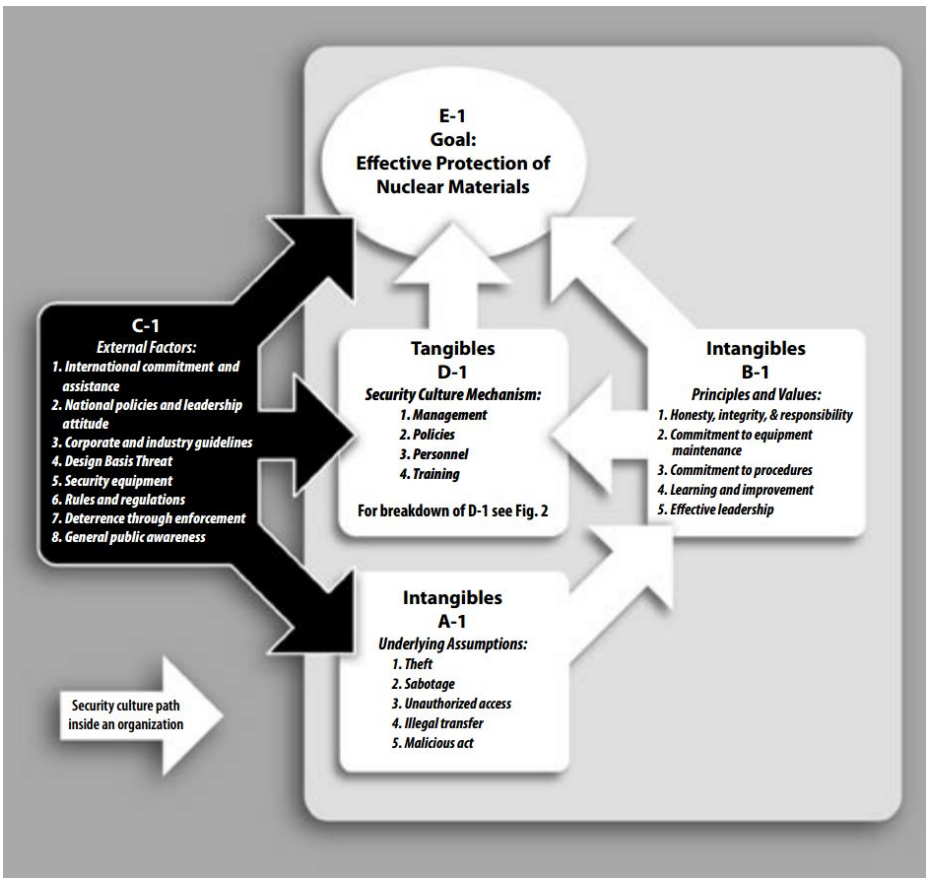


Figure 2.1 Model of nuclear security culture [4]

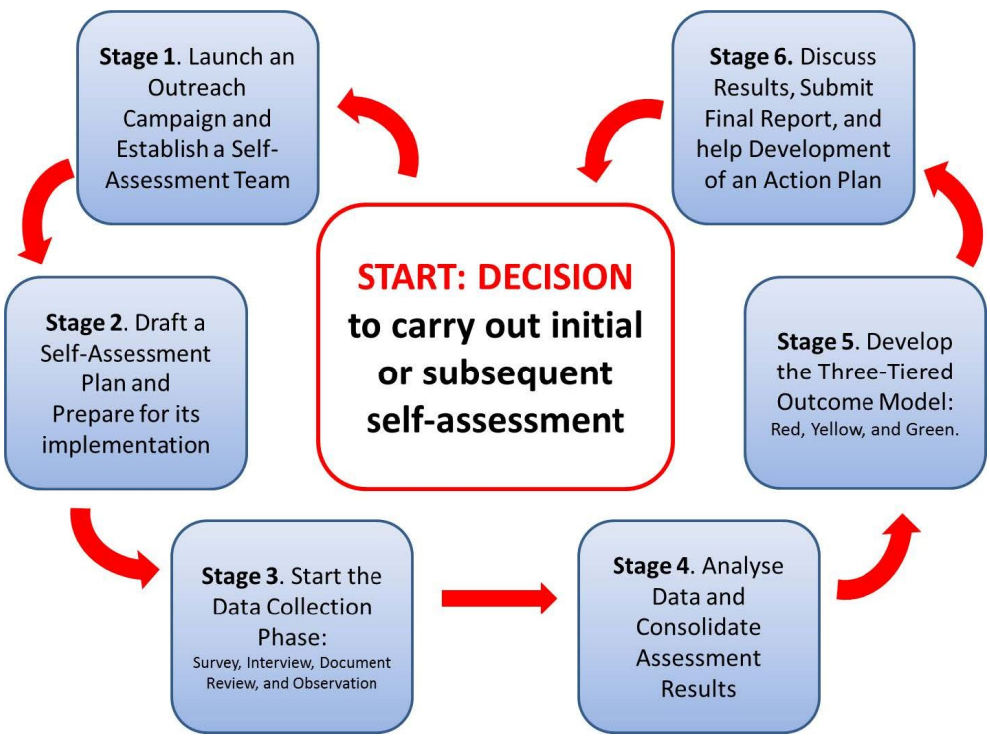


Figure 2.2 Six stage process of self-assessment of nuclear security culture [3]

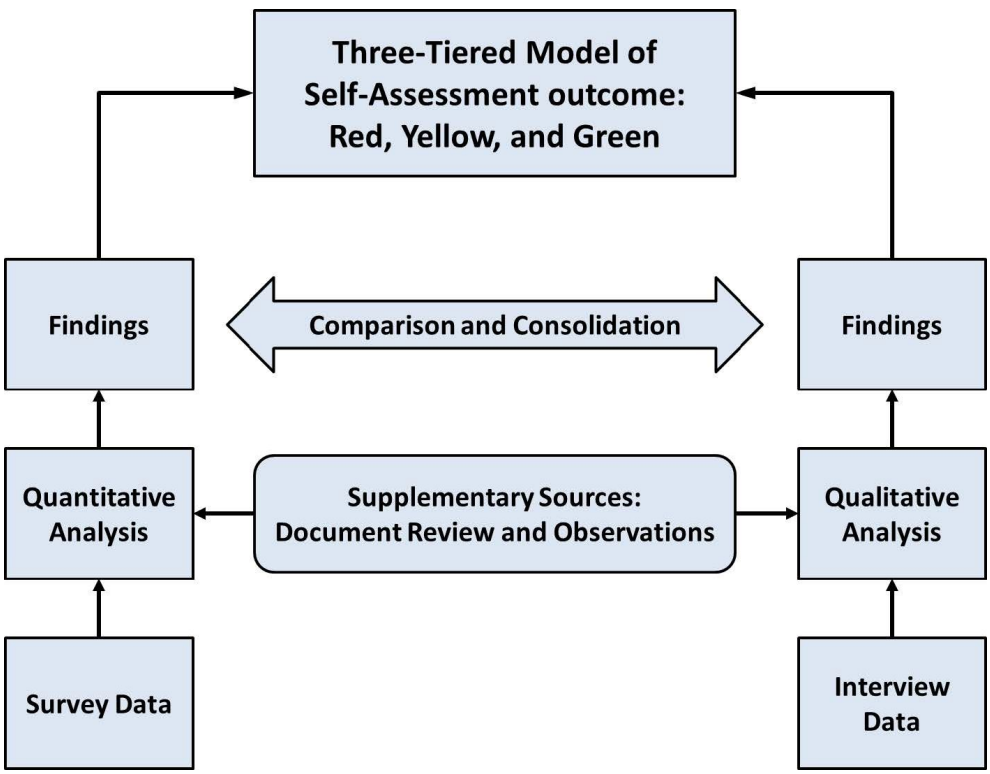


Figure 2.3 Use of quantitative and qualitative data for finding analysis [3]

2.2 System Dynamics

System Dynamics is an approach to understanding the complex feedbacks and nonlinear behaviors of natural and social systems over time. This method is derived from 'Individual Dynamics' of Prof. J.W. Forrester in MIT. Unlike the existing methods taking a single approach to the system to analyze only cause and effect, System Dynamics takes a comprehensive approach at the level of the entire system by analyzing the relationship between the sub-elements of the system.

A SD model is consisted of Casual Loop Diagram (CLD) and Stock Flow Diagram (SFD) [7]. A CLD is a logic flow chart of the elements of nuclear security culture to show their interactions. A SFD demonstrates the dynamic nature of the main elements in terms of stocks and flows processes. The example of the diagrams is shown in Figure 2.4. As shown in the CLD, the population increases with birth and decreases with death. This relation determines the causal link with a polarity, either positive (+) or negative (-). A positive link means that the dependent variable increases when the independent variable increases. Whereas, a negative link indicates that the dependent variable decreases when the independent variable increases. After assigning the polarity of the links, the characteristics of the loops made up with the links are determined. The left loop including the population and birth, which are connected with only positive links, is called reinforcing loop. The right loop including the population and death, which are connected with one positive link and one negative link, is called balancing loop. The reinforcing loop and the balancing loop cause the divergence and the convergence of the values respectively. In the SFD, the population is considered as stock and indicates the level of the residue, which is determined by the difference between inflow and

outflow. Inflow of the population is birth and influenced by birth rate. Outflow of the population is death and influenced by average lifetime. Based on these flows, it is possible to demonstrate the change in the stocks as time goes on. Furthermore, it helps effective decision-making by capturing the dynamic and fluid nature of the system, not just certain snapshot. There are several software to develop the SD model such as Vensim, ithink, and PowerSim.

This method is already applied in nuclear industry. The field of the study on nuclear safety culture particularly employs the model to assess the safety of non-technical factors such as organization/human factors at NPPs. The model is also used as a tool for comprehensive dosimetry, risk management on sabotage, and nuclear power technology valuation.

There are two main streams of the past studies, which use the SD model to investigate and assess the culture; Safety Culture and Information Security Culture.

2.2.1 Case Study: Safety Culture

The safety culture, in general, has been studied for a relatively long period of time and widely applied in many different field. As the preceding research using the SD model to investigate the culture, Leveson, N. G. et al (2005) simulate the level of concern and the fraction of corrective action to fix systemic problems based on general form of the model of socio-technical control [8]. They focus on the interaction between system development and system operation. Marais, K. and Leveson, N. G. (2006) represent two basic characteristics of the most common risk dynamics; Challenges of maintaining safety, Side effects and symptomatic responses [9]. As the challenges of maintaining safety, stagnant safety practices in

the face of technological advances, decreasing safety consciousness, eroding safety goals and complacency are suggested. They also bring up a problem about the side effects and symptomatic responses such as unintended side-effects of safety fixes, fixed symptoms rather than root causes and the vicious cycle of bureaucracy.

Lyneis, J. & Madnick, S. (2008) develop the SD model on the safety culture as shown in Figure 2.5 [10]. They focus on self-preservation, management safety actions, high priority of safety and organizational learning. The simulation result in Figure 2.6 shows that organizational learning provides a substantial incremental benefit only when safety priority is high. Accordingly, they suggest that giving safety a high priority is the most effective policy.

The recent studies on nuclear safety culture also employ the SD model [11, 12]. They consider the culture as a critical factor of NPPs and think that the robustness of NPPs can be damaged because of the low level of the culture. The CLD on the culture is developed based on the mechanism of major incidents. They emphasize the major feedback loops including organizational learning and the coordination of work schedules with social supports, incentives. Unlike the security incidents, not a few of the safety incidents are occurred. This feature makes corrective actions play an important role in organizational learning. They also simulate the SFD derived from the CLD with several scenarios to estimate the effect of each applicable policy and their combination.

2.2.2 Case Study: Information Security Culture

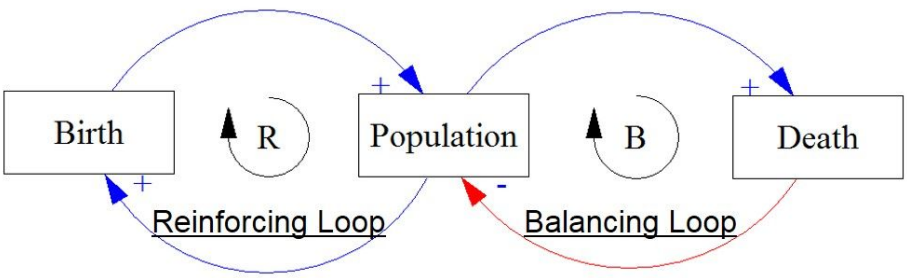
Many studies on the security culture are focused on information security culture. Especially, the information security is emphasized in IT organizations. Security

controls to secure an information system can be classified into three types of controls: Technical, Formal, and Informal Controls [13].

There two main streams of the studies using the SD model to investigate information security culture; Insider Threat and Information Security Management. In the research field of Insider Threat, C. Melara et al (2003) develop the SFD mainly focusing on technical and formal controls [14]. The structure of the model, which is derived from the Tim Lloyd/Omega Case, includes the effect of insider incidents on system downtime, the effect of insider actions on workplace discontent and security level reduction. Farhad Foroughi (2008) suggests the CLD and the SFD on insider-attack with 18 variables in 4 categories [15]. The categories are Detection Procedures, Motive Triggers, Focal Actor in Possibility of Attack and Preventative Polices. Sang-Chin Yang and Yi-Lu Wang (2011) review the historical background of insider threat analysis and their attributes and develop the SD model embracing Technology/Process/People [16]. The structure of the model is derived from the Taiwan's biggest corporate theft case.

In the research field of Information Security Management, J. M. Sarriegi et al (2008) establish the structure of security management subsystem and their combined model [17]. They simulate the technical, formal, and informal implemented security controls based on security effectiveness and overall desired security. Derek L. Nazareth and Jae Choi (2015) compare the effectiveness between security tools investment and deterrence investment using the SD model. The model is developed as shown in Figure 2.7. The simulation result in Figure 2.8 shows that security tools investment have greater effect on overall security cost than deterrence investment.

✓ **Casual Loop Diagram (CLD)**



✓ **Stock Flow Diagram (SFD)**

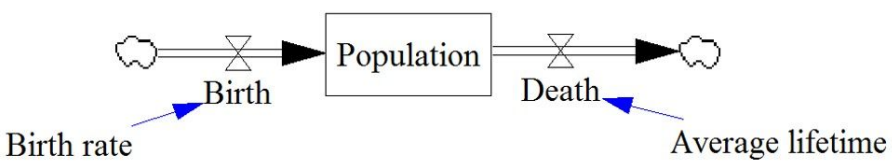


Figure 2.4 Example of CLD and SFD

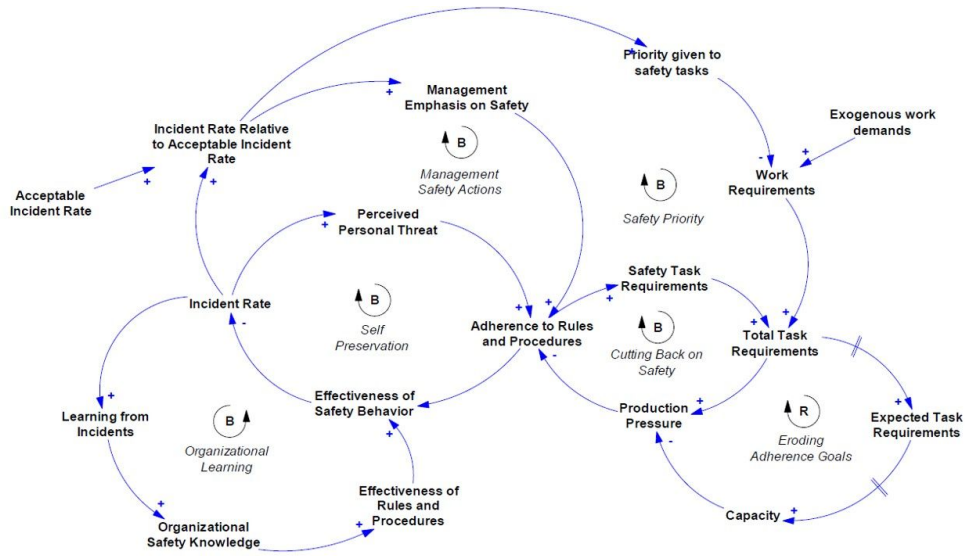


Figure 2.5 SD model on Safety Culture [10]

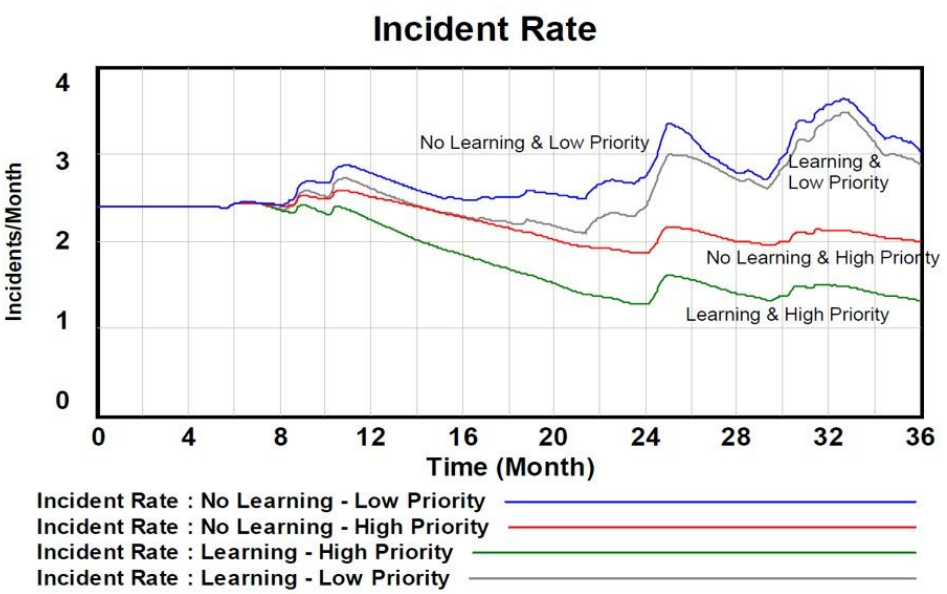


Figure 2.6 Simulation result from SD model on Safety Culture [10]

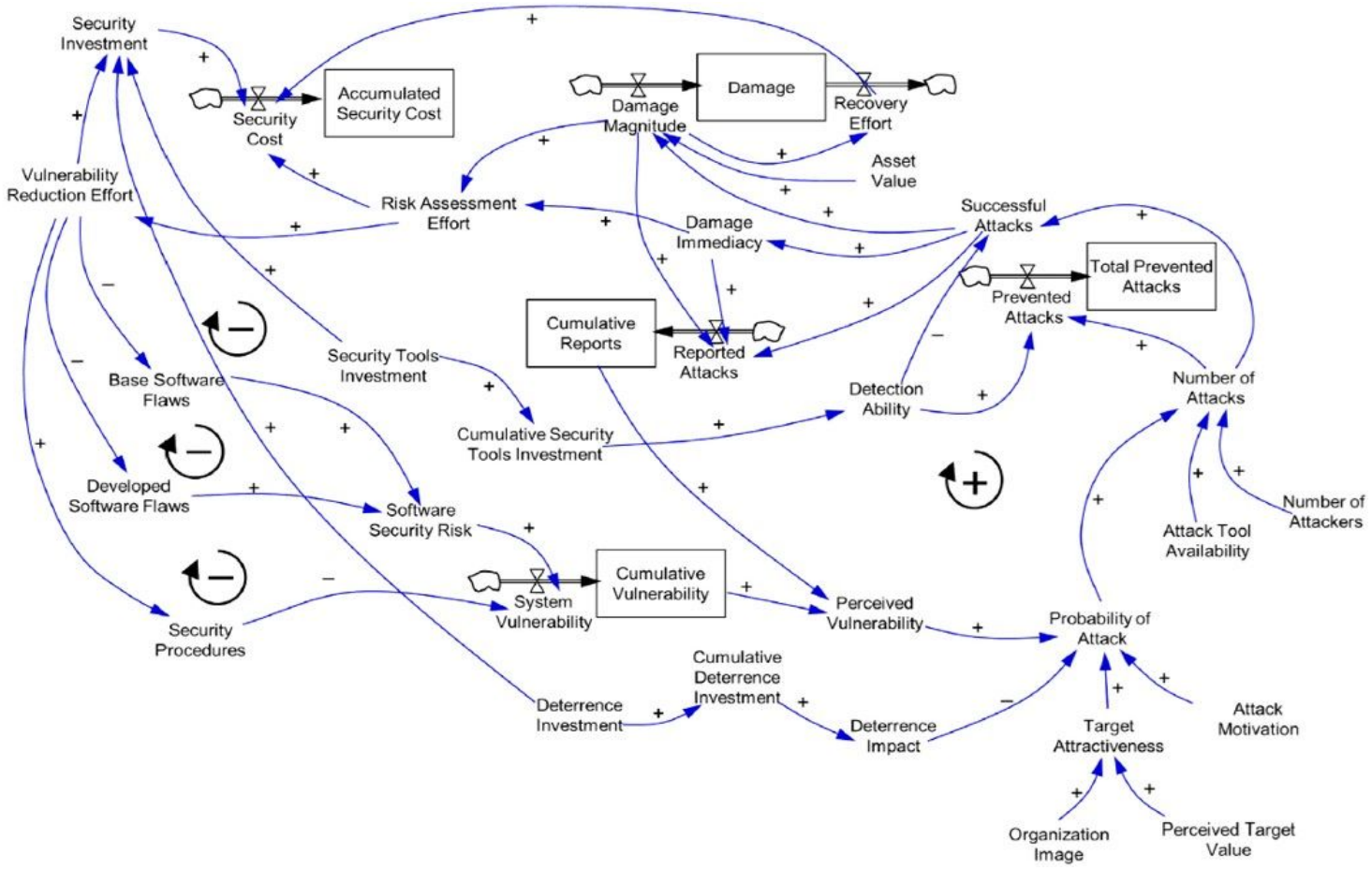


Figure 2.7 SD model on Information Security Management [18]

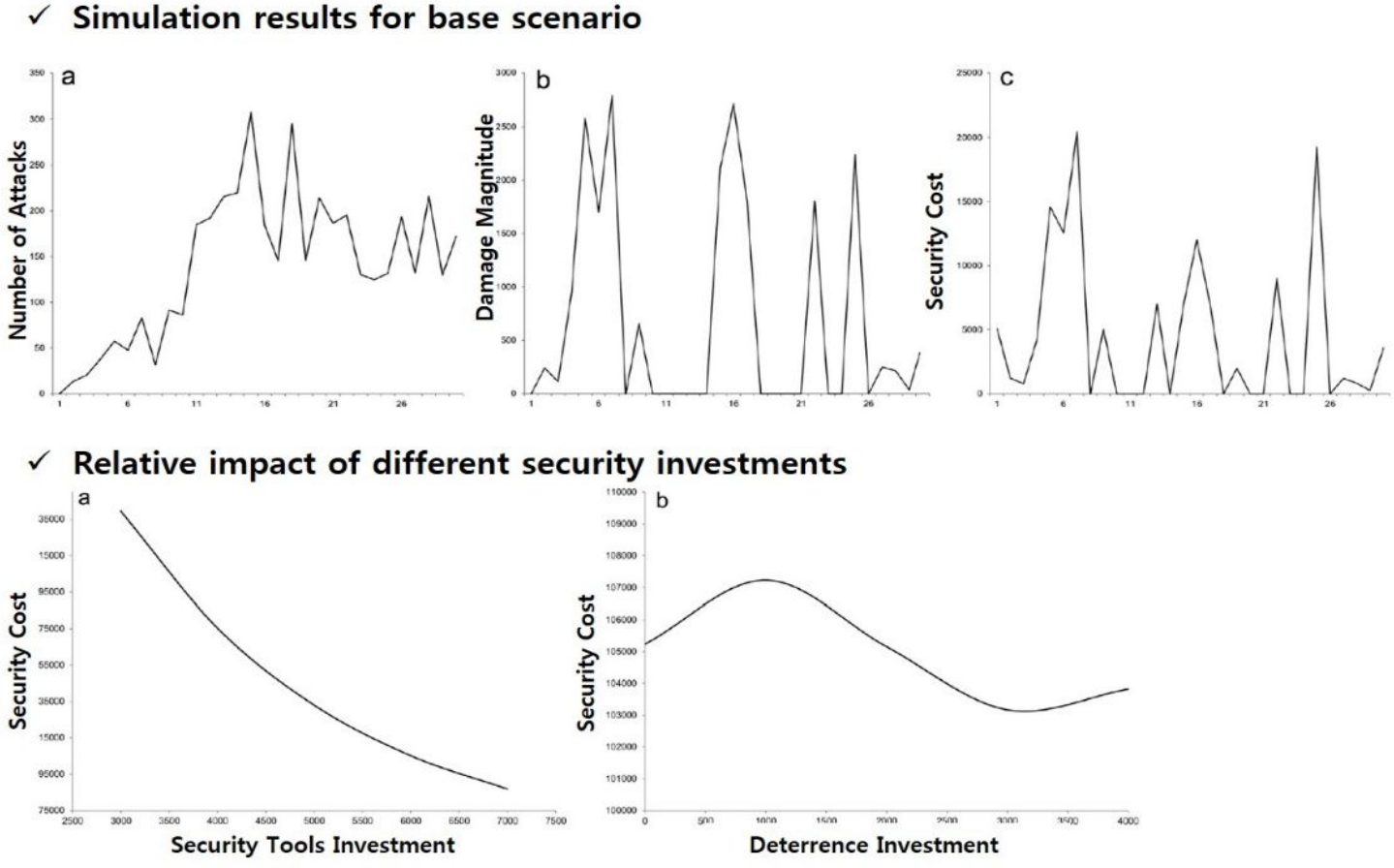


Figure 2.8 Simulation result from SD model on Information Security Management [18]

3. Rationale and Approach

3.1 Goals and Rationale

The goal of this thesis is to develop a SD model for the assessment of nuclear security culture at a nuclear power plant. The personnel at NPPs are considered as the primary target group for the establishment of the culture. By assessing the level of the culture based on their awareness and relevant infrastructure within NPPs, the concerned organization and individuals can feed the necessity of improving the culture. During the modeling process, the deep, shared and dynamic characteristics can be understood and help to improve the acceptance and cultural basis for nuclear security in domestic related organizations and corporations.

The research questions are as follows.

- How can we evaluate dynamics and soft attributes of nuclear security culture?
- How can we define the elements for constructing the model?
- How can we investigate the inter-relationships postulated in the model?
- What strategies are effective to enhance nuclear security culture?

As an appropriate assessment methodology, System Dynamics is applied. Before developing the CLD and the SFD on the culture, the constituent elements of the model are drawn from IAEA indicators suggested in Nuclear Security Series. These elements need to embrace the unique characteristics of the culture such as

qualitative, internal and comprehensive nature. To perform a quantitative analysis of the interaction between the elements derived, the SD model is developed in comparison with the SD model on the nuclear safety culture. A survey on the personnel at NPPs and their regulator is conducted to determine the input values which reflect the current level of each element. By performing the simulations for the base scenario and alternative improvement scenarios using the developed SD model, the policy recommendations towards the enhancement of the culture are made.

This aims to provide a quantitative analysis tool for reliable estimates of the cultural effects of relevant policy decisions as the basis for a significant stepping up of the study on nuclear security culture.

3.2 Approach

The overall approach of this research is shown in Figure 3.1. There are three steps; Development of a SD Model, Data Collection and Model Tuning, Model Application. As the first step, the elements of the culture are drawn from IAEA indicators suggested in Nuclear Security Series by considering their measurability. The CLD is developed by deducing their inter-relationship with the descriptive knowledge regarding the real world phenomenon. The SFD is derived from the CLD by assigning the stock variables and subdividing the major elements.

To investigate the inter-relationships postulated in the developed SD model, Data Collection and Model Tuning is performed. Two sets of survey questionnaires are developed, targeting the personnel at NPPs and their regulator. By analyzing the survey results statistically, the input values are determined. The SFD is

segregated into two models depending on whether their work includes security task. To ensure the reliability of the current (2015) survey data, the correlation equations used as inputs in the model are compared with the date of previous year (2014). To check the model reliability, an uncertainty caused by the input data uncertainties is evaluated using stochastic sampling method.

As the final step, Model Application is performed. Under the assumption that security knowledge and periodic model behavior in one year do not carry forward to the next year, the base scenario is simulated with two separate SD model. Based on the simulation result from the base scenario, sensitivity analysis is conducted to determine the effect of each parameter on the culture. By changing input variables by 10% respectively, these effects are measured by percentage changes in the level of security consciousness and action. The magnitude of changes compared to the levels simulated in the base scenario is defined as their sensitivity.

To make policy recommendations towards the enhancement of the culture, several improvement scenarios are developed and their effectiveness is compared. Furthermore, the developed SD model can help the relevant decision-makers to easily predict the effect of each policy before implementing them and improve the culture more effectively.

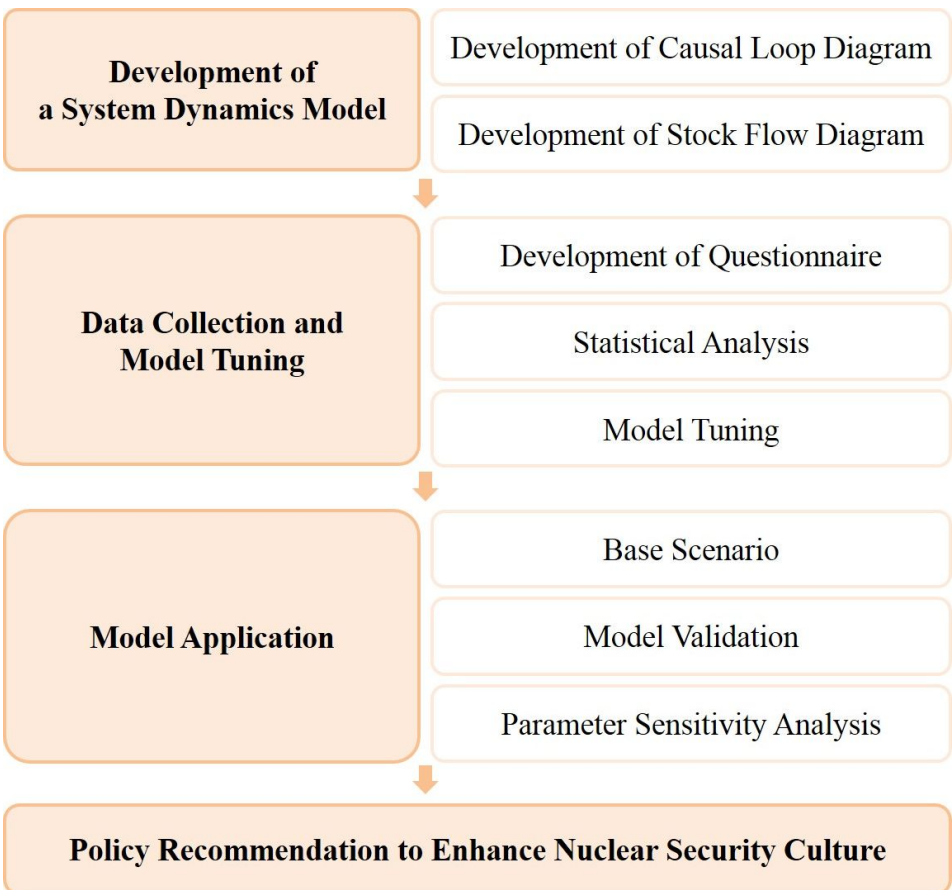


Figure 3.1 Overall Approach of Research

4. SD Model on Nuclear Security Culture

4.1 Development of Causal Loop Diagram

A SD model is consisted of two diagrams; Casual Loop Diagram (CLD) and Stock Flow Diagram (SFD). To develop the CLD, the elements of nuclear security culture should be defined and designed to enable their quantification by conducting the survey on personnel at NPPs. By determining the polarity of their correlation between the elements, a logic flow chart is constructed to show their interactions conceptually.

4.1.1 Element of Causal Loop Diagram

The attributes of nuclear security culture are directly connected to define the elements of the CLD. As mentioned in Chapter 2, its attributes are investigated by several studies to develop the concept of the culture more clearly. One of the studies is IAEA Nuclear Security Series No. 7. They suggest the characteristics of the culture as IAEA Security Culture Indicators.

4.1.1.1 IAEA Security Culture Indicators

IAEA Security Culture Indicators (hereafter IAEA Indicators) are divided into two types: Management systems and Behavior. They consider well-developed

management systems and individual behaviors as requirements for effective nuclear security in terms of cultural matters. The characteristics of management systems and behavior are defined with 16 indicators and 2 indicators respectively. They can be categorized as shown in Table 4.1.

'External factors' include Coordination with off-site organizations and Interface with the regulator. 'Facility policy' is linked to Visible security policy. 'Rules and procedure' embrace Clear roles and responsibilities, Operations and maintenance, Change management, Quality assurance, Determination of staff trustworthiness, Feedback process and Information Security. 'Education and training' is connected to Training and qualifications, Contingency plans and drills. 'Work environment' and 'Work management' are used as a category name and contain themselves. 'Outcomes' include Performance measurement and Self-assessment. Leadership Behavior and Personnel Behavior are categorized as 'Consciousness and action'. This categorization can be used to construct the simple structure of the CLD afterwards.

4.1.1.2 Element Selection

The twenty elements of the CLD are drawn from the detailed contents of the IAEA indicators by considering whether their values can be quantified or not. Based on their measurability, the elements are selected as shown in Table 4.2.

'Security policy level of government' is added as external factor, corresponding to the policy level of facility. 'Coordination with off-site organization' and 'Interface with the regulator' are used as suggested in IAEA indicators. 'Security policy level of facility' is drawn from Visible security policy and determines the overall level of the elements in the facility. 'Clear organization structure of facility'

is considered as the measurable element of Clear roles and responsibilities. ‘Security rule and procedure’ is drawn to embrace the detailed contents from several IAEA indicator. ‘Security workload’ is uncertain depending on their occupational group, but the contents of Information Security are included in common. ‘Total security execution time per personnel’, ‘Schedule pressure’ and ‘Stress’ are considered as the measurable element of Work management. ‘Security resource’ is added to connect Work environment with Security policy level of facility. ‘Human resource of security work’ and ‘Quality and quantity of security equipment’ are drawn from Work environment. ‘Security education and training’ is selected to combine the contents of Training and qualifications and Contingency plans and drills. ‘Security knowledge’ is added under the assumption of its quantification and determines the level of security consciousness. ‘Security consciousness’ is drawn from Leadership Behavior and Personnel Behavior. Some other contents of these Behavior indicators are included in ‘Security action’, which shows the level of individual performance and implementation. ‘Perception of necessity of security outcome enhancement’ is added to make a feedback loop to the policy level of facility. ‘Security outcomes’ is selected as the visible result of Performance measurements and has influence on the perception of security outcome enhancement. ‘Security accident rate and risk’ is drawn from the contents of Self-assessment, such as threat evaluation, assessment of security incidents rate and corrective action program.

According to this linkages between the elements and IAEA indicators, the definitions of the elements are also drawn from the contents of the indicators. The definitions are summarized as shown in Table 4.3. These elements are designed to enable their quantification by conducting the survey on personnel at NPPs.

4.1.2 Structure of Causal Loop Diagram

Based on these elements, the CLD is constructed to show their interactions, which are causal relations rather than simple correlations, with the descriptive knowledge regarding the real world phenomenon.

To construct the first level of the CLD, the categories of IAEA indicators is used: External factors, Facility policy, Rules and procedure, Education and training, Work environment, Work management, Outcomes, Consciousness and action. 'External factors' is to include the factors which affects the policy level of facility from outside. 'Facility policy', which is influenced with External factors, determines the level of 'Education and training', 'Rules and procedure', 'Work environment'. First, 'Education and training' plays a role in accumulating security knowledge against their natural decay or oblivion. 'Rules and procedure' determines the workload, which lengthens the security execution time. In contrast, 'Work environment' including human resource and equipment shortens the security execution time. The level of 'Consciousness and action' is determined by their knowledge and also interrupted with stress due to overtime. This level can be measured as 'Outcomes', which can be the motive of making efforts to improve it. This simple CLD is shown in Figure 4.1.

The second level of the CLD, as shown in Figure 4.2, has several feedback structures including 'Policy level-Work environment', 'Workload-Stress' and 'Learning'. 'Policy level-Work environment' emphasizes the security policy level of facility which directly affects overall resource, human resource and equipment for security tasks. 'Workload-Stress' addresses that the stress caused by additional security workload can hinder their security actions. 'Learning' is an important reinforcing loop for improving the culture in organizations. External segment of the

model includes the policy level of government, coordination with off-site organization and interface with regulators. The main feedback loops of the culture are presented in 'Workload-Stress' and 'Learning' with two reinforcing loops and two balancing loops (R1, R2, B1, B2). More detailed explanations are made in next section; Comparison with the Model on Safety Culture.

Figure 4.3 shows the linkage between the CLD and IAEA indicators (in red). The indicators which can be connected to each element of the CLD are placed at the bottom of them. Because nuclear security culture is an assembly of characteristics, attitudes, and behavior of organization and individual with the intention of supporting and improving nuclear security, the culture within facilities can be assessed indirectly with the level of security consciousness, security action, and security rules and procedures.

4.1.3 Comparison with the Model on Safety Culture

To ensure the robustness of the model, the second level of the CLD is compared to the model on safety culture. The referenced model is the SD model suggested in two of the literature review on nuclear safety culture. [11, 12]

4.1.3.1 Workload-Stress

Figure 4.4 shows the 'Workload-Stress' section of the each CLD in safety culture and security culture. To understand the impact of workload on stress in security culture, the prior studies on safety culture is compared as reference.

In safety culture, total task requirements increase when safety requirements

increases. The increased total task requirements make individuals get more time pressure. The increased requirements also raise the level of physical and mental stress. The increased stress causes the high accident rate.

In security culture, two loops (B1, R1) are relevant to workload and stress. The link from 'Total security execution time per personnel' to 'Security policy level of facility' is included in two loops in common. When the execution time increases, schedule pressure increases. This relation is equivalent to the relation of total task requirements and time pressure in the model on safety culture. The increased schedule pressure raises the level of stress, which is equivalent to the relation of total task requirements and stress in safety culture. When stress increases, security action decreases and when security action decreases, security accident rate and risk increases. This is the same as the high accident rate with the increased stress in safety culture. As security accident rate and risk increases, security outcomes are reduced. The reduced security outcomes raise the perception of necessity of security outcome enhancement. When this perception is raised in facilities, security policy level of the facility is also raised. In the model on security culture, the link from 'Security action' to 'Perception of necessity of security outcome enhancement' is subdivided by using the elements drawn from the detailed contents of Performance measurement.

In balancing loop (B1), as 'Security policy level of facility' increases, the resources assigned to nuclear security in facilities increase. When 'Security resource' increases, 'Human resource of security work' and 'Quality and quantity of security equipment' increases. However, this increment in overall resources and work resources including human resource and equipment is supposed to have temporal delays because it does not immediately increase. The increased human resource and equipment make the execution time shorten.

In reinforcing loops (R1), as ‘Security policy level of facility’ increases, the level of ‘Clear organization structure of facility’ increases. The increased clarity make the amount of ‘Security rule and procedure’ and ‘Security workload’ increase in order. The increased workload lengthens the execution time.

Focusing on balancing loop (B1) and reinforcing loop (R1) of the CLD on security culture, the causal relations between the elements relevant to workload and stress are confirmed by comparing with the model on safety culture.

4.1.3.2 Learning

Figure 4.5 shows the ‘Learning’ section of the each CLD in safety culture and security culture. Likewise, to understand the impact of learning in security culture, the prior studies on safety culture is compared as reference.

In safety culture, when learning increases, safety awareness of employees increases. The increased safety awareness raises the level of safety culture. The improved safety culture makes safety behavior increase. The increased safety behavior reduces nuclear accident and leads to balancing loop. The improved safety culture also increases the need for learning and leads to reinforcing loop by increasing learning.

In security culture, two loops (B2, R2) are relevant to learning. Unlike the model on safety culture which has safety culture as a clearly indicated element, the model on security culture has the subdivided elements of the culture such as security consciousness and security action.

In reinforcing loop (R2), when ‘Security policy level of facility’ increases, the resources allocated to nuclear security increase. The increased resources make more investments in ‘Security education and training’ with the temporal delay. This

investments raise the level of education and training and the level of security knowledge in order. This increased knowledge makes ‘Security consciousness’ increase. When ‘Security policy level of facility’ increases, ‘Leader’s Security consciousness’ increases directly. This loop has similar feedback structure with the reinforcing loop of the model on safety culture.

In balancing loop (B2), when ‘Security consciousness’ increases, ‘Security action’ increases. The increased security actions make ‘Security accident rate and risk’ reduces. When the accident rate and the risk reduces, ‘Security outcomes’ increases and ‘Perception of necessity of security outcome enhancement’ decreases in order. The decreased perception makes security policy level of the facility decrease and leads to balancing loop.

The element of ‘need for learning’ in the model on safety culture is presented in the increment of the investments in education and training in R2 and the decrement of the perception of outcome enhancement due to the increased security action in B2. In the case of the element of ‘incentives’, it is mentioned in safety culture, but not in security culture.

Table 4.1 Categorization of IAEA indicator

Category	IAEA Indicator (NSS No.7)
External factors	Coordination with off-site organization, Interface with the regulator
Facility policy	Visible security policy
Rule and procedures	Clear roles and responsibilities, Operations and maintenance, Change management, Quality assurance, Determination of staff trustworthiness, Feedback process, Information Security.
Education and training	Training and qualifications, Contingency plans and drills
Work environment	Work environment
Work management	Work management
Consciousness and action	Leadership behavior, Personal behavior
Outcomes	Performance measurements, Self-assessment

Table 4.2 Linkage between the element and IAEA indicator

Element	IAEA Indicator (NSS No.7)
Security policy level of government	
Coordination with off-site organizations	Coordination with off-site organization
Interface with regulators	Interface with the regulator
Security policy level of facility	Visible security policy
Clear organization structure of facility	Clear roles and responsibilities
Security rule and procedure	Operations and maintenance Change management Quality assurance Determination of staff trustworthiness Feedback process
Security workload	Information Security
Total security execution time per personnel	Work management
Schedule pressure	
Stress	
Security resource	
Human resource of security work	Work environment
Quality and quantity of security equipment	
Security education and training	Training and qualifications

	Contingency plans and drills
Security knowledge	
Security consciousness	Leadership behavior
	Personal behavior
Security action	Leadership behavior
	Personal behavior
Perception of necessity of security outcome enhancement	
Security outcomes	Performance measurements
Security accident rate and risk	Self-assessment

Table 4.3 Definition of the element

Element	Definition
Security policy level of government	Implementation level of international norms and national institutionalization
Coordination with off-site organizations	Understanding of emergency response organization, Collaboration between national and regional organizations
Interface with regulators	Feedback and exchange of information on nuclear security with regulatory agencies
Security policy level of facility	Prior considerations of nuclear security, Existence and implementation of nuclear security policy document
Clear organization structure of facility	Documenting and understanding of the roles and responsibilities of nuclear security for all employees
Security rule and procedure	Maintaining the level of nuclear security with appropriate provisions· procedures related security work
Security workload	The relative amount of security work, which includes both quantity and difficulty
Total security execution time per personnel	Total time to execute security work per day
Schedule pressure	Schedule pressure due to security work
Stress	Burden on security work
Security resource	Financial investment in security
Human resource of security work	Manpower of security work compared to the level required

Quality and quantity of security equipment	Quality and quantity of security equipment compared to the required level
Security education and training	Implementation of security education and training
Security knowledge	Extent of knowledge determined by increment from security education and training and decrement from oblivion
Security consciousness	Commitment and motivation for security-related communications Awareness and compliance with security rules and procedures
Security action	Goal Management and supervision on security Ensuring professionalism and maintaining vigilance during work
Perception of necessity of security outcome enhancement	The need for efforts to promote security outcome
Security outcomes	Achievement of security performance
Security accident rate and risk	Rate and risk of security accident at facility

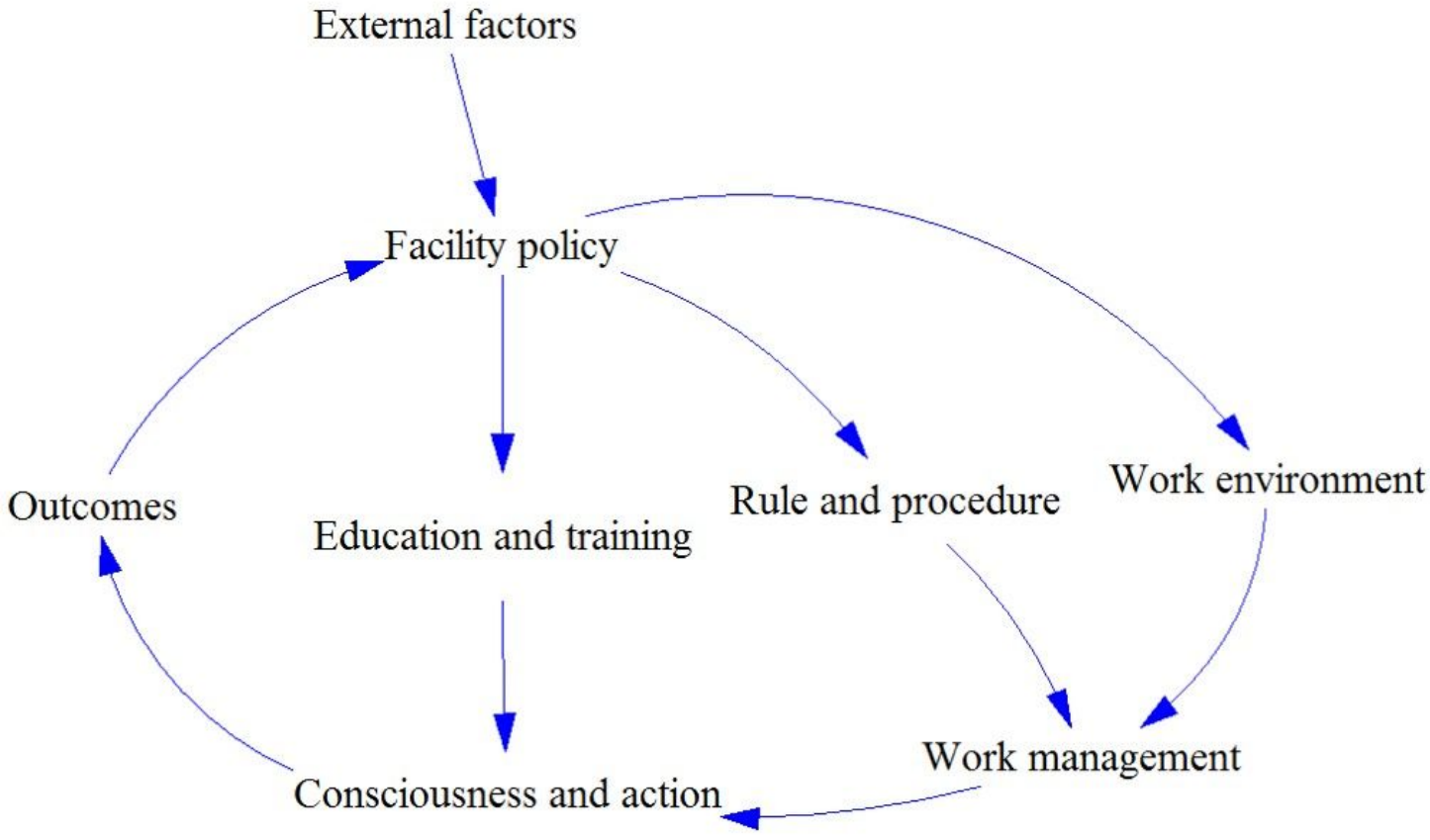


Figure 4.1 The first level of the CLD

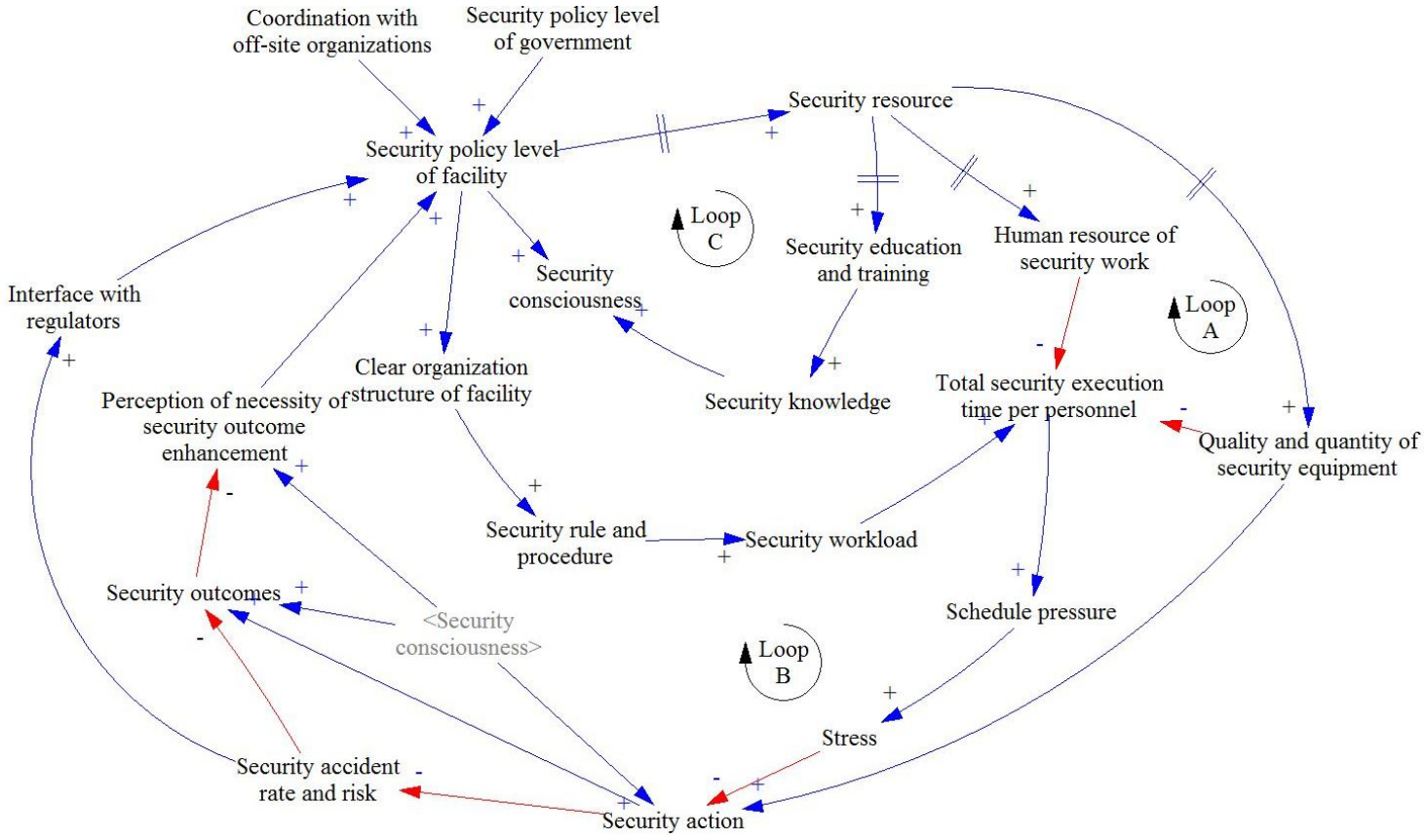


Figure 4.2 The second level of the CLD

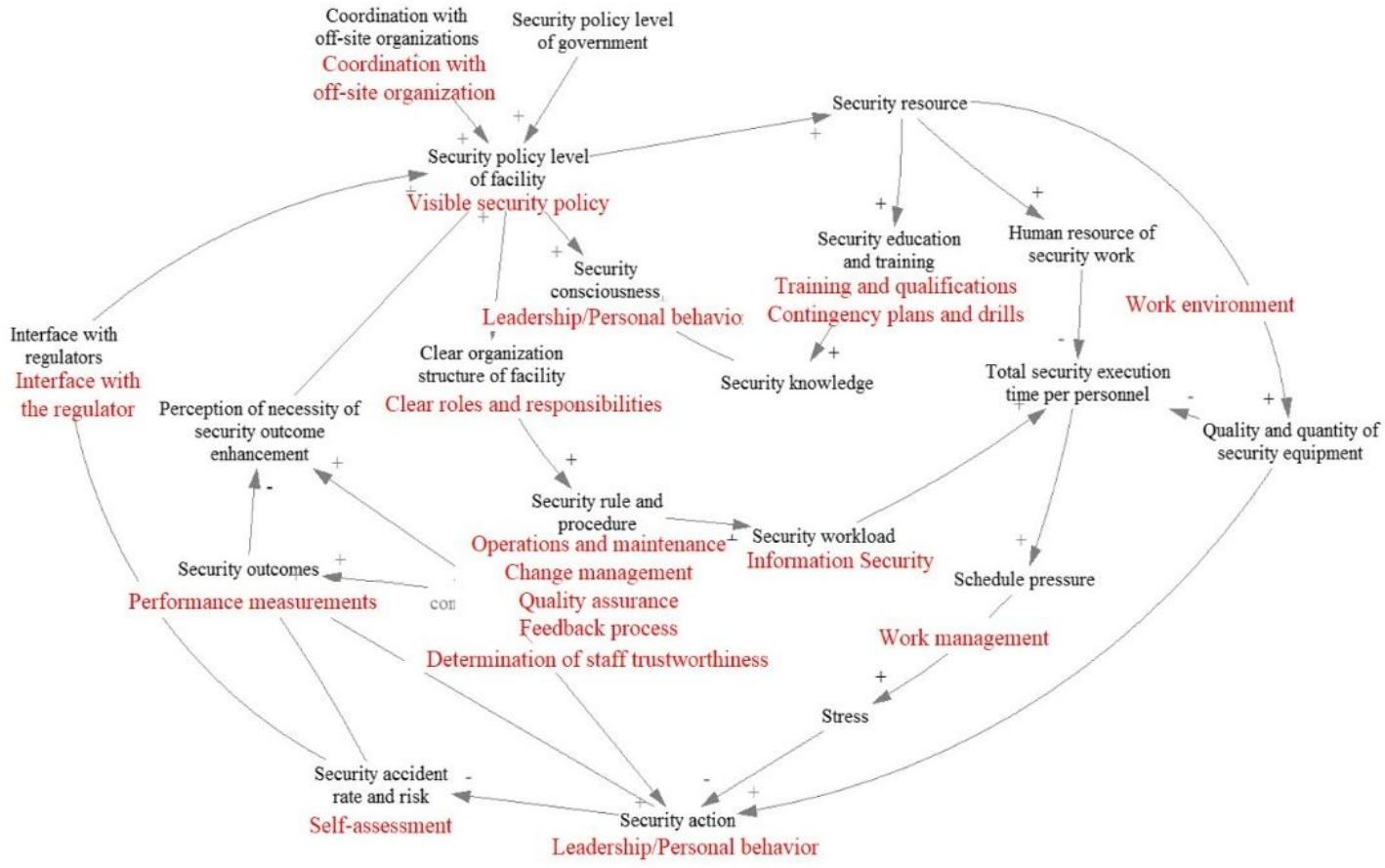


Figure 4.3 Linkage between the CLD and IAEA indicator

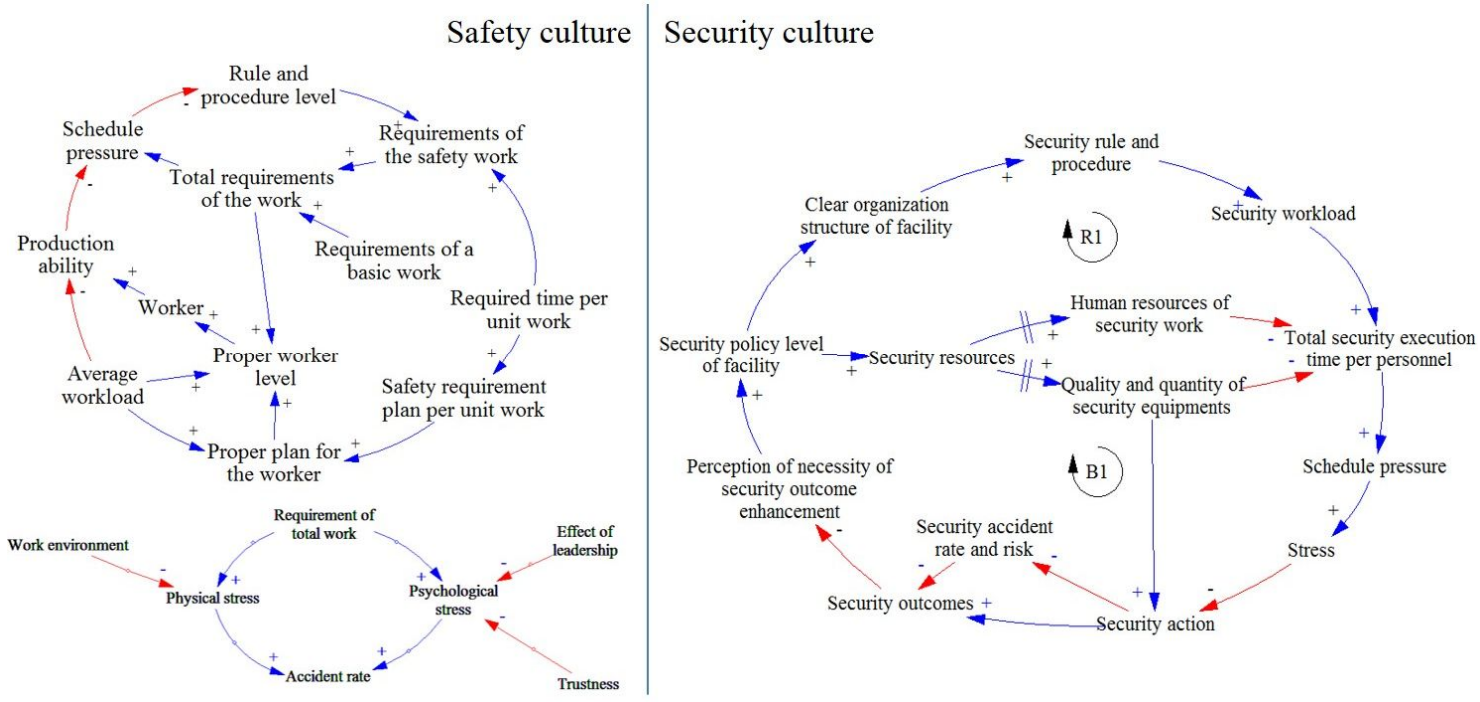


Figure 4.4 Comparison in 'Workload-Stress' section

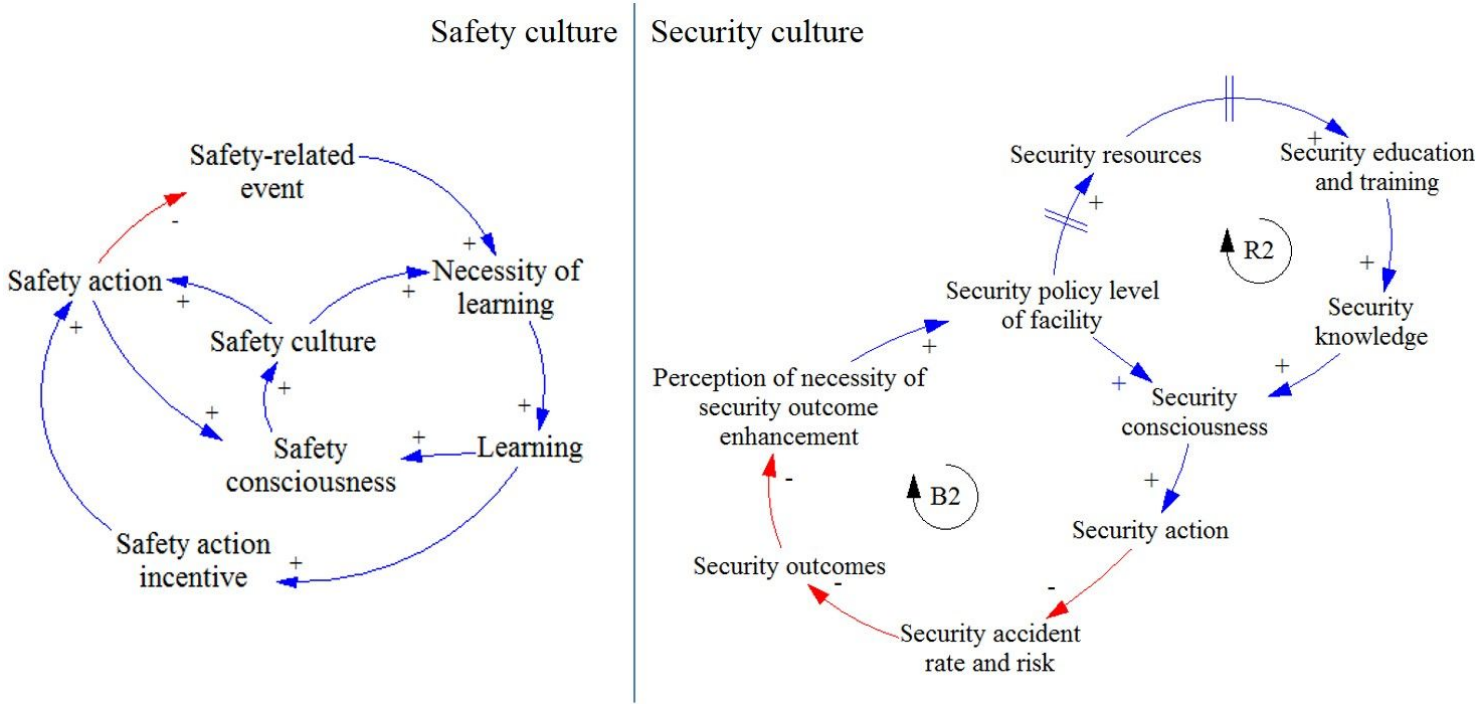


Figure 4.5 Comparison in 'Learning' section

4.2 Development of Stock Flow Diagram

The Stock Flow Diagram (SFD) is developed based on the CLD to demonstrate the transition phase of the elements by putting the concept of stock and flow. This diagram is suitable to capture dynamic characteristics.

4.2.1 Element of Stock Flow Diagram

The SFD has two kinds of the elements with different concepts. One is stock, which is an entity that accumulates or depletes over time, affected by flows. Flow is the rate of change in a stock and determined by the relations between other elements.

Before determining the elements of stock and flow, several elements are added and subdivided compared to the elements of the CLD. To give more details in determining the amount of security knowledge in terms of model quantification, 'Security education and training cycle' and 'Half-life of knowledge decay' is added. 'Security education and training cycle' is a cycle of security education and training on individuals. According to this cycle, security knowledge increases corresponding to the level of education and training at the time. 'Half-life of knowledge decay' is a speed of forgetting the knowledge acquired through education and training over time. The shorter half-life of knowledge decay means that the accumulated knowledge would be reduced quickly.

'Security consciousness' and 'Security action' are divided into Leader's and Employee's to enter their values more clearly. Thus, seven stocks are selected

among the elements of the CLD by considering their importance and relationships to demonstrate the transition phase: Security policy level of facility, Total security execution time, Security knowledge, Leader's/Employee's security consciousness, Leader's/Employee's security action. The inflows and outflows for each stock are as follows.

For security policy level of facility, the inflows are Security policy level of government, Coordination with off-site organizations, Interface with regulators and Perception of necessity of security outcome enhancement. Its outflow is oblivion.

For the execution time, the inflow is Security workload and the outflows are Human resource of security work, Quality and quantity of security equipment.

For security knowledge, the inflow is Security education and training. Its outflow is oblivion.

For Leader's security consciousness, the inflows are Security policy level of facility and Security knowledge. Its outflow is oblivion.

For Employee's security consciousness, the inflows are Leader's security consciousness and Security knowledge. Its outflow is oblivion.

For Leader's security action, the inflow is Leader's security consciousness and the outflow is stress.

For Employee's security action, the inflows are Employee's security consciousness, Quality and quantity of security equipment. Its outflow is stress.

4.2.2 Structure of Stock Flow Diagram

Based on these stocks and their flows, the structure of SFD is developed. In the first level of the SFD, as shown in Figure 4.6, 'External factors' have an influence

on ‘Security policy level of the facility’. The policy level of the facility determines the level of ‘Education and training’, ‘Rule and procedure’, and ‘Work environment’. ‘Education and training’ is inflow for ‘Security knowledge’ against their natural decay or oblivion. The accumulated knowledge increases the level of ‘Security consciousness and Security action’.

Workload determined by ‘Rule and procedure’ is inflow for ‘Total security execution time per personnel’. Its outflow, which shortens the execution time, is ‘Work environment’ including human resource and equipment. This execution time determines the level of stress in individuals, which decreases the level of security consciousness and security action.

Security consciousness and security action are measured as ‘Outcomes’. The increased outcomes decrease the policy level of the facility.

The second level of the SFD, as shown in Figure 4.7, have several feedback structures corresponding to the CLD. ‘Learning’ is detailed with the added element: ‘Security education and training cycle’ and ‘Half-life of knowledge decay’. The security knowledge increases at the indicated intervals, which is the cycle of education and training, corresponding to the level of education and training at the time. The accumulated knowledge becomes forgotten over time according to half-life of knowledge decay.

‘Security consciousness’ is divided into Leader’s and Employee’s. ‘Security policy level of the facility’ increases ‘Leader’s security consciousness’. Leader’s security consciousness increases not only ‘Employee’s security consciousness’, but also ‘Perception of necessity of security outcome enhancement’ directly. This means ‘Leader’s security consciousness’ has a direct impact on the perception of outcome enhancement and the policy level of the facility in order. The outflow of security consciousness is oblivion.

Likewise, ‘Security action’ is also divided into Leader’s and Employee’s. ‘Employee’s security action’ is influenced by ‘Quality and quantity of security equipment’ directly. The outflow of security consciousness is stress caused by overtime to manage the increasing security workload.

The temporal delays are supposed in the change of ‘Security resource’, ‘Security education and training’, ‘Human resource of security work’, ‘Quality and quantity of security equipment’, because they don’t immediately increase or decrease.

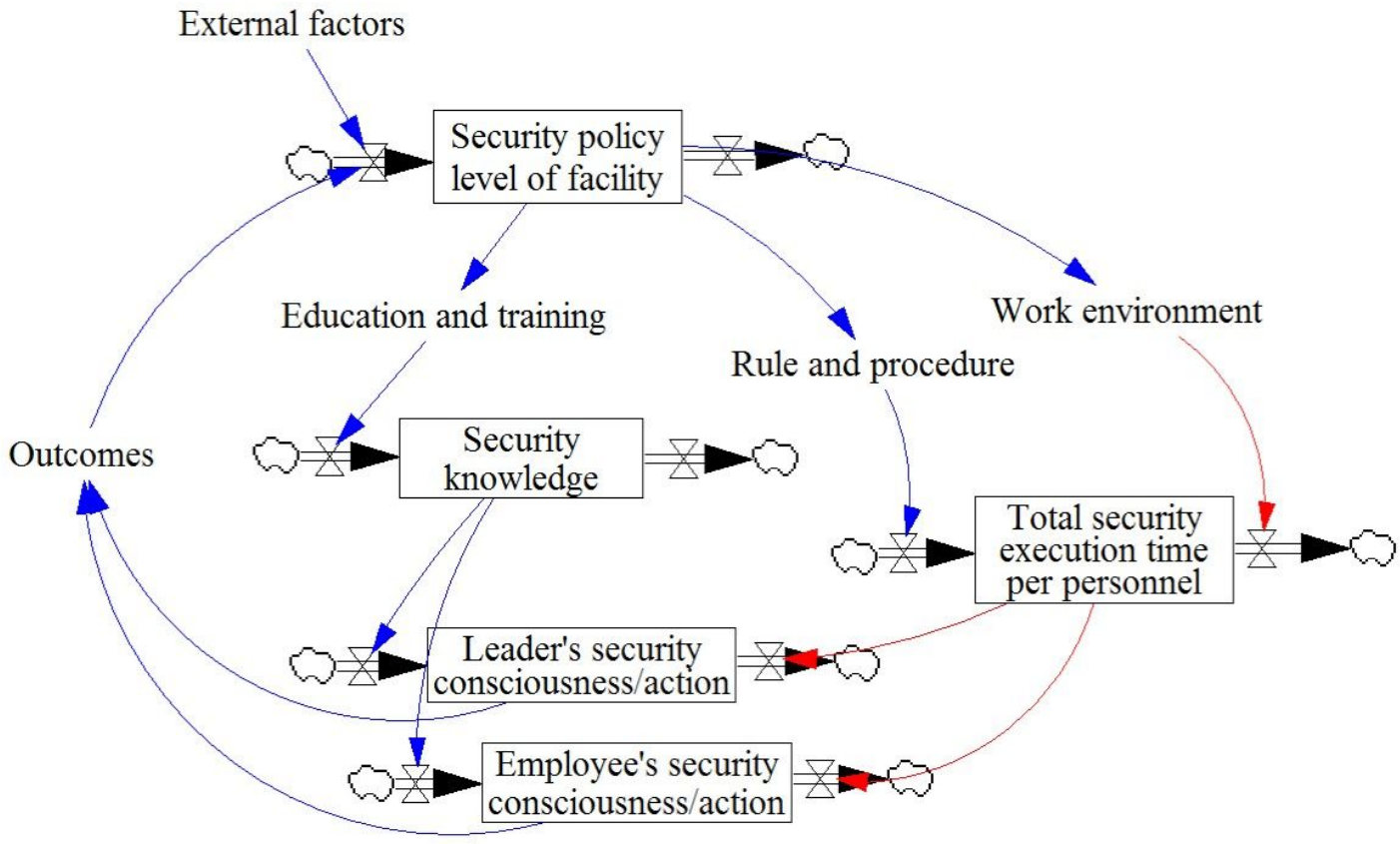


Figure 4.6 The first level of the SFD

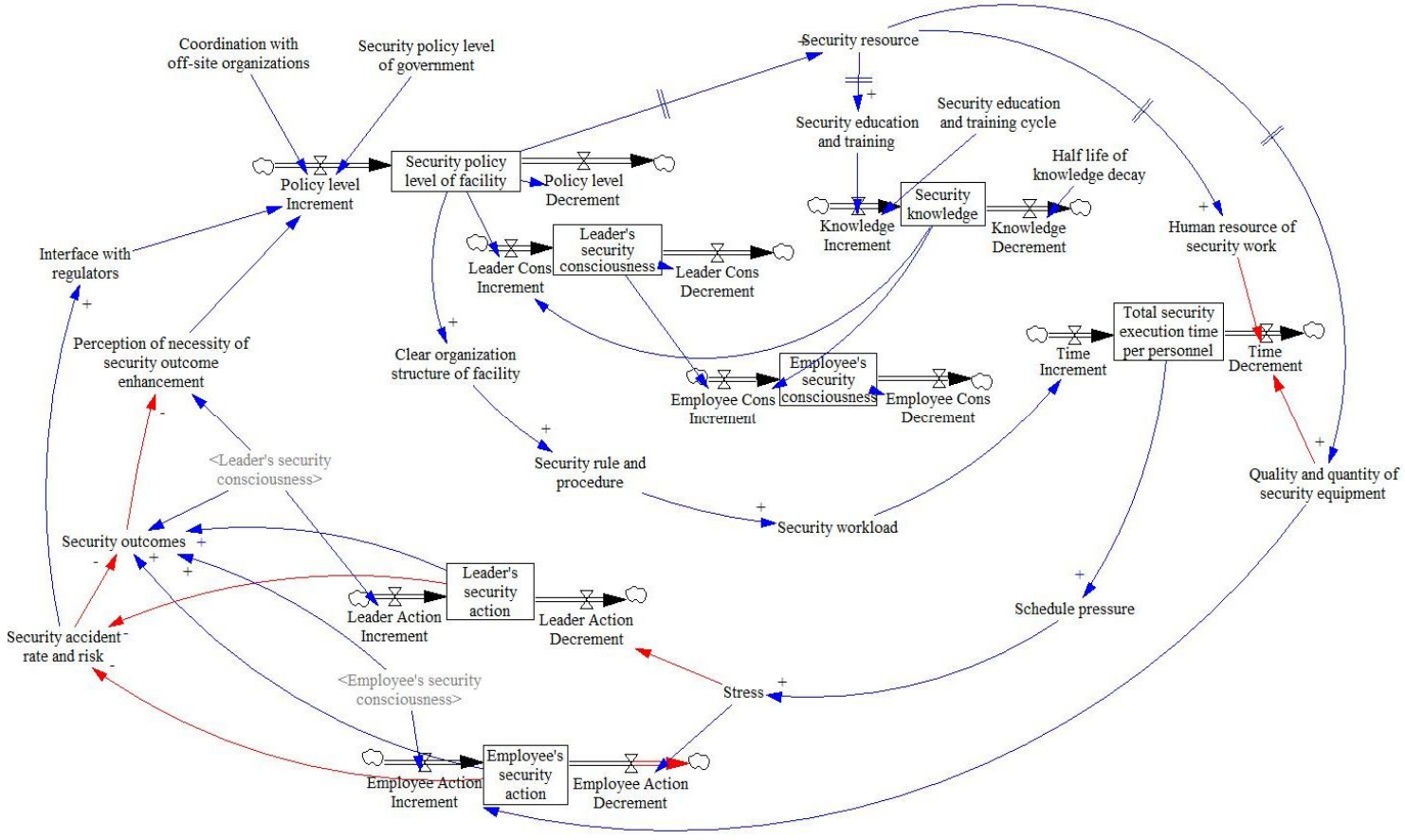


Figure 4.7 The second level of the SFD

5. Data Collection and Model Tuning

5.1 Development of Questionnaire

External factors, such as Security policy level of government, Coordination with off-site organizations, Interface with regulators and Security education and training cycle, Half-life of knowledge decay need the initial constant values, because these elements are not affected by other elements.

Stocks including Security policy level of facility, Total security execution time, Security knowledge, Leader's/Employee's security consciousness and Leader's/Employee's security action also need the initial values and the relationships between their inflow and outflow. The difference between inflow rate and outflow rate is integrated to the initial value of the stocks using the INTEG function representing the integral at every STEP TIME. To determine the values of other elements, the relationships between them is also required.

To determine the initial values and investigate the inter-relationships postulated in the developed SD model, two sets of survey questionnaires are developed, targeting the personnel at NPPs and their regulator. Each survey set is made of 39 and 6 questions which are designed to evaluate awareness of nuclear security culture and relevant infrastructure, respectively.

5.1.1 Questionnaire targeting the personnel at NPPs

The questionnaire targeting the personnel at NPPs is designed based on the definition of each element. As shown in Table 5.1, 39 questions are developed to determine the initial values of fifteen elements and their correlation equations. The contents of the questions are briefly summarized.

The survey is conducted among the executives and staffs in Korea Hydro & Nuclear Power Co. The data sets are collected from 846 people at NPPs. 198 people and 648 people are considered as the Leaders and Employees respectively. Among the 39 items, 37 questions use five-point Likert Scale (Strongly Disagree-Disagree-Equal-Agree-Strongly Agree). Other 2 questions are closed-answer question using the units of hours, minutes to investigate total working hours and the security execution time per day.

To classify the respondents, gender, age group, tenure of office, workplace and department, occupational group and assignment task (Physical protection/etc.) are asked as wells as their position.

The questions about Leader's security consciousness and action are particularly answered by both Leaders and Employees to minimize the tendency of Leaders to give themselves high scores. Therefore, the results of Leader's security consciousness and action are calculated with the combination of the data sets from Leaders and Employees. The data is combined with the ratio of 0.234 (198/846) from Leader's data sets and 0.766 (648/846) from Employee's data sets, which are proportional to the number of respondents in each group.

5.1.2 Questionnaire targeting the regulator

The questionnaire targeting the regulator is also designed based on the definition of two elements: Coordination with off-site organizations, Interface with regulators. As shown in Table 5.2, 6 questions are developed to determine their initial values. The contents of the questions are briefly summarized.

The survey is conducted among the experts in Korea Institute of Nuclear Nonproliferation and Control. The number of respondents is 10, who are experts in physical protection. 6 questions use five-point Likert Scale (Strongly Disagree-Disagree-Equal-Agree-Strongly Agree).

5.2 Statistical Analysis

The data sets are collected from 846 people at NPPs and 10 experts at their regulatory agency. Regression analysis are applied to verify their statistical significance as well as reliability and validity, before determining the initial values and their relationships.

In reliability analysis, reliability is defined as the possibility to obtain the same result when the measurement is repeated for the same concept. Typically, this analysis uses the internal consistency method with Cronbach's α coefficient. Cronbach 'α coefficient, which is expressed in Equation (5-1), needs to be larger than at least 0.60 to ensure reliability of the survey result.

$$\alpha = \frac{K}{K-1}\left(1 - \frac{\sum_{i=1}^{K} \sigma_{Y_i}^2}{\sigma_X^2}\right) \quad (5-1)$$

where K: # of Questions, $\sigma_{Y_i}^2$: Variance of ith Question,

σ_X^2: Variance of All Questions

Using the equation, the result from reliability analysis is shown in Table 5.3. The elements which are asked with just one question are excluded. The data sets collected from 846 people at NPPs are used to calculate the Cronbach 'α coefficients of Security policy level of facility, Clear organization structure of facility, Security rule and procedure, Security education and training, Security consciousness and action. Their coefficients are larger than 0.60 and the reliability of the survey result is confirmed. The data sets collected from 10 experts at their regulatory agency are used to calculate the Cronbach 'α coefficients of Coordination with off-site organizations, Interface with regulators. Contrary to the prior results, the coefficients are not larger than 0.60. Instead, the coefficients can become large enough when 'Q.3 Education for subcontractor' and 'Q.3 Exchanging enough information' are removed from Coordination with off-site organizations and Interface with regulators respectively.

Validity analysis is the method to verify whether abstract concepts of the targets have actually been measured by appropriate measurement tools. This statistical method enables to combine several highly correlated items into a few elements, while minimizing the loss of information inherent in each item. In this context, factor analysis is applied to measure the validity of the items to be combined into the assigned elements. Generally, the statistical significance of the items are recognized as the sub-elements when their factor loadings are larger than at least 0.6 for a single dimension. The result from factor analysis is shown in Table 5.4. The elements with one item are excluded. Every relationships between the

elements and their items are validated with the values of factor loadings, which are larger than 0.6 for the assigned elements.

Regression analysis is the statistical method to investigate the functional relationship between two variables. To determine the postulated in the developed SD model, the correlation equations are estimated using method of least squares. The R-squared, which is expressed in Equation (5-2), is the percentage of the variation explained by the regression line compared to the total variation.

$$R^2 = \frac{\sum_{i=1}^{n}(\hat{y}_i - \bar{y})^2}{\sum_{i=1}^{n}(y_i - \bar{y})^2}, \quad 0 \leq R^2 \leq 1 \qquad (5-2)$$

where n: # of Samples, $\hat{y}_i$: The estimated value of Y with ith sample,

$\bar{y}$: The mean of Y

As the value of R-squared gets closer to 1, the goodness of fit of the correlation equations becomes higher. The result from regression analysis is shown in Table 5.5. Some relationships are excluded, when they are not significant statistically. To raise the values of R-squared and better reflect the real world phenomenon, the data sets can be separated by the ratio of total security execution time to total working hours. For determining an appropriate ratio to improve the quality of the result from regression analysis, the ratio from 0.1 to 0.9 is tested under the condition of significance probability < 0.05. As a result of trial and error, it turns out that 0.2 is the most appropriate ratio for clarifying the existing relationships and showing the different features between two groups of the ratio above 0.2 and below 0.2. Based on these results, the model can be developed into two separate models.

5.3 Model Tuning

As a result of statistical analysis, it turns out that two separate SD models can be built using responses from security-worker and non-security-worker as distinguished by the ratio of total security execution time to total working hours and better reflect the real world phenomenon. 0.2 is the most appropriate ratio for showing the differences between two groups. One group of the ratio above 0.2 is considered as Security-worker. The other group of the ratio below 0.2 is considered as Non-security-worker. Therefore, the SFD, which demonstrates the dynamic nature of the main elements in terms of stocks and flows processes, is developed into two separate models; Model A (Security-worker) and Model B (Non-security-worker).

5.3.1 Model for Security-Worker

The Model A, which is the model for Security-worker is shown in Figure 5.1. There are two major different characteristics from the prototype of the SFD. When the execution time increases, schedule pressure decreases. It can be understood that they are not overloaded. The other difference is that stress due to security work does not have a significant impact on security action. Because security work is all they have to do for Security-worker.

Compared to Model B, the execution time of Security-worker can decrease by raising the level of human resource and equipment. Their security action increases with their security consciousness only.

5.3.2 Model for Non-Security Worker

The Model B, which is the model for Non-security-worker is shown in Figure 5.2. Likewise, there are two major different characteristics from the prototype of the SFD. When security execution time increases, schedule pressure increases. It can be understood that they think of security works as additional work. Contrary to Model A, stress due to security work has a significant impact on Employee's security action.

In addition, the execution time of Non-security-worker cannot decrease by raising the level of human resource and equipment. This means that their security work is not directly reduced by those resources. Security action increases with not only their security consciousness but also quality and quantity of security equipment. This means that the adequate equipment can improve security action of Non-security-worker.

Table 5.1 Questionnaire targeting the personnel at NPPs

Element	Question
Security policy level of facility	Q.1. Establishment of clear security goals
	Q.2. Sustainable management for achieving the security goals
Clear organization structure of facility	Q.1. Documentation-level of roles and responsibilities relevant to security
	Q.2. Job training for roles and responsibilities relevant to security
Security rule and procedure	Q.1. Establishment of rules and procedures for security work
	Q.2. Accessible guidelines and procedures document relevant to security
	Q.3. Providing management guidance on important information
	Q.4. Appropriate measures for reported security-related complaint
	Q.5. Adequacy of assessment method to determine staff trustworthiness
	Q.6. Adequacy of timing and frequency of assessment method applied
Total security execution time per personnel	Q.1. Total working hours per day
	Q.2. Total execution time for security work per day
Schedule pressure	Q.1. The level of schedule pressure due to security work
Stress	Q.1. The level of stress due to security work
Security resource	Q.1. The level of resources allocated to security work

Human resource of security work	Q.1. The level of human resource compared to the level required
Quality and quantity of security equipment	Q.1. The quality and quantity of security equipment compared to the level required
Security education and training	Q.1. Implementation of internal / external training programs on security
	Q.2. Regular implementation of emergency response training
	Q.3. Accessible reporting window for security-related complaint
	Q.4. Self-assessment of security work
	Q.5. Periodic audit of information security
Perception of necessity of security outcome enhancement	Q.1. Continuous efforts to solve security-related issues
Leader's security consciousness	Q.1. Creating an atmosphere to report freely security-related complaint
	Q.2. Regularly sharing information about security-related incidents and problems
	Q.3. Encouraging various proposals for enhancing security
	Q.4. Recognition of one’s contribution
Employee's security consciousness	Q.1. Understanding of their role and responsibilities relevant to security
	Q.2. Responsibility for enhancing security
	Q.3. Recognition of the importance of standardized performance procedures
	Q.4. Compliance with security rule and procedure

Leader's security action	Q.1. Establishing and sharing short-term goals relevant to security
	Q.2. Leading by example
	Q.3. Continuous monitoring and supervision of security work
	Q.4. Constructive feedback
Employee's security action	Q.1. Retaining security knowledge related to their assignment task
	Q.2. Familiarity with internal security policy
	Q.3. Attention to security threat
	Q.4. Response to the detected security threat according to security guidelines

Table 5.2 Questionnaire targeting the regulator

Element	Question
Coordination with off-site organizations	Q.1. Coordination with national organizations
	Q.2. Coordination with local police, military, medical facilities, etc.
	Q.3. Education for subcontractor
Interface with regulators	Q.1. Cooperation on regulatory assessment
	Q.2. Implementation of instructions from regulatory agencies
	Q.3. Exchanging enough information

Table 5.3 Result from reliability analysis

	Security policy level of facility	Clear organization structure of facility	Security rule and procedure	Security education and training	Security Consciousness		
					Leader		Employee
Cronbach 'α coefficient	0.845	0.856	0.931	0.863	0.839	0.868	0.824
# of Questions	2	2	6	5	4	4	4
Maximum Cronbach 'α coefficient	.	.	.	.	0.840 [Removal of Q.4] (recognition of one's contribution)	.	.

	Security Action			Coordination with off-site organizations	Interface with regulators
	Leader		Employee		
Cronbach 'α coefficient	0.857	0.891	0.776	-0.077	0.396
# of Questions	4	4	4	3	3
Maximum Cronbach 'α coefficient	0.872 [Removal of Q.2] (leading by example)	.	.	0.833 [Removal of Q.3] (education for subcontractor)	0.926 [Removal of Q.3] (exchanging enough information)

Table 5.4 Result from validity analysis

Element	Factor loading	Items
Security policy level of facility	0.900	Q.1. Establishment of clear security goals
	0.609	Q.2. Sustainable management for achieving the security goals
Clear organization structure of facility	0.904	Q.2. Job training for roles and responsibilities relevant to security
	0.803	Q.1. Documentation-level of roles and responsibilities relevant to security
Security rule and procedure	0.851	Q.2. Accessible guidelines and procedures document relevant to security
	0.844	Q.4. Appropriate measures for reported security-related complaint
	0.717	Q.1. Establishment of rules and procedures for security work
	0.633	Q.3. Providing management guidance on important information
	0.616	Q.5. Adequacy of assessment method to determine staff trustworthiness
	0.603	Q.6. Adequacy of timing and frequency of assessment method applied
Security education and training	0.862	Q.2. Regular implementation of emergency response training
	0.785	Q.4. Self-assessment of security work
	0.757	Q.3. Accessible reporting window for security-related complaint
	0.683	Q.5. Periodic audit of information security
	0.617	Q.1. Implementation of internal / external training programs on security

Table 5.5 Result from regression analysis

Element	Correlation Equation	R^2
Clear organization structure of facility	=0.827*(Security policy level of facility)+0.771	0.539
Security rule and procedure	=0.523*(Clear organization structure of facility)+1.137	0.633
Security resource	=0.814*(Security policy level of facility)+0.705	0.160
Human resource of security work	=0.778*(Security resource)+0.697	0.509
Quality and quantity of security equipment	=0.417*(Security resource)+2.565	0.222
Security education and training	=0.255*(Security resource)+2.782	0.215
Stress	=0.758*(Schedule pressure)+0.537	0.487

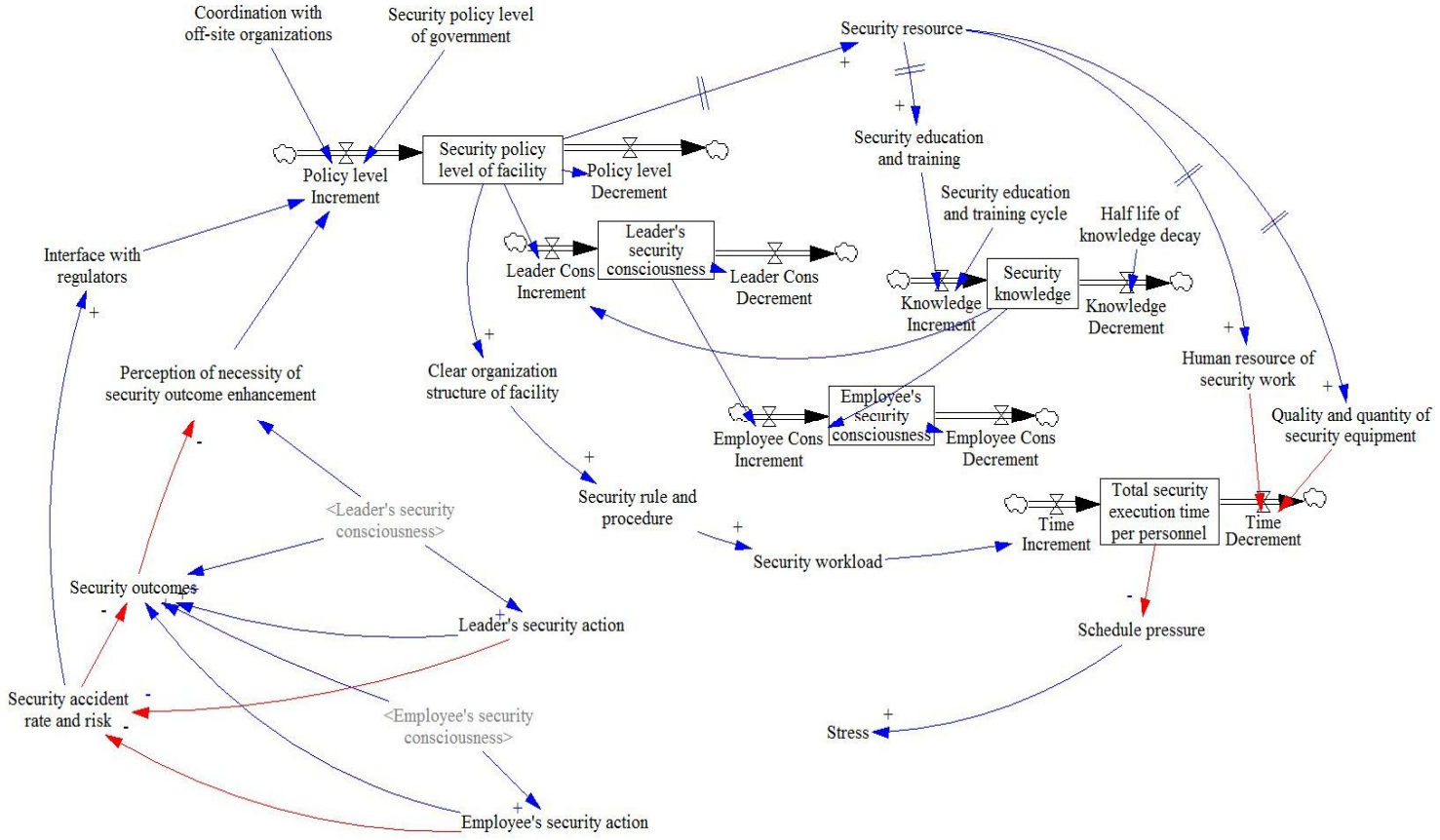


Figure 5.1 The SFD for Security-worker (Model A)

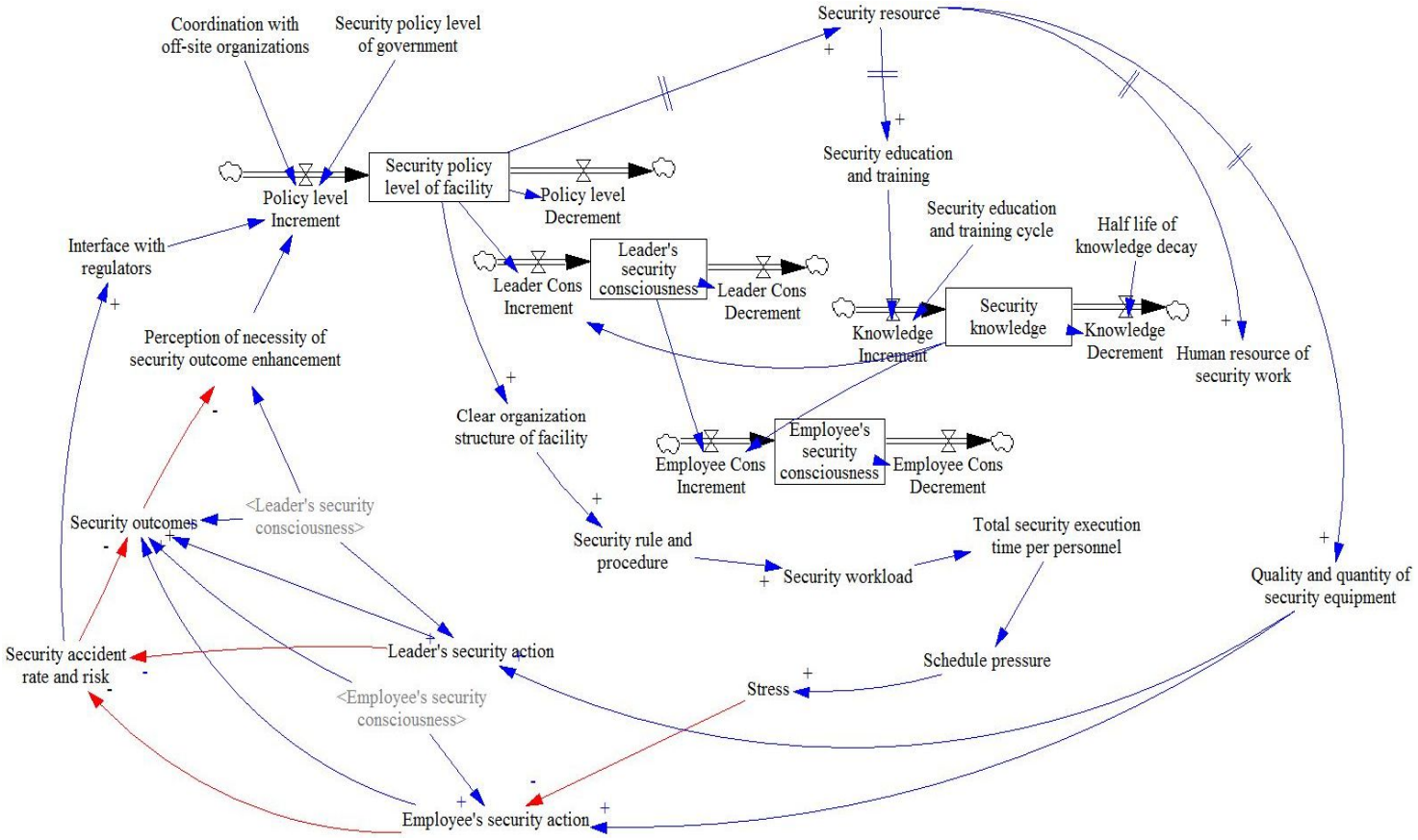


Figure 5.2 The SFD for Non-security-worker (Model B)

6. Model Application

6.1 Base Scenario

To make an assumption for a base scenario, the result of the same survey in 2014 and 2015 was compared as shown in Table 6.1. There is no significant change in the level of consciousness and action. Therefore, the assumption that security knowledge and periodic model behavior in one year do not carry forward to the next year is made. Under the assumptions, the two separate models are simulated in the base scenario.

From the survey results, the initial values of the elements on a five-point scale and their correlation equations are incorporated into the models. The average of each question is used to determine the initial values and linear regression is applied to obtain the correlation equations. Additionally, the initial value of 'Security policy level of government' is estimated on a five-point scale, based on the Nuclear Threat Initiative (NTI) Nuclear Threat Index. However, there are still some challenges remaining to determine the abstract values such as 'Half-life of policy level decay', 'Half-life of knowledge decay' and 'Half-life of consciousness decay'. Some correlations among 'Security accident rate and risk', 'Security outcomes', 'Perception of necessity of security outcome enhancement' and 'Interface with regulators' are also difficult to be determined.

Therefore, some additional assumptions are made to simulate the base scenario as follows.

[Unit of Half-life: month]

· No accumulated security knowledge yearly.

· Repeated model behavior according to the cycle of security education and training.

· Model A and B: Half-life of policy level decay 0.77

· Model A and B: Half-life of knowledge decay is 1.39

· Model A: Half-life of consciousness decay is 1.14 for leaders, 3.14 for employees

· Model B: Half-life of consciousness decay is 2.49 for leaders, 2.69 for employees

· Model A and B: The assumed equations

① Security outcomes = (Leader's security consciousness+Leader's security action+Employee's security consciousness+Employee's security action)/4 *EXP(-Security accident rate and risk)

② Security accident rate and risk = EXP(-(Leader's security action+Employee's security action))

③ Perception of necessity of security outcome enhancement = Leader's security consciousness *EXP(-Security outcomes/5)

④ Interface with regulators = Initial Value*EXP(Security accident rate and risk)

The simulation is performed through the Vensim, which is the typical software for System Dynamics Analysis. As the basic simulation settings, the unit of time is set to month, and TIME STEP = 0.25, INITIAL TIME = 0, FINAL TIME = 60. This can derive the simulation result for 60 months including the transition phases of all the elements over time by calculating them at every TIME STEP according to the relationships entered. All the temporal delays between 'policy level change-resource', 'resource change-human resource, equipment, education and training' are assumed as three months.

More detailed inputs for the base scenario and their simulation results are explained in next sections: Model for Security worker (Model A) and Model for Non-security-worker (Model B).

6.1.1 Model for Security-worker

The inputs used in the base scenario for Security-worker (Model A) are summarized as shown in Table 6.2. These initial values and the relationships are re-derived with the 328 responses of which the ratio is above 0.2.

The graphs in Figure 6.1 show the result from the base scenario for Model A. As education and training have 12-month interval, the knowledge increases rapidly with the cycle of 12 months. This accumulated knowledge decreases according to the half-life of knowledge decay. Based on the changes in the knowledge, other elements, such as security policy level of facility, security consciousness and action, show periodic behavior with the cycle.

6.1.2 Model for Non-security-worker

The inputs used in the base scenario for Non-security-worker (Model B) are summarized as shown in Table 6.3. These initial values and the relationships are re-derived with the 518 responses of which the ratio is below 0.2.

The graphs in Figure 6.2 show the result from the base scenario for Model B. Likewise, the knowledge increases rapidly and decreases to almost zero with the cycle of education and training. Other elements are also changed with the cycle of 12 months just like the graphs of Model A

6.2 Model Validation

The validation of the SD models is impossible, because the models are already limited, simplified representations of the real world. The models, which have not yet been refuted, are accepted. Therefore, those acceptances are always conditional [7]. Instead of presenting direct evidence that the model is valid, the data collected in 2015 is compared with the data from the previous year (2014). In addition, an uncertainty is evaluated to check the model reliability.

6.2.1 Comparison with the 2014 data

To ensure the reliability of the current (2015) survey data, the correlation equations used as inputs in the model are compared with the date of previous year (2014). Based on the 2014 and 2015 data, two relationships between 'Security policy level of facility-Clear organization structure of facility' and 'Clear organization structure of facility-Security rule and procedure' are compared. The comparison between other elements is not performed due to the differences of the questionnaires. Specifically, the questions about change management, working hours, resources, workload and stress are not included in the 2014 questionnaire. In addition, some questions, which are subdivided in 2015, are combined in 2014. This comparison can be performed thoroughly with further studies based on the survey results in next three years (2016-2018).

First, the relationship between 'Security policy level of facility' and 'Clear organization structure of facility' is compared. The result is shown in Table 6.4 and Figure 6.3. The coefficients of the equations are 0.853 and 0.827 in the 2014 and 2015 data respectively. Compared to the value of 0.879, 0.827 plus 0.052 which is

two times its standard deviation in the 2015 data, 0.853 in the 2014 data is smaller. This means that the coefficient of the 2014 data exists within the 95% confidence intervals and the equation of 2015 is verified with the 2014 data. Similarly, the constants of the equations are compared. The constant 0.790 (2014) is smaller than the value of 0.957, 0.771 (2015) plus 0.186 (Standard deviation*2, 2015).

Second, the relationship between 'Clear organization structure of facility' and 'Security rule and procedure' is compared. The result is shown in Table 6.5 and Figure 6.4. The coefficient 0.545 (2014) exists within the 95% confidence intervals which range in 0.523 (2015) plus or minus 0.028 which is two times its standard deviation in the 2015 data. Similarly, the constant 1.070 (2014) is larger than the value of 1.035, 1.137 (2015) minus 0.102 (Standard deviation*2, 2015).

In this context, the coefficients and constants of the equations used as inputs in the model are indirectly validated with the 2014 data.

6.2.2 Uncertainty Evaluation

To check the model reliability, an uncertainty caused by the input data uncertainties is evaluated. The uncertainty means the estimate of the error, which is estimated value minus true value. When the true value is unknown and unknowable, the estimate of the error is only possible. The typical method to evaluate the uncertainty is stochastic sampling method. This method, so-called Brute force method, is to estimate the variance of z by sampling with many different sets of input according to their distribution with the Equation (5-3) below.

$$\sigma_Z^2 \equiv \sigma^2\left[\overline{Z}\right] = \frac{1}{N(N-1)}\sum_i^N \left(Z_i - \overline{Z}\right)^2;\ \overline{Z} = \frac{1}{N}\sum_i^N Z_i \qquad (5-3)$$

where N: # of Samples, Z_i: The estimated value of Z with ith sample,

$\bar{Z}$: The mean of Z

To apply the method to the models, a random sampling with 1000 different sets of coefficients and constants, which are varied according to the normal distribution with their means and standard deviation, is conducted. The estimated uncertainty, which is the variance of the level of consciousness and action, with 500 samplings after 5 years for 95% confidence interval is shown in Table 6.6.

6.3 Parameter Sensitivity Analysis

Based on the simulation result from the base scenario, sensitivity analysis is performed to determine the effect of each parameter on the level of security consciousness and action. To make changes in input variables, the initial values of each parameter are changed by 10% respectively. These effects are measured by percentage changes in the level of security consciousness and action. The magnitude of changes compared to the levels simulated in the base scenario is defined as their sensitivity. The process of the method is shown in Figure 6.5.

The result from this analysis on Model A and B can be summarized as shown in Figure 6.6 and 6.7. For example, 2.50% in the upper right of Figure 6.6 is the percentage change in the level of Leader's security consciousness in the model A, when the initial value of Security policy level of government is changed to +10%. In Model B, the percentage change in the level of Leader's security consciousness is 1.89% under the same conditions. Thus, it turns out that the level of Leader's security consciousness increases 0.61%P more in Model B than Model A

quantitatively against the same change of Security policy level of government.

By changing the initial values to -10% as well as +10%, the difference of impact between the certain amount of increment and decrement in the indicated element can be compared. For example, when the initial values of Security education and training cycle and Half-life of knowledge decay are changed to -10% rather than +10%, the percentage change in the level of Leader's security consciousness is bigger.

In both Model A and B, the level of security consciousness and action is very sensitive about the change of 'Security education and training', 'Security education and training cycle' and 'Half-life of knowledge decay'. When the initial value of Security education and training is changed to +10%, it is more effective as much as 0.67%P to 1.74%P in Model B than Model A in terms of raising the level of security consciousness and action. This means that Non-security-worker is more sensitive than Security-worker about the change of Security education and training. Likewise, when the initial value of Half-life of knowledge decay is changed to +10%, it is more effective as much as 0.79%P to 1.88%P in Model B than Model A. The initial values of some other elements, such as Security resource, Security education and training cycle, also have bigger impact in Model B, the Model for Non-security-worker.

In contrast, in Model A, the Model for Security-worker, the changes of the initial values of some elements, such as Security policy level of government, Coordination with off-site organizations, Interface with regulators and Perception of necessity of security outcome enhancement, have bigger impact on the level of security consciousness and action. This means that External factors including government, off-site organizations and regulators have influence on Security-worker substantially. The perception of necessity of outcome enhancement would

also contribute to raising the level of security consciousness and action of Security-worker directly.

Comparing the extent of changes in security consciousness with security action, the action has smaller dynamic range than the consciousness. Because the consciousness receive more direct impacts from the changes in the elements than the action. In addition, comparing Leader's consciousness and action with Employee's consciousness and action, Leaders are more influenced with External factors including government policy, off-site organizations and regulators. For Employees, the effects of resources, education and training appear more significantly.

Based on these results, a strategy to enhance nuclear security culture including security consciousness and action can be developed. For Leaders, the level of security consciousness and action can be raised through education and training by emphasizing the participation in the relevant programs and prioritizing them. For Employees, the importance of interactive relationship between external factors and internal security system needs to be recognized. More detailed policy recommendations are made in next section.

6.4 Policy Recommendation

The following six strategies are suggested for Security-worker and Non-security-worker from the sensitivity study result.

Strategy 1) Raising the policy level

Strategy 2) Expanding investment in education and training

Strategy 3) Shortening the cycle of education and training

Strategy 4) Raising the quality of education and training

Strategy 5) Raising the frequency of interaction with regulators

Strategy 6) Increasing allocation of security resource

The effectiveness of each strategy is compared in Table 6.7. As a result, a strategy to prevent security knowledge from becoming forgotten such as Strategy 3 and 4, would be the effective policy for all the workers. Especially, it is expected that the policy would be more effective for Non-security-worker, because the extent of the changes in Model B is bigger than Model A. For Security-worker, a strategy to raise the policy level or the frequency of regulations such as Strategy 1 and 5 is highly recommended.

Because the impact of the changes of the elements related to education and training, including 'Security education and training' is relatively big, the effort to expand the investment on relevant resources and to raise the quality and quantity of education and training would be very effective.

As discussed in the sensitivity result, security action has smaller dynamic range than security consciousness about the changes of almost every element. To enhance security actions effectively, an incentive program can be introduced and provide bonuses and extra points on performance rating for reporting abnormal behaviors and incidents.

Furthermore, this quantitative analysis tool for reliable estimates of the cultural effects caused by relevant policy decisions can be applied with many different scenarios before implementing them. By comparing the effectiveness of each improvement strategy as to security consciousness and action quantitatively, the

decision makers can find more effective policy towards the enhancement of the culture. The SD modeling process can also help improve the understanding of the complex system and secure the cultural foundation for nuclear security in commercial nuclear facilities in Korean settings.

Table 6.1 Comparison of the same survey results in 2014 and 2015

Element	Score (1-5 scale)		
	2014	2015	
Leader's security consciousness	4.13	3.97	▼ 0.16
Employee's security consciousness	4.42	4.43	△ 0.01
Leader's security action	4.22	4.18	▼ 0.04
Employee's security action	4.38	4.31	▼ 0.07

Table 6.2 Inputs for Security-worker (Model A)

Element		Input
Security policy level of government		=4.26
Coordination with off-site organizations		=3.73
Interface with regulators		=3.65*EXP((Security accident rate and risk))
Security policy level of facility		=INTEG((Policy level Increment)-(Policy level Decrement)) Initial value: 3.465
	(Policy level Increment)	=((Security policy level of government)+(Coordination with off-site organizations)+(Interface with regulators)+(Perception of necessity of security outcome enhancement))/4
	(Policy level Decrement)	=0.9585*(Security policy level of facility)
Clear organization structure of facility		=0.777*(Security policy level of facility)+0.93
Security rule and procedure		=0.535*(Clear organization structure of facility)+1.068
Security workload		=1*(Security rule and procedure)
Total security execution time per personnel		=INTEG((Time Increment)-(Time Decrement)) Initial value: 3.335
	(Time Increment)	=0.64937*(Security workload)
	(Time Decrement)	=0.149*(Human resource of security work)+0.379*(Quality and quantity of security equipment)
Schedule pressure		=-0.151*(Total security execution time per personnel)+3.851
Stress		=0.731*(Schedule pressure)+0.637
Security resource		=0.897*(Security policy level of facility)+0.201
Human resource of security work		=0.707*(Security resource)+0.811

Quality and quantity of security equipment		=0.4*(Security resource)+2.589
Security education and training		=0.235*(Security resource)+2.837
Security education and training cycle		=12
Half-life of knowledge decay		=1.39
Security knowledge		=INTEG((Knowledge Increment)-(Knowledge Decrement)) Initial value: 0
	(Knowledge Increment)	=PULSE TRAIN(0, 1, (Security education and training cycle), 120)*0.8*(Security education and training)
	(Knowledge Decrement)	=(Half-life of knowledge decay)*(Security knowledge)
Leader's security consciousness		=INTEG(0.1*((Leader Cons Increment)-(Leader Cons Decrement))) Initial value: 3.73
	(Leader Cons Increment)	=1.0975*(Security knowledge)+0.399*(Security policy level of facility)
	(Leader Cons Decrement)	=(Leader's security consciousness)/2.034
Employee's security consciousness		=INTEG(0.1*((Employee Cons Increment)-(Employee Cons Decrement))) Initial value: 4.36
	(Employee Cons Increment)	=0.38*(Security knowledge)+0.204*(Leader's security consciousness)
	(Employee Cons Decrement)	=(Employee's security consciousness)/4.524
Leader's security action		=0.735*(Leader's security consciousness)+1.237
Employee's security action		=0.662*(Employee's security consciousness)+1.465
Security outcomes		=((Leader's security consciousness)+(Leader's security action)+(Employee's security consciousness)+(Employee's security action))/4 *EXP(-(Security accident rate and risk))
Security accident rate and risk		= EXP(-(Leader's security action)+(Employee's security action))

Perception of necessity of security outcome enhancement	=(Leader's security consciousness) *EXP(-(Security outcomes)/5)

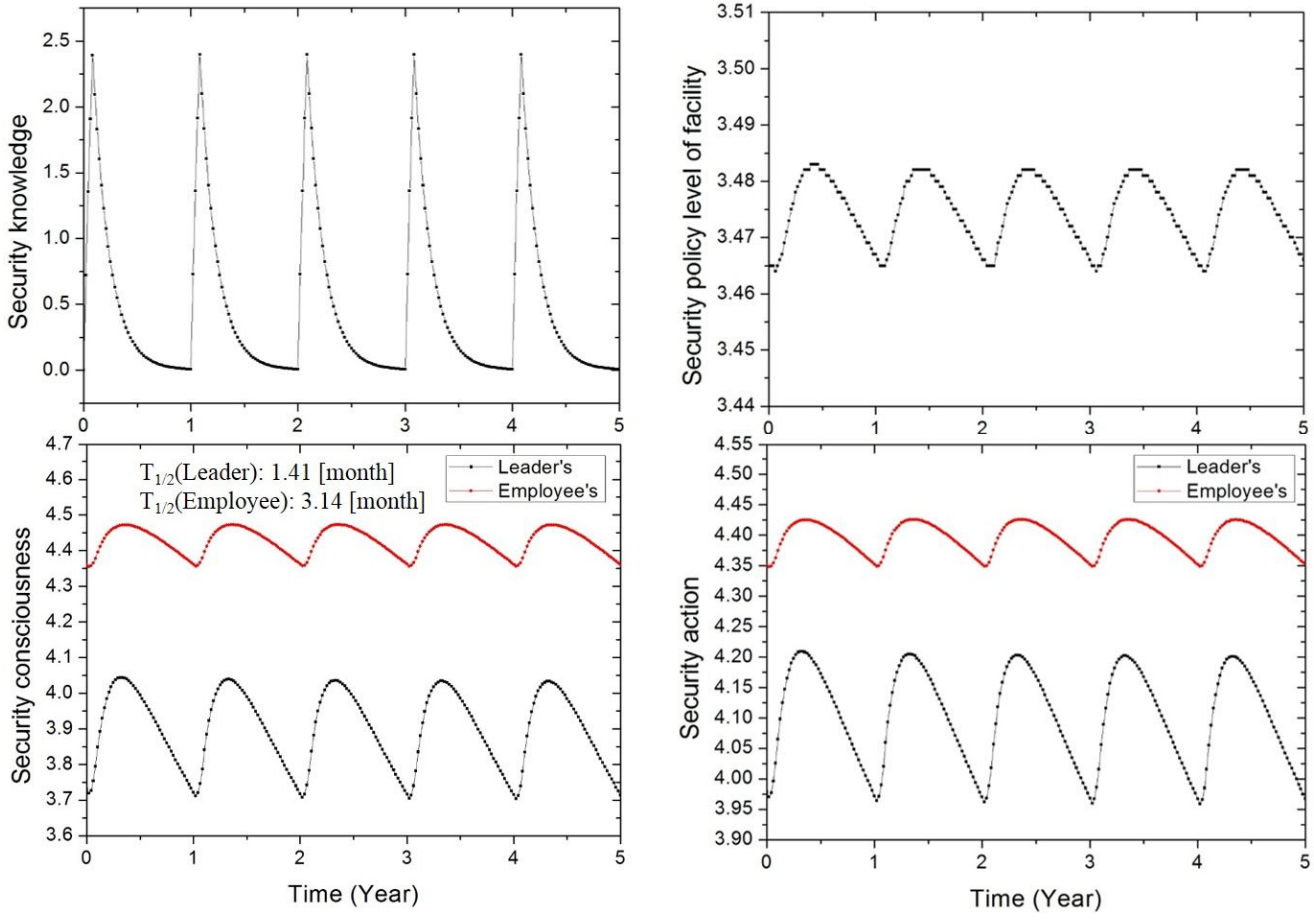


Figure 6.1 Base scenario for Security-worker (Model A)

Table 6.3 Inputs for Non-security-worker (Model B)

Element		Input
Security policy level of government		=4.26
Coordination with off-site organizations		=3.73
Interface with regulators		=3.65*EXP((Security accident rate and risk))
Security policy level of facility		=INTEG((Policy level Increment)-(Policy level Decrement)) Initial value: 3.537
	(Policy level Increment)	=((Security policy level of government)+(Coordination with off-site organizations)+(Interface with regulators)+(Perception of necessity of security outcome enhancement))/4
	(Policy level Decrement)	=0.9425*(Security policy level of facility)
Clear organization structure of facility		=0.854*(Security policy level of facility)+0.686
Security rule and procedure		=0.512*(Clear organization structure of facility)+1.195
Security workload		=1*(Security rule and procedure)
Total security execution time per personnel		=0.033*(Security workload)+0.334
Schedule pressure		=0.797*(Total security execution time per personnel)+2.931
Stress		=0.773*(Schedule pressure)+0.479
Security resource		=0.723*(Security policy level of facility)+1.16
Human resource of security work		=0.798*(Security resource)+0.701
Quality and quantity of security equipment		=0.421*(Security resource)+2.573
Security education and training		=0.269*(Security resource)+2.739
Security education and training cycle		=12
Half-life of knowledge decay		=1.39

Security knowledge		=INTEG((Knowledge Increment)-(Knowledge Decrement)) Initial value: 0
	(Knowledge Increment)	=PULSE TRAIN(0, 1, (Security education and training cycle), 120)*0.8*(Security education and training)
	(Knowledge Decrement)	=(Half-life of knowledge decay)*(Security knowledge)
Leader's security consciousness		=INTEG(0.1*((Leader Cons Increment)-(Leader Cons Decrement))) Initial value: 3.86
	(Leader Cons Increment)	=1.05125*(Security knowledge)+0.169*(Security policy level of facility)
	(Leader Cons Decrement)	=(Leader's security consciousness)/3.595
Employee's security consciousness		=INTEG(0.1*((Employee Cons Increment)-(Employee Cons Decrement))) Initial value: 4.35
	(Employee Cons Increment)	=0.55625*(Security knowledge)+0.215*(Leader's security consciousness)
	(Employee Cons Decrement)	=(Employee's security consciousness)/3.88
Leader's security action		=0.623*(Leader's security consciousness)+0.177*(Quality and quantity of security equipment)+0.996
Employee's security action		=0.77*(Employee's security consciousness)+0.109*(Quality and quantity of security equipment)-0.03*(Stress)+0.473
Security outcomes		=((Leader's security consciousness)+(Leader's security action)+(Employee's security consciousness)+(Employee's security action))/4 *EXP(-(Security accident rate and risk))
Security accident rate and risk		= EXP(-(Leader's security action)+(Employee's security action))
Perception of necessity of security outcome enhancement		=(Leader's security consciousness) *EXP(-(Security outcomes)/5)

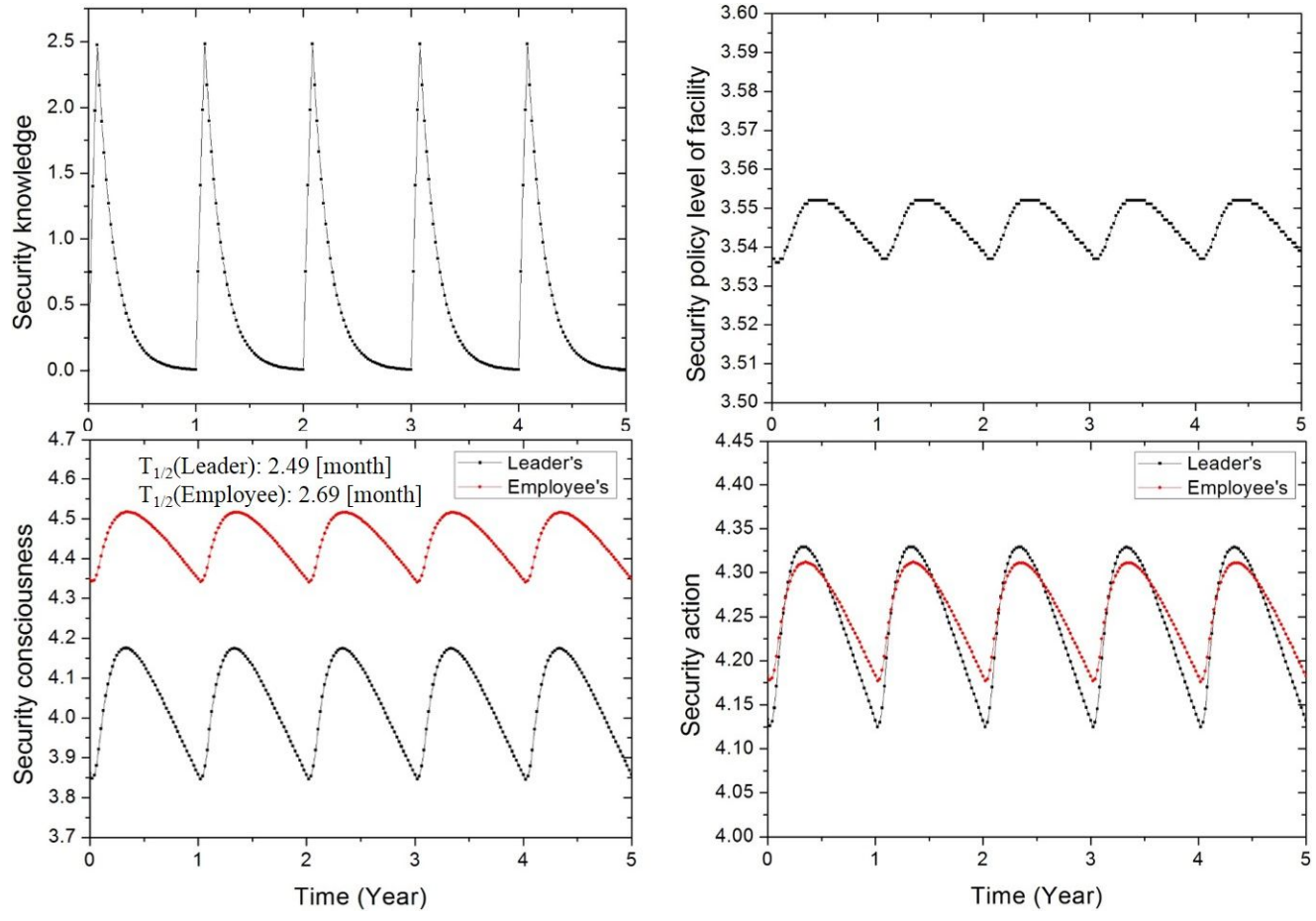


Figure 6.2 Base scenario for Non-security-worker (Model B)

Table 6.4 Comparison of the correlation equation (1)

Data	Correlation Equation (Clear organization structure of facility)	Standard Deviation*2 (Coefficient)	Standard Deviation*2 (Constant)
2015	=0.827*(Security policy level of facility)+0.771	0.052	0.186
2014	=0.853*(Security policy level of facility)+0.790	0.036	0.064

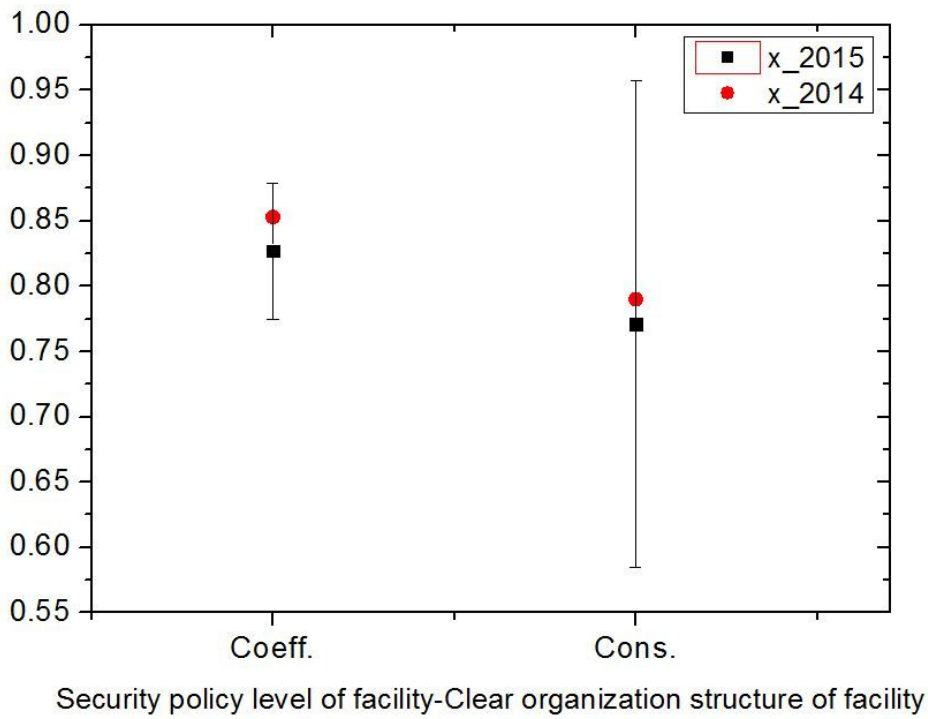


Figure 6.3 Graph on comparison of the correlation equation (1)

Table 6.5 Comparison of the correlation equation (2)

Data	Correlation Equation (Security rule and procedure)	Standard Deviation*2 (Coefficient)	Standard Deviation*2 (Constant)
2015	=0.523*(Clear organization structure of facility)+1.137	0.028	0.102
2014	=0.545*(Clear organization structure of facility)+1.070	0.028	0.104

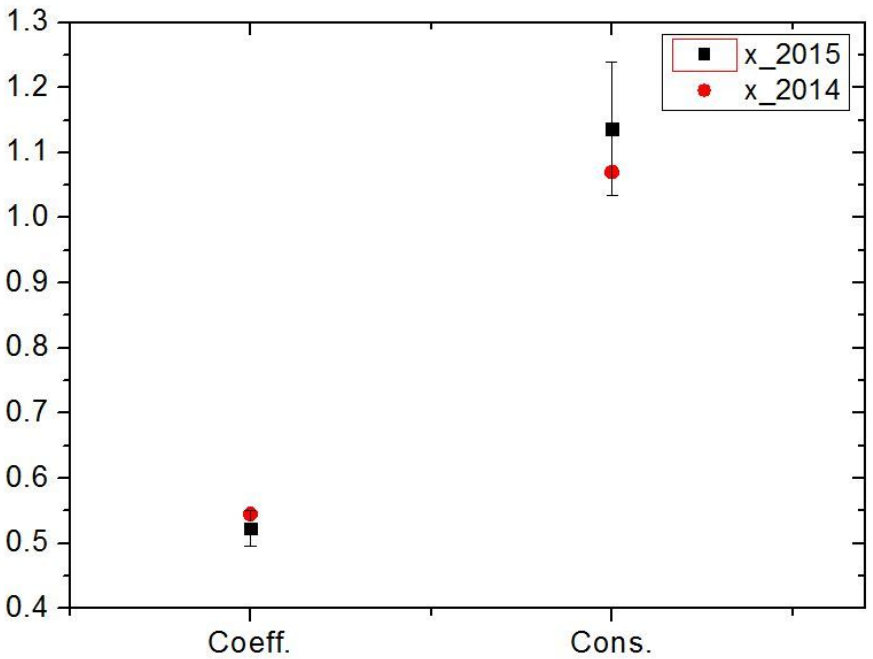


Figure 6.4 Graph on comparison of the correlation equation (2)

Table 6.6 Result from uncertainty evaluation

After 5yr / $\sigma^2[\bar{z}]$ (95% confidence interval)	Score (1-5 scale)	
	Model A (Standard Deviation)	**Model B** (Standard Deviation)
Leader's security consciousness	3.72 (0.02)	3.86 (0.02)
Employee's security consciousness	4.36 (0.02)	4.35 (0.02)
Leader's security action	3.97 (0.01)	4.14 (0.01)
Employee's security action	4.35 (0.01)	4.18 (0.01)

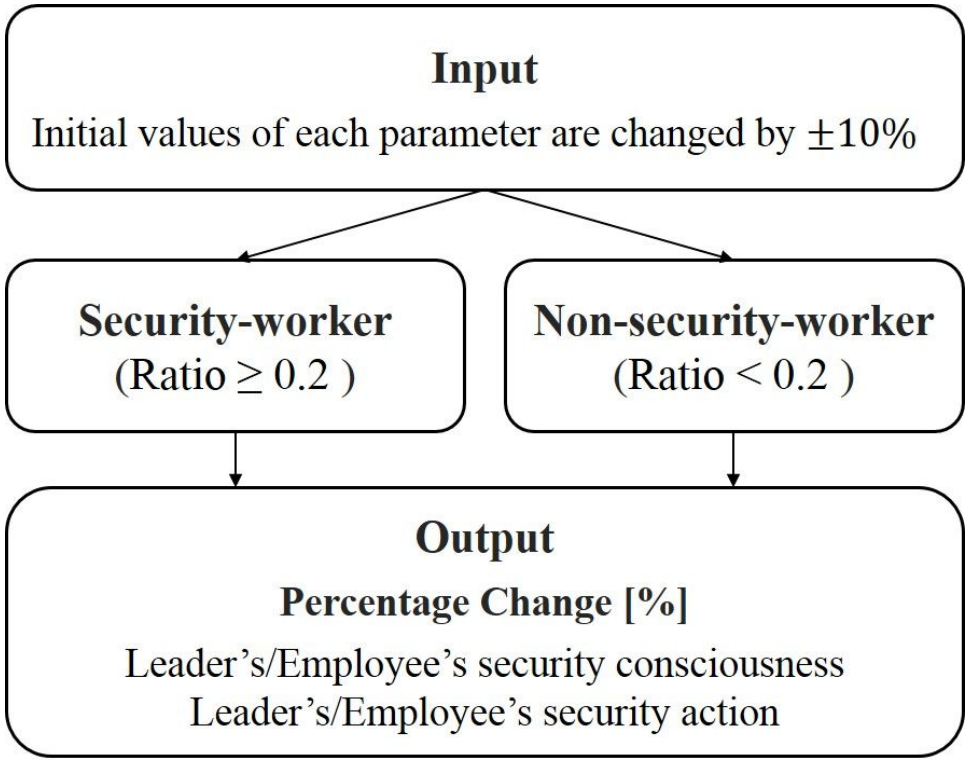


Figure 6.5 Process of sensitivity analysis method

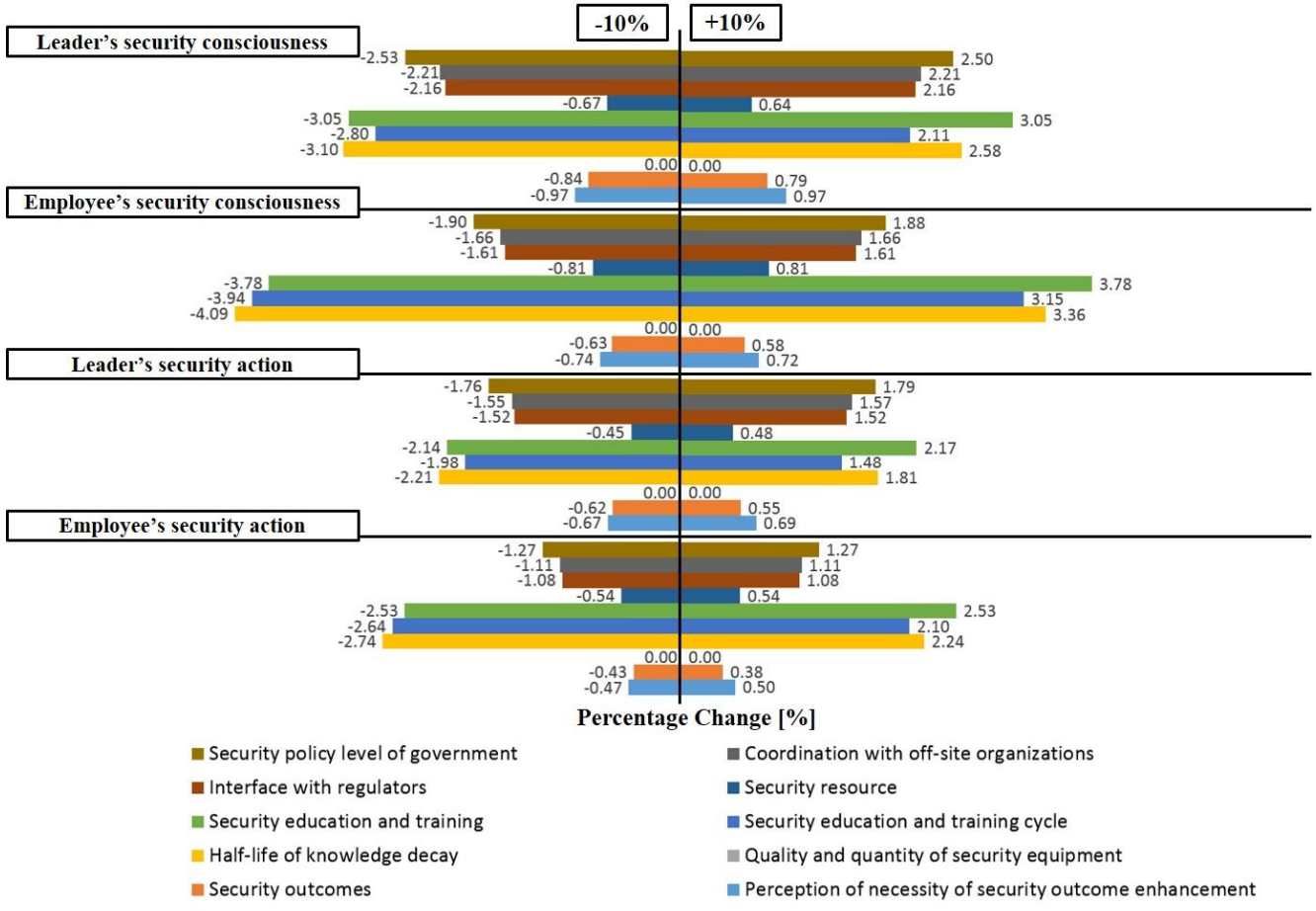


Figure 6.6 Result from parameter sensitivity analysis (Model A)

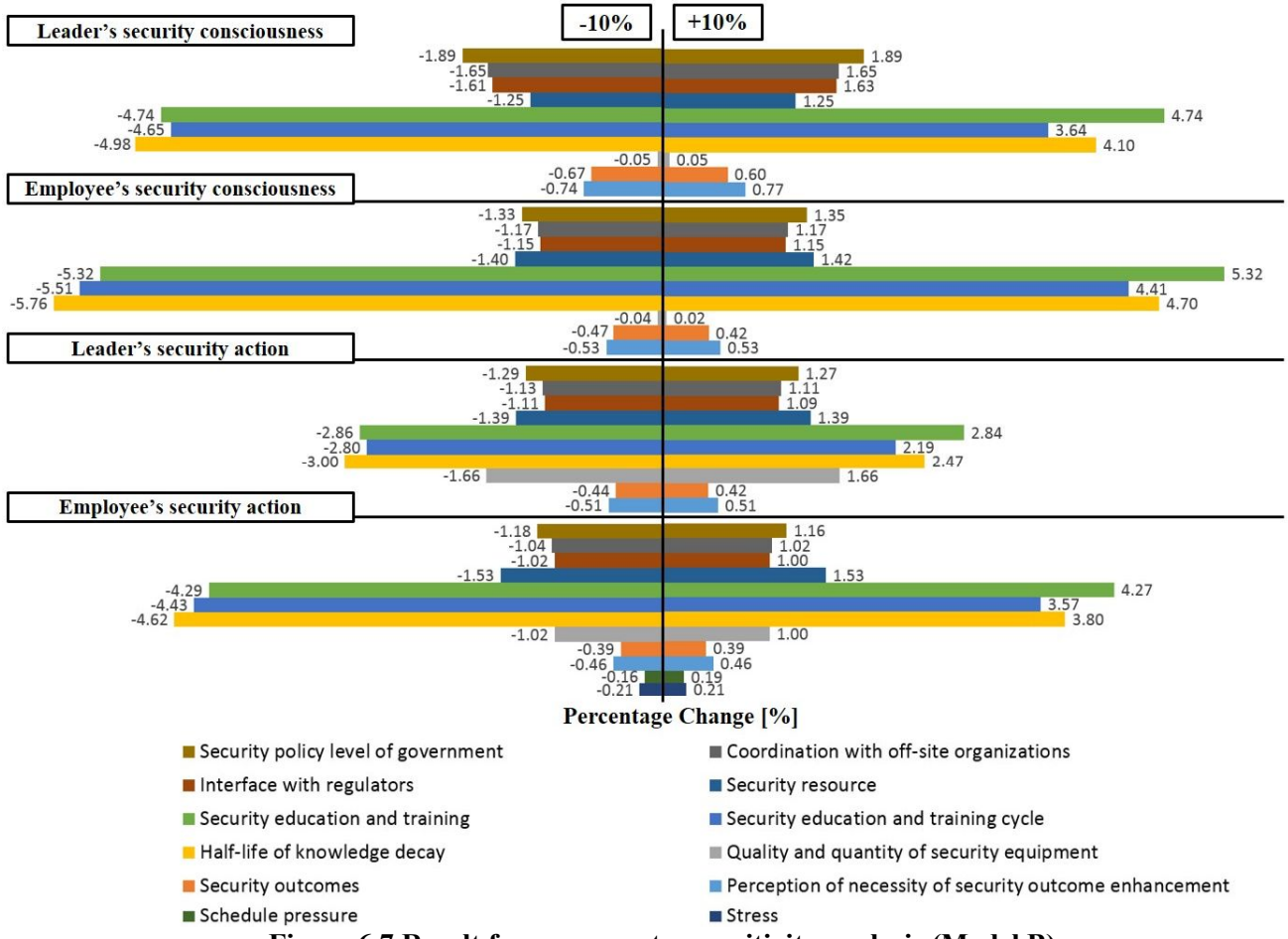


Figure 6.7 Result from parameter sensitivity analysis (Model B)

Table 6.7 Effectiveness of each strategy

Percentage Change [%]	Strategy 1		Strategy 2		Strategy 3	
Security-worker	1.86	0.44%P	2.88	1.41%P	2.84	1.51%P
Non-security-worker	1.42		4.29		4.35	

Percentage Change [%]	Strategy 4		Strategy 5		Strategy 6	
Security-worker	3.04	1.55%P	1.59	0.37%P	0.62	0.78%P
Non-security-worker	4.59		1.22		1.40	

7. Conclusion

7.1 Conclusion

This thesis emphasizes the systemic assessment of nuclear security culture as an instrumental vehicle to improve security readiness at Korean nuclear power plant effectively. To capture the dynamic and complex characteristics of the security culture, the approach involving System Dynamics (SD) models, large-scale surveys and inter-element sensitivity analysis is applied. A total of twenty key elements are employed for the development of the SD model based on the IAEA guidelines. Among those elements, their inter-relationship is deduced with the descriptive knowledge regarding the real world phenomenon. Two sets of survey questionnaires are developed, targeting the workers at nuclear power plants (NPPs) and their regulatory staffs, to determine the initial values of the elements on a one-to-five scale and to derive their correlation equations. Some abstract values and correlations need to be assumed to simulate a base scenario with the assumption that security knowledge and periodic model behavior in one year do not carry forward to the next year. As a result of statistical analysis, it turns out that two separate SD models can be built for Security-worker and Non-security-worker, respectively, as distinguished by the ratio of total security-related work hours to total work hours in order to better reflect the real world phenomenon.

To ensure the reliability of the current (2015) survey data of this thesis, the correlation equations used as inputs in the model are verified against the data set of

the previous year (2014). To test the model reliability, the model uncertainty caused by the input data uncertainties is statistically evaluated using the stochastic sampling method. By random sampling of many different sets of input data from their distribution, the uncertainty with 500 samplings after 5 years for 95% confidence interval is evaluated.

Based on the simulation result from the base scenario, the sensitivity analysis shows that the level of ‘Security consciousness and action’ is very sensitive to the change of 'Security education and training’, 'Security education and training cycle’ and ’Half-life of knowledge decay’. On this ground, a strategy to prevent security memory losses can include shortening the cycle of education and training and raising their quality. In addition, it is highlighted that providing sufficient education and training for Non-security-worker is particularly important to maintain the high-level of the culture within the facilities. For Security-worker, a strategy to raise the policy level or to increase the frequency of inspection can be effective mechanism. To promote security action, some incentive programs which can directly encourage the actions would be required. After comparing the effectiveness of each improvement strategy as to security consciousness and action quantitatively, six strategies are suggested for the policy recommendations towards the enhancement of the nuclear security culture at NPPs.

The primary contribution of this paper is to provide a systemic and quantitative analysis tool for reliable estimates of the cultural effects of relevant policy decisions by developing the SD model for the assessment of nuclear security culture at NPPs. The SD modeling process would help improve the understanding of the complex system and secure the cultural foundation for nuclear security in commercial nuclear facilities in Korean settings.

7.2 Future Work

The developed SD models, in this thesis, need to be improved with more detailed information that can be acquired by future work. There was a limit in the amount of accessible information related to nuclear security, due to both time and cost constraints. By acquiring more detailed information, especially from the same targeted facilities, the model improvement can be substantial.

By collecting data over several years in a consistent manner, the additional validation of the model is warranted. To ensure the reliability of the inputs including the initial values and their correlation equations further, the data used in the model should be validated using the multiyear data.

As additional considerations, the cost and benefit of the recommended strategies should be examined to test their effectiveness for rational policy-making, although difficult.

Ideally, the models on nuclear safety culture and those on nuclear security culture can be integrated to holistically understand their inter-relationships and to amplify their synergy, based on the limited comparison of the developed SD model with those on safety culture that is already performed in this thesis. By connecting the common elements of both models, an integrated unified SD model can be developed for use as a new research tool to encompass nuclear safety and nuclear security in terms of culture.

References

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, “Nuclear Verification and Security of Material: Physical Protection Objectives and Fundamental Principles”. GOV/2001/41, IAEA, Vienna, 2001; also contained in the amendment to the CPPNM.

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, “Nuclear Security Culture: Implementing guide”. Nuclear Security Series No. 7, IAEA, Vienna, 2008.

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, “Self-assessment of Nuclear Security Culture in Facilities and Activities that use Nuclear and/or Radioactive material”. Draft Technical Guidance, NST026, IAEA, Vienna, 2014.

[4] I. Khripunov, J. Holmes, D. Nikonov, M. Katsva, “Nuclear Security Culture: The Case of Russia”. Center for International Trade and Security, University of Georgia, 2004.

[5] M. Briere, D. Winter, “Nuclear Security Culture”. International Conference on Nuclear Security: Global Directions for the Future. London, United Kingdom, 16-18 March 2005.

[6] Hosik Yoo, Jeong-Ho Lee, “Results of Nuclear Security Culture Survey on personnel at nuclear power plants”. Annals of Nuclear Energy, 2015.

[7] John D. Sterman, “Business Dynamics: Systems Thinking and Modeling for a Complex World”, Irwin/McGraw-Hill, 2000.

[8] Leveson, N. G., Barrett, B., Carroll, J., Cutcher-Gershenfeld, J., Dulac, N., Zipkin, D., “Modeling, Analyzing, and Engineering NASA’s Safety Culture”, Phase 1 Final Report. MIT, 2005.

[9] Marais, K., Leveson, N. G., “Archetypes for organizational safety”, Safety Science 44(7), 2006.

[10] Lyneis, J., Madnick, S., “Preventing Accidents and Building a Culture of Safety: Insights from a Simulation Model”, Working paper, Composite Information Systems Laboratory, Sloan School of Management. MIT, 2008.

[11] Oh Youngmin, “Systems thinking perspective on the organizational safety culture of nuclear power plants in Korea”, Korean System Dynamics Society, Vol. 15, No. 1, 2014.

[12] Kim Byung-Suk, Jo Hyung-Woong, Oh Youngmin, “A study on the effects of nuclear power plant workers and organizational characteristics on accidents”, Korean System Dynamics Society, Vol. 15, No. 2, 2014.

[13] Gurpreet Dhillon, “Managing and controlling computer misuse”, Information Management & Computer Security, Vol. 7 Issue 4, pp.171–175, 1999.

[14] C. Melara, J. M. Sarriegi, J. J. Gonzalez, A. Sawicka, D.L. Cooke, “A System Dynamics Model of an Insider Attack on an Information System”, in From Modeling to Managing Security: A System Dynamics Approach, Norwegian Academic Press, Kristiansand (Norway), 2003.

[15] Farhad Foroughi, “The Application of System Dynamics for Managing Information Security Insider-Threats of IT Organization”, Proceedings of the World Congress on Engineering 2008, Vol. I, 2008.

[16] Sang-Chin Yang and Yi-Lu Wang, “System Dynamics Based Insider Threats Modeling”, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, 2011.

[17] J. M. Sarriegi, J. Santos, J. M. Torres, D. Imizcoz, E. Egozcue, D. Liberal, “Modeling and Simulating Information Security Management”, Critical Information Infrastructures Security, 2008.

[18] Derek L. Nazareth, Jae Choi, “A system dynamics model for information security management”, Information & Management 52, 2015.

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, “Safety culture”. INSAG-4, IAEA, Vienna, 1991.

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, “Self-assessment of safety culture in nuclear installations”. TECDOC-1321, IAEA, Vienna, 2002.

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, “The Interface Between Safety and Security at Nuclear Power Plants”. INSAG-24, IAEA, Vienna, 2010.

[22] Oh Youngmin, “Organizational safety culture for a safer society: Concepts and implementations in nuclear power plant”, Book Korea, 2014.

[23] INTERNATIONAL ATOMIC ENERGY AGENCY, “Objective and Essential Elements of a State's Nuclear Security Regime”. Nuclear Security Series No. 20, IAEA, Vienna, 2013.

[24] INTERNATIONAL ATOMIC ENERGY AGENCY, “Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme”. Nuclear Security Series No. 19, IAEA, Vienna, 2013.

[25] INTERNATIONAL ATOMIC ENERGY AGENCY, “Nuclear Security Plan 2014–2017”, Board of Governors General Conference, IAEA, Vienna, 2013.

[26] INTERNATIONAL ATOMIC ENERGY AGENCY, “Enhancing Nuclear Security Culture in facilities and activities that use nuclear and/or radioactive material”, Technical Guidance NST027, IAEA, Vienna, 2014.

[27] INTERNATIONAL ATOMIC ENERGY AGENCY, “Milestone in the Development of a National Infrastructure for Nuclear Power”, Nuclear Energy Series No. NG-G-3.1, IAEA, Vienna, 2007.

[28] World Institute for Nuclear Security, “International Best Practice Guides Nuclear Security Culture Version 2”, WINS, 2011.

[29] UK Agency of Health and Safety, “Guidance on the Assessment of Nuclear Security Culture within a Company/Organization”, UK Agency of Health and Safety Executive Civil Nuclear Security Technical Assessment Guide (CNS-TAST-GD-002 Revision 0), 2013.

[30] Ferly Hermana, Khairul Khairul, Bayu Purnomo, “Indonesia’s pioneering effort to self-assess nuclear security culture”, National Nuclear Energy Agency (BATAN), 1540 COMPASS, Issue 10, 2016.

[31] CSURGAI Jozsef, SOLYMOSI Mate, HORVATH Kristof, VASS Gyula, “Nuclear security culture self-assessment in a radioactive material associated facility”, Academic and Applied Research in Military and Public Management Science, Vol. 14, Issue 3, 2015.

[32] Nuclear Safety and Security Commission, “National Nuclear Security Culture Implementing Guide”, NSSC, 2013.

[33] Korea Institute of Nuclear Safety, “Study on Improvement of Nuclear Regulatory Performance using System Dynamics”, KINS/RR-1064, 2013.

[34] “Act on Measures for the Protection of Nuclear Facilities, etc. and Prevention of Radiation Disasters”, Act No.12665, Partial Amendment, Enforcement Date: 22. Aug, 2014.

[35] “Enforcement Decree of the Act on Physical Protection and Radiological Emergency”, Presidential Decree No.26140, Amendment by Other Act, Enforcement Date: 11. Mar, 2015.

[36] Schein, E. H., “Organizational Culture and Leadership”, 4th edition, Jossey-Bass, 2010.

[37] M.J. Hatch, “The Dynamics of Organizational Culture”, Academy of management review, 1993.

[38] Jack Boureston, Tanya Ogilvie-White, “Seeking Nuclear Security Through Greater International Coordination”, Working Paper, International Institutions and Global Governance program, 2010.

[39] Kim Do-Hoon, Moon Tae Hoon, Kim Dong Hwan, “System Dynamics”, Daeyoung Publishing Co., 2001.

[40] Jaekook Yu, Namsung Ahn, Moosung Jae, “A quantitative assessment of organizational factors affecting safety using system dynamics model”, Journal of Korean Nuclear Society, Vol. 36, No. 1, pp.64-72, 2004.

[41] Kyung Min Kang, Moosung Jae, “Development of radiation risk assessment simulator using system dynamics methodology”, Journal of Nuclear Science and Technology, Vol. 45, Supplement 5, 2008.

[42] Leveson, N.G. “Applying systems thinking to analyze and learn from events”, Safety Science 49, pp.55-64, 2011.

[43] M.D. Cooper, “Towards a model of safety culture”, Safety Science 36, pp.111-136, 2000.

[44] T. Lee, K. Harrison, “Assessing safety culture in nuclear power stations”, Safety Science 34, pp.61-97, 2000.

[45] Y. Barlas, “Formal Aspects of Model Validity and Validation in System Dynamics”, System Dynamics Review, Vol. 12, No. 3, 1996.

[46] Tobias, M.I., Cavana, R.Y., Bloomfield, A., “Application of a System Dynamics Model to Inform Investment in Smoking Cessation Services in New Zealand”, American Journal of Public Health, Vol 100, No. 7, 2010.

[47] Cheng Qi, Ni-Bin Chang, “System dynamics modeling for municipal water demand estimation in an urban region under uncertain economic impacts”, Journal of Environmental Management 92, pp.1628-1641, 2011.

[48] Houghton J., Siegel M., Wirsch A., Moulton A., Madnick S., Goldsmith D., “A Survey of Methods for Data Inclusion in System Dynamics Models: Methods, Tools and Applications”, Working Paper# 2014-03, Composite Information Systems Laboratory, 2014.

[49] Umit S. Bititci, Kepa Mendibil, Sai Nudurupati, Patrizia Garengo, Trevor Turner, “Dynamics of performance measurement and organisational culture”, International Journal of Operations & Production Management, Vol. 26, Issue 12, pp.1325 - 1350, 2006.

[50] DongHan Ham, “Research Trends of Cognitive Systems Engineering Approaches to Human Error and Accident Modelling in Complex Systems”, Journal of the Ergonomics Society of Korea 30(1), pp.41-53, 2011.

[51] World Nuclear News, “IAEA concludes lessons of Pelindaba break-in”, 28 January, 2008.

[52] NEI Nuclear Notes, “Exelon Terminates Wackenhut Security Contract at Peach Bottom Nuclear Power Plant”, 24 September, 2007.

[53] World Nuclear News, “Activists hack KHNP's computer systems”, 22 December, 2014.

[54] Nuclear Threat Initiative, “Nuclear Security Index 2014/2016”, NTI, 2016.

국문 요약서

핵안보는 평화적인 원자력 이용을 위한 큰 축의 하나이며, 핵안보 문화는 이를 강화하기 위한 효과적인 지렛대이다. 특히, 핵안보는 물리적 방호 및 보안사항 등을 포함하기 때문에 다른 국가와의 협력이 제한적일 수밖에 없다. 다만 핵안보 체제의 구축에 있어서 저변이 될 수 있는 국가, 기관, 개인의 핵안보 의식과 행동을 증진시키는 것이 중요하며, 이것이 핵안보 문화에 대한 논의가 제기되는 시작점이다.

핵안보 문화의 개념과 지침은 2008년 IAEA에 의해 제시된 후 많은 국가들로부터 그 중요성을 인정받았으나, 문화라는 복잡하고 추상적인 개념에 대한 평가에 어려움이 있다. 이에 원자력발전소 내 핵안보 문화를 평가하고 개선방안을 도출하기 위한 시스템 다이내믹스 기반의 평가모델을 개발하였다.

모델에 사용될 20개의 핵안보 문화 평가지표는 IAEA 핵안보 문화 지표를 기반으로 도출되었다. 평가 대상인 시설의 외부 요인으로는 정부의 핵안보 정책 수준, 규제기관과의 교류, 현장 외 기관과의 교류 등의 지표를 반영하였으며, 시설 내부 요인으로는 시설의 핵안보 정책 수준을 기반으로 크게 규정 및 절차, 업무 관리, 근무 환경, 교육 및 훈련, 의식 및 행동, 성과 측정에 대한 지표를 포함시켰다.

도출된 평가지표를 바탕으로 시스템 다이내믹스를 적용해 지표들의 동태적 역학관계를 분석하고자 핵안보 문화 인과지도(CLD)를 작성하였다. 원자력 안전 문화에 대한 선행연구를 기반으로 업무량과 스트레스, 학습 등을 중심으로 양과 음의 피드백 루프를 구성하였다. 또한 주요 모델요소들의 시간에 따른 변화 양상을 분석하기 위하여

저량/유량 흐름도(SFD)를 작성하였다. 모델의 시뮬레이션에 필요한 각 요소의 초기 값과 상관관계를 얻기 위해 한국수력원자력(주)의 임직원과 한국원자력통제기술원의 전문가를 대상으로 설문을 수행하였다. 설문 결과에 대한 신뢰성 분석, 타당성 분석, 회귀 분석 등의 통계 분석을 통해 결과의 신뢰성 및 타당성을 확보하고 필요한 입력 값들을 도출하였다.

보다 데이터를 명확하게 반영하기 위해 핵안보 업무 비율 0.2를 기준으로 핵안보 업무 종사자의 응답을 기반으로 한 모델 A와 핵안보 업무 비종사자의 응답을 기반으로 한 모델 B로 모델을 세분화하였다. 두 모델에 대해 핵안보 의식 및 행동이 일정한 수준을 유지하는 안정된 기본 시나리오를 구현하였으며, 이는 핵안보 문화 개선 방안들의 효과를 정량적으로 평가하는 기준선의 역할을 한다.

두 모델에 대한 민감도 분석을 위해 각 요소의 초기 값을 ±10%로 변화시켰을 때, 지도자 및 근무자의 핵안보 의식과 행동 수준이 변화하는 비율을 분석하였다. 그 결과, 핵안보 의식과 행동 모두 '핵안보 교육 및 훈련', '핵안보 교육 및 훈련 주기'와 '학습효과 감소율'의 변화에 따라 큰 영향을 받는다는 것을 확인할 수 있었다.

이를 바탕으로 시설 내 핵안보 문화를 증진하기 위한 방안으로 다음의 여섯 가지 시나리오가 선정되었다. ① 핵안보 정책 수준 향상, ② 핵안보 교육 및 훈련에 대한 투자 증대, ③ 핵안보 교육 및 훈련의 주기 단축, ④ 핵안보 교육 및 훈련의 품질 향상, ⑤ 규제기관과의 교류 증대, ⑥ 핵안보 자원 증대이다. 모델 A와 B의 시뮬레이션 결과를 통해 각 시나리오의 효과를 평가한 결과, 핵안보 업무 비종사자에 대해서도 충분한 핵안보 교육 및 훈련을 제공하여 핵안보 의식 및 행동을 높은 수준으로 유지하려는 노력이 필요함을 확인했다.

모델의 검증 단계로써 2015년 설문조사 데이터를 기반으로 도출된 모델요소 간의 관계식을 2014년 데이터와 비교하였다. 또한, 모델의 건전성을 확인하기 위해 입력 값으로 사용된 설문조사 데이터의 불확실성으로 인해 모델에서 출력되는 값이 갖게 되는 불확실성을 평가하였다.

본 연구는 핵안보 문화 평가모델 개발을 통해 핵안보 정책 방안의 문화적 영향에 대한 정량적인 분석 툴을 제공하였다. 이는 핵안보 문화의 저변 확대를 위한 기초 단계로써 원자력발전소 내 현재 상태를 진단하고 개선점을 도출하는 평가기반으로 활용될 수 있다.

주요어: 핵안보 문화, 조직문화 평가, 시스템 다이내믹스, 설문조사, 민감도 분석, 불확실성, 의사 결정 도구

학번: 2014-22722