Chapter 7

Integrated Risk Assessment of Safety, Security, and Safeguards

Mitsutoshi Suzuki

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.71522

Abstract

The peaceful use of nuclear energy has been pursued for more than half a century, and even after the catastrophic disaster at the Fukushima nuclear power plant in 2011, a new market in East Asia has been growing from the viewpoint of stable supply of nuclear energy. Countermeasures against malicious aircraft attacks have been introduced worldwide after the 9/11 terrorist attack in 2001 as synergies between safety and security. Although safeguards and security communities have different histories and technical aspects compared to safety, not only the mitigation plans as emergency preparedness but also a risk assessment as a supplement to the current requirements could be developed to promote synergism between safety, security, and safeguards (3S). The optimal installment of 3S countermeasures could be encouraged by a risk assessment to enhance reliability, robustness, and transparency of those facilities. One of the synergies of the integrated 3S risk assessment is a 3S by Design (3SBD) approach for new nuclear facilities. An introduction of 3SBD into the conceptual design stage increases regulatory effectiveness as well as operational efficiency and also reduces expensive and time-consuming retrofitting.

Keywords: probabilistic risk assessment (PRA), safety, security, and safeguards (3S), integrated risk assessment, 3S by design (3SBD), proliferation risk, sabotage risk

1. Introduction

After the Fukushima accident, the Nuclear Regulation Authority (NRA) in Japan developed the new safety standard, and soon after many utility companies submitted revised license applications to restart their nuclear power plants as soon as possible. Malicious aircraft attacks are considered in the standard, and mitigation plans are required to minimize possible consequences as synergies between safety and security in [1]. This time-consuming installment of

3S countermeasures could be encouraged by a risk assessment to enhance reliability, robustness, and transparency of the facilities as in [2].

The 3S initiative launched in 2008 emphasized on three (safety, security, and safeguards) of the 19 infrastructure elements of the Milestones in the Development of a National Infrastructure for Nuclear Power by IAEA as in [3]. One of the most apparent synergies is an adoption of 3SBD approach for new nuclear facilities. This benefit of the concept of 3SBD was pointed out recently in [4], and the Safeguards by Design (SBD) approach has been discussed extensively. The international safeguards has been implemented by the IAEA, and the IAEA has clear responsibility for the verification activities for the state's compliance with the NPT treaties and agreements, while their role in safety and security is limited on regulatory standardization. This means that there is not an obligatory authority governing safety and security regulations worldwide. Therefore, in order to achieve the 3SBD synergy, the realization of SBD approach with the IAEA and member states is challenging to achieve an international consensus in [5].

In addition to this, regarding institutional and technical issue for the internal and international regulators, a risk notion should be harmonized to be shared with the 3S authorities concerned. In safety, a frequency of accident is estimated from the past experienced data, and the accident sequence is analyzed with ETs/FTs, and the probabilistic assessment methodologies have been developed by the long historical trials and discussions. Because of the recent concern about nuclear security, the similar probabilistic assessment is extended to be used in the guideline against sabotage in nuclear security in [6]. The conventional vulnerability assessment in physical security has been well developed on a deterministic and prescriptive basis, on the

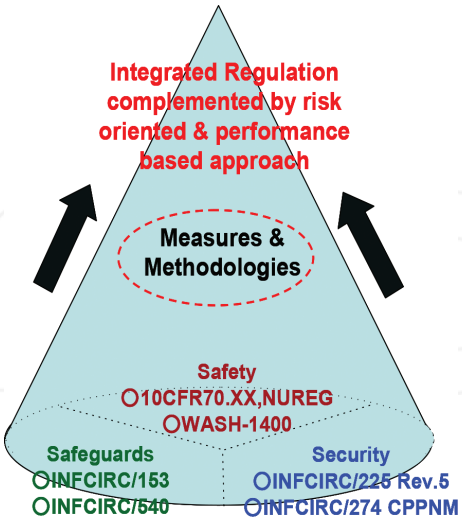


Figure 1. Integrated regulation by risk-informed and performance-based approach.

other hand, safeguards effectiveness is involved in proliferation resistance (PR) evaluation as extrinsic barriers, and a diversion pathway analysis is used to investigate a proliferation risk of nuclear cycles. Initial efforts for harmonization between reliability and safety and PR and physical protection (PP) are initiated under the Generation IV (GEN IV) international framework in [7]. In this regard, integrated measures and methodologies could be developed to evaluate an optimized balance between the 3S performance quantitatively as shown in **Figure 1**.

2. Mathematical model for 3S risk assessment

A major difficulty encountered in applying the probabilistic methods to safeguards is how to determine an initiation of diversion and misuse. In safeguards, the diversion of nuclear material and misuse of technology are induced by motivation of states and intentional acts of facility operator, so that estimating from historical incidences and predicting intentional human acts are generally very difficult. In comparison with the security, event sequence is analyzed probabilistically on a basis of the plant layout, system design, and structural robustness. Candidate tools for proliferation assessment were broadly investigated in [8]. As well-known international PR methodologies, Innovative Nuclear Reactors and Fuel Cycles (INPRO) program that was IAEA-led international project has developed the checklist approach, while the GEN IV's Proliferation Resistance and Physical Protection Working Group (PR&PP WG) has developed a risk-informed methodology in the qualitative and quantitative manner in [9]. To assess 3S risks, several mathematical tools are categorized to consider incident frequency and governing law resulting in the incidence shown in **Figure 2**.

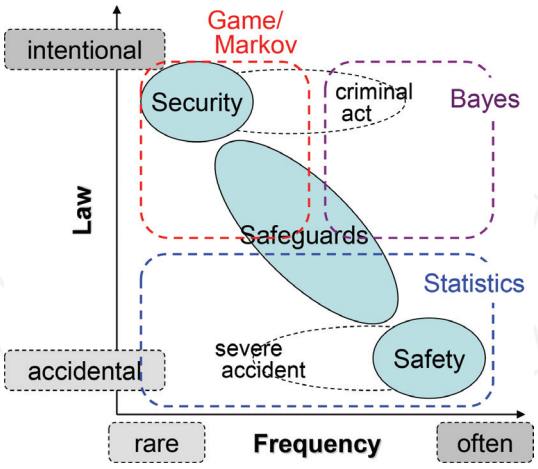


Figure 2. Mathematical models and assessment methodologies applied to safety, security, and safeguards (3S). The governing law and incidence frequency are selected to classify the inherent nature among the 3S incidences. The mapping of individual 3S region is drawn heuristically.

2.1. Probabilistic risk model in safeguards

Although the mathematical formalization for the international safeguards has been developed for several decades as in [10], the discussion of adopting probabilistic methodology to address nonproliferation issues was done in a different perspective in [11]. In safeguards, the estimation of intentional act leading to the diversion and misuse of nuclear material is generally very difficult. In addition to the incidence probability, there is another uncertainty related to measurement error in material accounting. This is the significant quantity (SQ) and timeliness goal that underline the basis for nuclear material accountancy (NMA). Based on the prescriptive and deterministic logic, uncertainty of NMA should be controlled under this limit as a first priority in safeguards. The IAEA determined the threshold value for nuclear material losses for each type of facility and process. However, as an amount of nuclear material increases in large-scale facilities, uncertainty due to measurement error becomes large and likely exceeds the limit. Because it is important to control the measurement error within the absolute threshold of NMA, a probability distribution of the measurement error of NMA has to be considered in conjunction with the incidence probability as shown in **Figure 3**.

The two-dimensional probability formalization is proposed as in the Eq. (1) as follows in [12, 13]:

$$R = P \times C = P(t, m) \times C = P(t) \times P(m \mid t) \times C \tag{1}$$

In the Eq. (1), the measurement error probability is defined as ($P(m)$) related to measurement uncertainty in material accounting. The measurement error probability is expressed as the probability density function in the measurement error axis in **Figure 3**. The accumulated distribution function leads to the detection probability. On the other hand, the incidence probability is defined as a Poisson density function under an assumption of random occurrence of diversion incidence. It should be noted that both probabilities are not independent and those would be closely correlated each other because of the inherent nature of intentional acts.

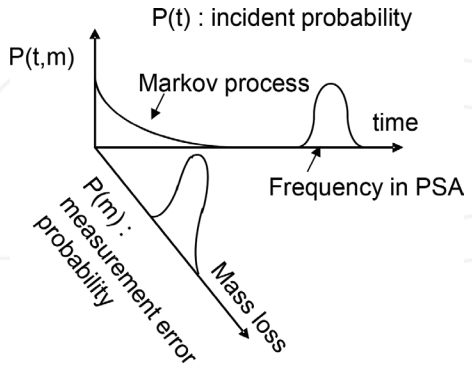


Figure 3. Two-dimensional probability for safeguards. The probability distribution composed of two random variables, the incidence time and the measurement error, is a characteristic feature of the proliferation risk.

2.2. Probabilistic risk model in security

In safety, Probabilistic Safety Analysis (PSA) has been developed by the long historical trials and discussions. This approach is to estimate the frequencies of accidents and failures from the historical data and to analyze the accident sequence with ETs/FTs based on these parameters. Because of the recent concern about nuclear security, similar probabilistic assessment was extended for use in developing guidelines for protection of nuclear power plants against sabotage in [14]. Although the conventional vulnerability assessment in physical security has been well developed on a deterministic and prescriptive basis, an inherent difficulty in determining the frequency of terrorist attack by malicious acts is undertaken by the conservative estimate. The risk formalization in security is expressed as in the Eq. (2) in [15]:

$$\mathrm{R} = P_A \times (1 - P_E) \times C = P_A \times (1 - P_I \times P_N) \times C \tag{2}$$

where (P_A) is the incidence probability, (P_E) the performance probability, (P_I) the interruption probability, (P_N) the neutralization probability, and (C) the consequence, respectively. Because of the difficulty of specifying the incidence probability, the security system is usually evaluated by the performance probability in which the timeline analysis is performed to identify the interruption probability and the security countermeasures; fence, sensor, camera, and so on are designed and installed into actual nuclear facilities. The neutralization probability is the unique feature of the security risk assessment and is determined by the performance of the response force. In addition to this, the deterrence effect can be estimated with a Bayesian method utilizing historical data, the game method assuming rational behavior and payoff matrix, and others, and the incidence probability could be evaluated qualitatively as in the decision process in [16].

Especially in the security risk study, sabotage risk is defined by taking the product of the frequency of sabotage incidence and the magnitude of consequences. Although it is difficult to estimate the initiation frequency, the risk can be described using the conditional probability and the magnitude of consequence as follows in [17]:

$$R_j = \pi_j p_j c \tag{3}$$

R_j = The risk due to sequence j leading to consequence, π_j = The probability that an adversary will attempt to complete sequence j, p_j = The conditional probability of success of causing consequence given attempt of sequence j, c = The magnitude of consequence.

For certain sabotage attacks, it is assumed that it is possible to identify well-defined sabotage sequences leading to consequence. In addition, a sequence is a cut set of a sabotage fault tree equation and does not necessarily imply a particular time order because a saboteur might attack the fault tree components in an intentional way.

Considering all sequence levels, the total risk, R, is expressed as follows:

$$R = \sum_{j=1}^{\mu} \pi_j p_j c = c \sum_{j=1}^{\mu} \pi_j P_{DC_j} \prod_{k=1}^{\eta_j} q_{jk} \quad (4)$$

μ = The number of sequences leading to consequence, P_{DCj} = The probability of release reduction by the damage control measures, q_{jk} = The probability of completion of the k^{th} event in sequence j, η_j = The number of discrete events in sequence j.

The three categories of measures, which are physical protection, damage control, and plant layout design, provide protection against radiological sabotage. The physical protection measures have been regulated; however, the other two measures are not fully discussed. In order to investigate the effect of damage control and plant layout design on the sabotage protection, the probability of release reduction by damage control measures, P_{DCj}, and the probability of completion of event sequence, q_{jk} , are important.

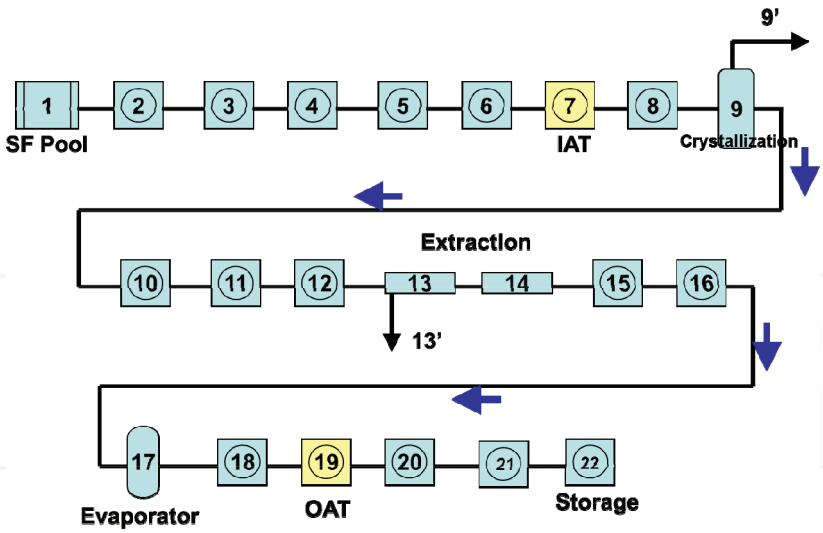
3. Case study of individual risk analysis

3.1. Probabilistic risk analysis (PRA) in safety

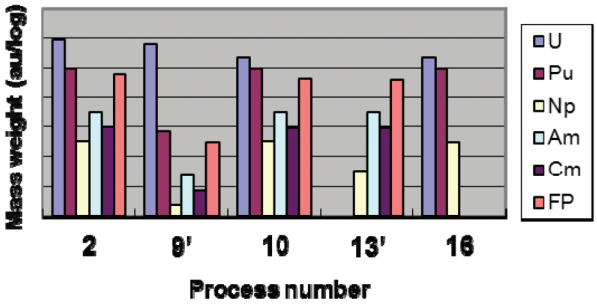
The terminology, PSA, has been used in nuclear engineering field in Japan to introduce probabilistic risk analysis (PRA) that has been fully developed in safety assessment of nuclear power plant worldwide. According to the unique history of the introduction of PSA, the case study of PSA in safety is shown as the PRA study.

In the advanced fuel cycle project, Japan Atomic Energy Agency (JAEA) studied fast breeder reactor (FBR), advanced aqueous reprocessing, and fuel fabrication technologies. The details of these technologies have not been developed yet. However, a conceptual design of the advanced aqueous reprocessing process is used for safety risk study as shown in **Figure 4** as in [12, 13]. In this diagram, some challenging technologies and revolutionary instruments are included, and further development should be needed to proceed to engineering phase. After measuring the input plutonium amount at input accountability tank, most of uranium is removed at the crystallization process indicated as no. 9, and the remaining solution is adjusted to be treated correctly at the extraction process as nos. 13 and 14. Fission product and minor actinide are extracted at the extraction process. After the extraction process, the separated plutonium is always accompanied by uranium, and plutonium does not exist solely in the entire process. Through the evaporator output plutonium is measured at output accountability tank, and the mixture of plutonium and uranium is stored as reprocessed product. Several innovative technologies have been investigated in the FBR project. And in this feasibility study, as a typical FBR reprocessing process, the process throughput is assumed to be 200 ton-HM/year for spent fuel from FBR that is approximately corresponding to 18 ton-Pu/year, and the process is to be operated during 200 days/year.

Using PSA methodology, the risk for radioactive material release and damage to public health is estimated based on failure data of instruments and associated reference values in [6]. Severe



(a) Diagram of advanced aqueous reprocessing process



(b) Mass weight content of TRU and FPs at some processes

Figure 4. Diagram of advanced aqueous reprocessing process. Spent fuels discharged from fast breeder reactor are stripped to remove the uranium contents at the crystallization, no. 9, and extracted to remove the minor actinide contents using centrifugal extraction machines.

accident that would cause release of radioactive material is evaluated with expert judgment. With an assumption of multiple failures of instruments and human error, some important scenarios are selected as follows:

- *Scenario 1*: At the outlet piping of the extraction process, plutonium is leaked into high active liquid waste (HALW) tank, because a shape of the HALW tank is not manufactured to avoid criticality and then a critical accident is induced.
- *Scenario 2*: After removing americium (Am), curium (Cm), and fission product (FP) into raffinate component at the extraction process, Am and Cm are recovered using chromatography

technique into minor actinide (MA) tank. At that time, MA is leaked from the outlet piping of MA tank, and then the leaked waste solution is boiled.

- *Scenario 3*: The coolant system is broken down due to a pump failure, and then self-heat-generation source tanks, HALW and MA tanks, are boiled. Radioactive solution materials are evaporated. After chocking and destructing high efficiency performance air (HEPA) filter, those effluents are discharged into outside.
- *Scenario 4*: Organic solvent is very volatile and is leaked from the outlet piping of the extraction process, and then fire accident is induced.

After specifying important factors and making an ET for success and/or failure branches, an accident sequence is decided. Moreover the incident frequency is estimated with a FT and instrumental data, and the total probability for the sequence is calculated. The assessment result is shown in **Figure 5**. Even in the worst case scenario 2, the estimated risk is still two orders lower than the safety target that is a design goal in the FaCT project.

3.2. PRA in safeguards

As the case study of the risk analysis in safeguards, the proliferation risk assessment that is applied to reprocessing process is described in this section. General description of large aqueous and PUREX process model is shown in **Table 1**. These process parameters are assumed to represent characteristics of large PUREX commercial plant and do not contain any proprietary information and sensitive technologies. They are simply decided to perform a preliminary investigation on this study while maintaining characteristics of large commercial reprocessing plant.

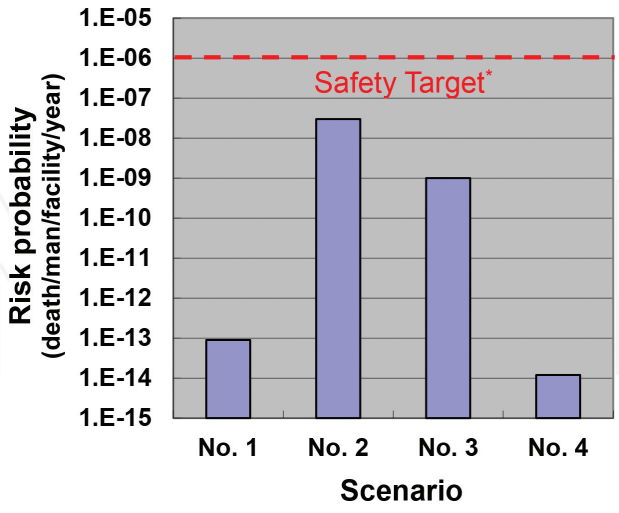


Figure 5. Probabilistic safety assessment for possible accident scenario. The safety target is decided to be 1×10^{-6} (death/man/facility/year).

Throughput (t/year)	800
(tPu/year)	7
Input (batch/day)	~ 1b/day
(gPu/L)	~ 3
Product (batch/day)	1b/5 days
(gPu/L)	250
Inventory (kg-Pu)	~400
Working days	200

Table 1. Typical parameters in a large reprocessing plant.

The schematics of the process components are shown in **Figure 6**. These are composed of adjusting and input accountability, extraction and partition, and plutonium purification and concentration processes. The annual throughput is 800 ton-HM/y, and the working days per year are 200 days. In a steady-state operation, about 40 kg-Pu is a daily throughput, and plutonium inventory of the entire process is around 400 kg-Pu. It should be noted again that the model lacks the proprietary information. This is constructed from general PUREX specification and does not include design and performance information of dissolver, extraction process, and other sensitive technologies.

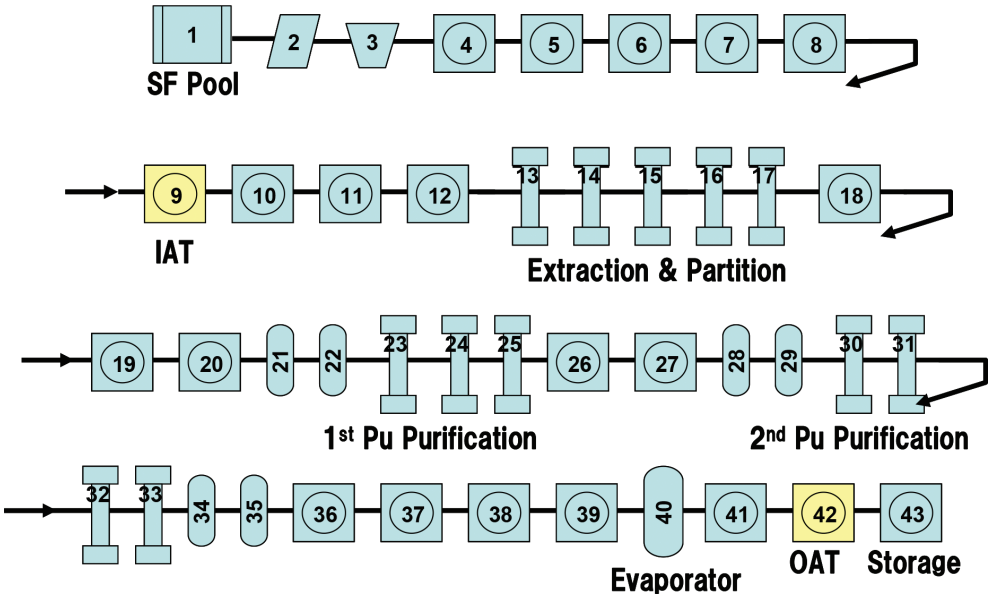


Figure 6. Schematics of PUREX reprocessing process.

In order to investigate adaptability of risk notion in a PUREX reprocessing process, PRA is carried out using the Markov model developed by the PR&PP WG. The PR&PP WG has also discussed the safeguard ability of an installation, defined as the degree to which a system can be put with effectiveness and efficiency under international safeguards, and the attributes have been defined for its characterizations. One of the evaluation methodologies has clearly noted for the notion of proliferation risk with assuming the Markov process model, and the proliferation risk analysis directly indicates the vulnerable diversion path instead of an expert elicitation.

As shown in **Figure 7**, the Markov process model is applied to the PUREX process to perform proliferation risk analysis, and in addition to the extrinsic effects by safeguards

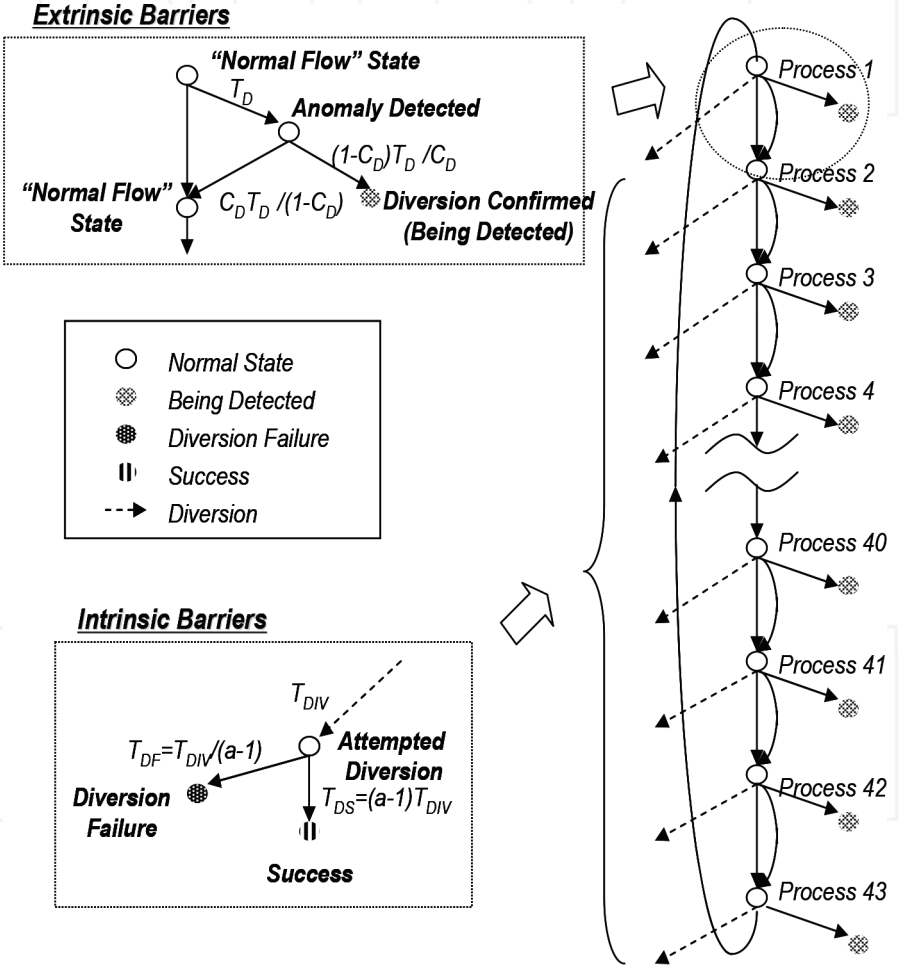


Figure 7. Markov model for proliferation risk analysis. Both extrinsic effects and intrinsic barriers are considered in the model. The extrinsic effect is modeled for safeguards implementation and the intrinsic barriers are for material difficulty due to radiation exposure and high temperature.

implementation, characterized by "T_D" and "$C_{D,}$" the intrinsic effects by radiation strength in materials, by "a," are considered as technical difficulty. Dip tubes for the solution monitoring system is installed in the 82 tanks in Rokkasho Reprocessing Plant (RRP) and can be used as in-line level and density monitoring. While the solution monitoring can generate real-time signals of the solution, the sensitivity should depend on not only performance of pattern recognition algorithm but also meaningless background by sampling, homogenization, evaporation, and so on. The solution monitoring sensitivity is considered according to the process steps with an assumption that the plutonium concentration would determine the detection capability of the solution level change corresponding to 1 SQ (= 8 kg-Pu). Both the extrinsic effects of safeguards implementation and the intrinsic barriers by radiation from residuals are also considered to evaluate a proliferation risk in the reprocessing process. As shown in **Figure 8**, the detection probability at the process number 1, spent fuel pond, shows the largest probability due to the residence time. The success probability increases clearly after the process number 34, downstream from the second purification process, and especially after the number 40, evaporator, due to high concentration of plutonium as well as low radioactivity in [18].

Although the proliferation is caused by intentional acts, it is assumed that a Poisson process, which is based on random incidence and is a theoretical background of the Markov model, could be applied to the risk analysis in the reprocessing. It is not yet applied to classical safeguards because PRA is not yet a quantitative safeguards component. In addition, measurement error probability in nuclear material accounting should be considered simultaneously with the incident probability that is a key component in the Markov model.

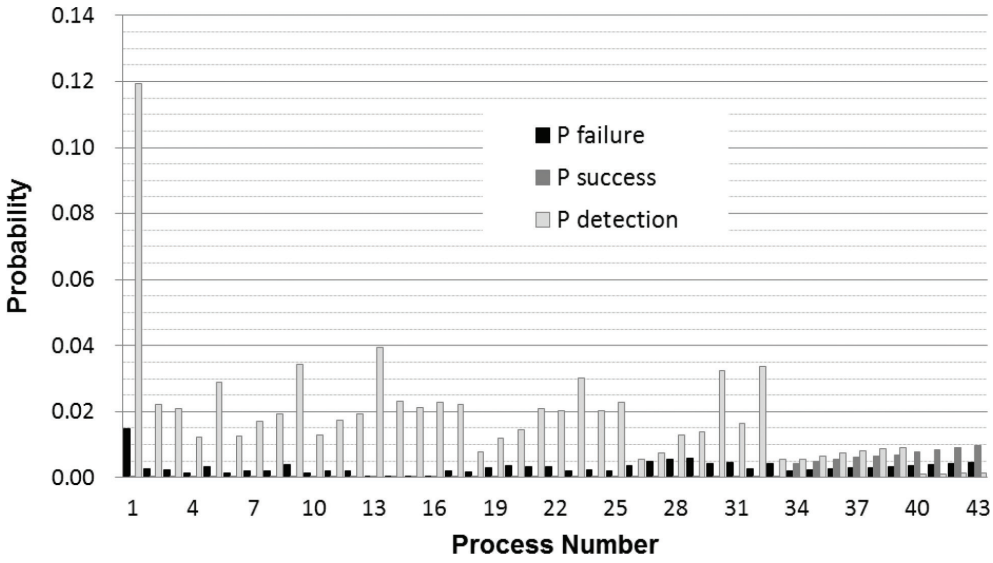


Figure 8. According to the individual process numbers, the detection, failure, and success probabilities are shown. A typical PUREX process is assumed to be composed of the 43 different processes: pool, dissolution, extraction, purification, evaporation, and storage.

3.3. PRA in security

In this case study, firstly, the Markov approach is applied to the sabotage risk assessment, and the Bayes updating is used to estimate the incident probability. And finally, the risk is considered with taking into account the sabotage sequences.

3.3.1. Markov model approach

In **Figure 9**, the sabotage pathway of hypothetical nuclear reactor is shown. This example scenario represents a sabotage of nuclear reactor at full power operation by disabling decay heat removal function of the reactor, and the decay heat removal can be performed either by destroying coolant loop or failing the sea water circulation. It is assumed that this sabotage scenario is carried out by a conventional strategy such as unauthorized intrusion. And this unauthorized intrusion is defined as design basis threat (DBT) for physical protection system

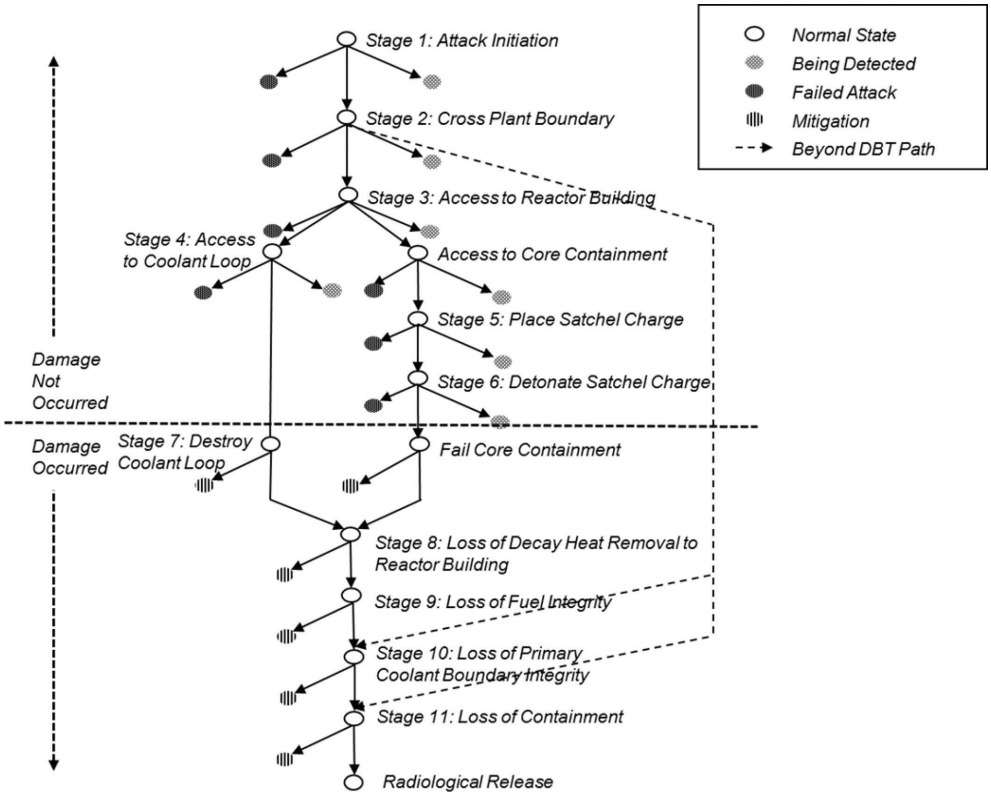


Figure 9. Sabotage pathway to radiological release of nuclear power reactor. The Markov model is used to model this sabotage pathway analysis. An intrusion attack is assumed as DBT, and a standoff stack is as beyond DBT.

in this hypothetical nuclear reactor. In addition, a standoff attack scenario is considered as a typical example of beyond DBT. In the beyond DBT, standoff attacks are performed to fail the primary coolant boundary integrity and containment integrity, and the serious consequences result in radiological release to the atmosphere.

In this security risk evaluation, two sabotage scenarios for nuclear power plants are considered. As the DBT, an intrusion incidence is investigated in the case (a), and terrorists attempt to overcome physical barriers and to destroy a reactor building using explosives. In the case (b), a standoff attack is modeled, and aircraft and/or missile attacks are assumed as beyond DBT. The failure, mitigation, detection, and success probabilities are calculated according to the elapsed time shown in **Figure 10**. It is understood that the detection probability is very high, and the success probability is very low in the case (a). This means that physical protection system perform efficiently for the DBT scenario. On the contrary, the mitigation and success probabilities increase gradually in accordance with fuel melting in the case (b). This indicates that the physical protection system does not work well in the case of beyond DBT and mitigation plans are important to minimize the consequence. Therefore, it is understood that a good cooperation between facility operator and national response authority is essential to mitigate the consequence against the sabotage attack.

3.3.2. Bayes updating

To compare the risk representation in security with that in safety, an incidence probability is roughly estimated with the Bayes updating using past 17 data taken from global terrorism incidences against nuclear power plant in the world from 1972 to 2007 as shown in **Figure 11** as in [19].

In the Bayes updating, the prior probability distribution is assumed to be a gamma distribution, and the most updated mean value of the probability is about 4×10^{-2} (1/the number of global NPPs/year). This is about 10^{-4}(1/year) for individual nuclear power plant.

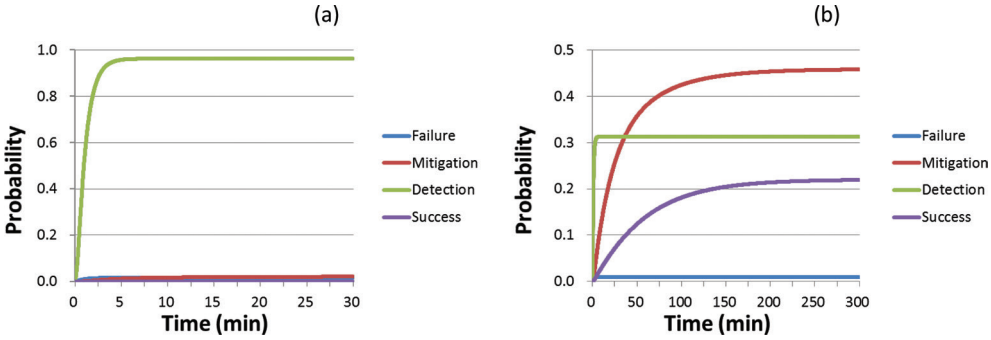


Figure 10. The failure, mitigation, detection, and success probabilities are calculated according to the elapsed time from an incidence. In the case (a), sabotage by an intrusion is assumed as design-based threat (DBT), and aircraft and/or missile attacks are assumed as beyond DBT in the case (b).

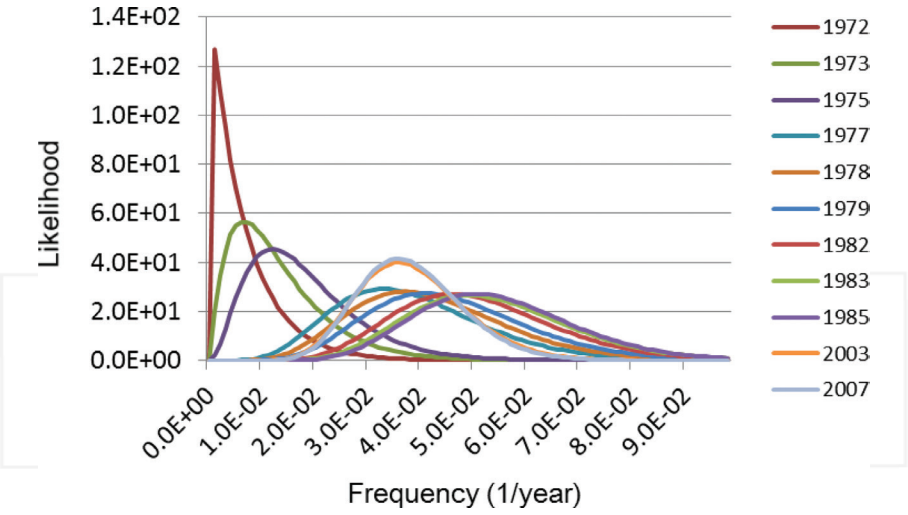


Figure 11. Incident probability is roughly estimated by Bayes updating. Experienced 17 data taken from past terrorism incidences in the world from 1972 to 2007 are used.

3.3.3. Sabotage sequence analysis

A loss of offsite power (LOOP) is the typical case scenario in the sabotage protection study because of its vulnerability of the offsite power source and transmission line. In addition, a loss of onsite power by emergency diesel generator (EDG) is assumed because of the new safety regulation considering the Tsunami in the Fukushima accident. All these sabotage sequences including a reactor cooling by auxiliary feed water (AFW), breeding steam into containment vessel (CV), and loss of all direct current (DC) and alternate current (AC) power are shown. In order to investigate an effect of damage control design, five design changes cited from reference [20] and emergency power source are included into the event sequence as in **Figure 12**.

In order to evaluate an effect of the design change, the number of target sets is shown in bar charts as histograms in **Figure 13**. The horizontal position of each bar corresponds to the vulnerability derived from the individual target element. The vulnerability is shown as the polyline in the same figure. In the reference case, the hollow bars are seen around the high vulnerability region, the left-hand side in the figure, and the number of elements is 1 or 2. The cumulative number of the target sets is not so large; however, these target sets should be very vulnerable for the sabotage protection. On the contrary, considering the design change, the cumulative number of the target sets is large, but those vulnerabilities are very low. This does not mean that the target sets with the design change are vulnerable.

The sabotage risk in Eq. (3), which is proportional to a summation of the multiplication of the number of target set and the vulnerability, is shown as a function of the number of elements in the target set with and without the design change in **Figure 14**. The number of element

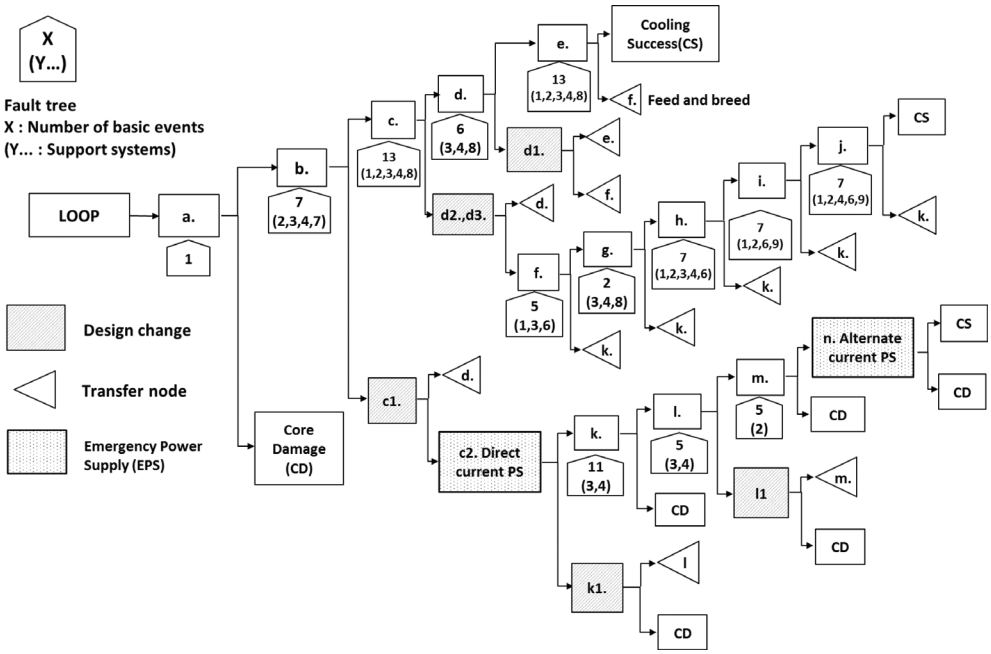


Figure 12. The name of heading and that of the design change in the event tree and all fault trees are abbreviated due to security concerns.

constituting the target set changes in the range of 1–3, and the effect of design change for damage control is shown. The total risk in all cases, regardless of the number of element, is reduced by considering the design change for damage control. It is verified that the built-in measures are effective and resistant compared to the emergency equipment placed outdoors. The movable equipment is flexible and resilient measure in accident management. It should be noted, however, that the equipment has to be used properly as the defense-in-depth (DiD) measures due to the possible adversary's interference.

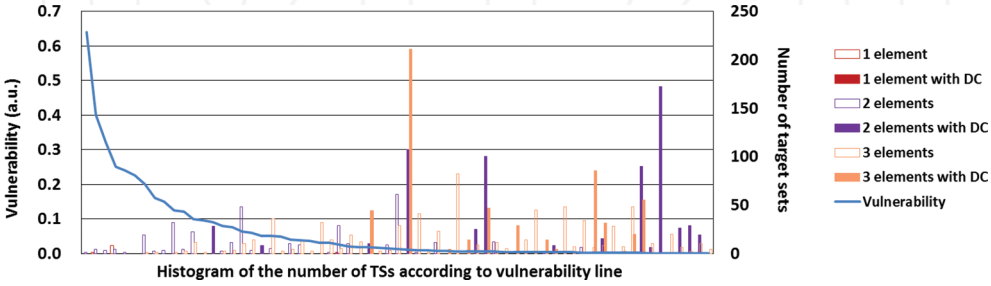


Figure 13. The number of target set (TS) and the vulnerability with and without the design change (DC).

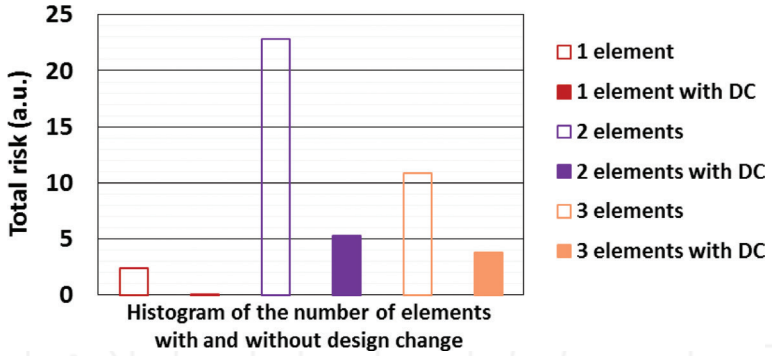


Figure 14. Reduction of total risk due to the design change (DC).

4. Prospect of integrated risk analysis

The PRA is an important method to evaluate equality in cost-effectiveness (CE) among 3S countermeasures, and quantification of risk in safeguards and security is always a challenge. The safety CE can be calculated by Eq. (5). And the frequency and damage cost in Eq. (5) have been well investigated. For the security CE, the incidence probability can be roughly estimated as shown in the previous section, and the damage cost can be evaluated according the individual scenario. On the contrary, for the safeguards CE, there is no method to estimate the incidence of diversion and/or misuse:

$$Safety\ CE\ =\ Frequency\left(\frac{1}{\frac{NPPs}{year}}\right)\times DamageCost\ (\$) \tag{5}$$

$$Safeguards\ CE\ =\ Unknown\times DamageCost\ (\$) \tag{6}$$

$$Security\ CE\ =\ Rough\ Estimation\left(\frac{1}{\frac{NPPs}{year}}\right)\times DamageCost\ (\$) \tag{7}$$

This is a current status toward the integrated 3S risk evaluation trial. However, the balanced management in resource allotment is highly appreciated to introduce nuclear energy in full compliance with international regimes as well as in a cost-effective manner. An integrated management system based on the quantitative risk evaluation would be the future research area in nuclear engineering field.

PRA in safeguards and security has been evolving and applying to the promotion of 3SBD activities. However, the theoretical basis is diverse, and the effectiveness of PRA in these areas has not been clearly demonstrated yet. Not only for an advanced instrument but also for risk-informed installation, it is shown that the Markov model approach is a good example of Safeguards by

Design activities. The model is applied to PRA with the PUREX model, and it is clearly demonstrated that the vulnerable path in the PUREX process is safeguarded by the solution monitoring (SM) originally installed based on the expert elicitation. The recent study on SM is the uncertainty analysis to optimize the safeguards measures with the trade-off relation between the safeguards performance due to measurement error and the economical consideration as increasing the throughput in the advanced reprocessing process. Both the harsh circumstances with the residual MA and FPs and the increase of measurement uncertainty due to the large throughput support more NDA installment than DA with considering the initial and running cost of those measures.

The probabilistic risk methodologies in security have been developing, and the inherent difficulties due to intentional acts are still challenges. However, the Markov model, the Bayes updating, and the sabotage sequence analysis could be applicable to the decision problems in security. In fact, the sabotage scenario analysis using vital area identification methodology has been used to increase an effectiveness of sabotage protection in nuclear power plants. And the sabotage logic trees that have been originally developed as ETs/FTs in the safety PRA are used for the security protection.

Finally, integrating the PSA in safety as the risk assessment techniques with the PRA in safeguards and security would have a potential to be fascinated by the younger generation, and the comprehensive 3S regulation based on the qualitative and quantitative risk discussion should be transparent and persuasive for a reasonable approach in the mandatory 3S implementation.

Author details

Mitsutoshi Suzuki

Address all correspondence to: suzuki.mitsutoshi@jaea.go.jp

Integrated Support Center for Nuclear Nonproliferation and Nuclear Security, Atomic Energy Agency, Japan

References

[1] Outline of New Regulatory Requirements For Light Water Nuclear Power Plants (Severe Accident Measures), April 3, 2013. http://www.nsr.go.jp/data/000067119.pdf

[2] Suzuki M, Izumi Y, Kimoto T, Naoi Y, Inoue T, Hoffheins B. Investigating 3S Synergies to Support Infrastructure Development and Risk-Informed Methodologies for 3S by Design. Vienna Austria: IAEA-CN-184/64, IAEA safeguards symposium; 2010. Nov. 1–Nov. 5

[3] IAEA Nuclear Energy Series, No. NG-G-3.1, Milestones in the Development of a National Infrastructure for Nuclear Power, Vienna: IAEA; 2007

[4] Stein M, *et al*. Safety, security, and safeguards by design – An industrial approach, proceedings of global 2009, Paris, France; Sep, 2009. 6-11

[5] Suzuki M, Burr T, Howell J. Risk-informed approach for safety, safeguards, and security (3S) by design, ICONE19-43154, 19th international conference on nuclear engineering. Vol. 16-19. Chiba, Japan. May, 2011

[6] Kurisaka K, Kubo S, Kamiyama K, Niwa H. Comprehensive Safety Examination of Commercialized Fast Reactor Cycle Systems – Examination of Safety Development Target and Risk Analysis of the Aqueous Fuel Cycle Systems-, JNC TN9400 2002-031, 2002

[7] Yue M, Cheng LY, Bari R. A Markov model approach to proliferation-resistance assessment of nuclear energy systems, Nuclear Technology. 2008;**162**(26):28-44

[8] Suzuki M, Terao N. Solution Monitoring Evaluated by Proliferation Riks Assessment and Fuzzy Optimization Analysis for Safeguards in a Reprocessing Process, Science and Technology of Nuclear Installations. Vol. 2013, Hindawi; 2013

[9] Gen IV International Forum, PR-PP Expert Group, Evaluation Methodology for Proliferation Resistance and Physical Protection, Rev. 5, GIF/PRPPWG/2006/005, OECD, November 30, 2006

[10] Cobb D. Sequential tests for near-real-time accounting, INMM Proceedings; 1981. pp. 62-70

[11] Avenhaus R, Canty MJ. Formal models for NPT safeguards, Journal of Nuclear Material Management. 2007;**354**:69-76

[12] Suzuki M, Burr T, Howell J. Risk-informed approach for safety, safeguards, and security (3S) by design, ICONE19-43154, proceedings of ICONE19. Chiba, Japan: 19th International Conference on Nuclear Engineering, May 16-19, 2011

[13] Suzuki M, Demuth S. Proliferation Risk Assessment for Large Reprocessing Facilities with Simulation and Modeling, Paper 399247, Proceedings of Global 2011, Chiba, Japan, December 16-11-2011

[14] "Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage", IAEA Nuclear Security Series No.4. Vienna: Technical Guidance, IAEA; 2007

[15] Sandia National Laboratories Security Risk Assessment Methodologies. Available from: http://www.sandia.gov/ram/RAM-CI.html

[16] Kardes E, Hall R. Survey of literature on strategic decision making in the presence of adversaries, CREATE Report, March 15; 2005

[17] Ericson DM, Bruce Varnado G. Nuclear power plant design concepts for sabotage protection, NUREG/CR-1345, SAND80-0477/1, 1981

[18] Suzuki M, Howell J, Burr T, Demuth S. Proposal of Proof-of-Principle Study on Aqueous Reprocessing Facility, IAEA CRP meeting; 2012

[19] Steinhausler F. Countering Security Risks to Nuclear Power Plants, Jeddah: International Symposium on the Peaceful Applications of Nuclear Technology in the GCC countries; 2008

[20] Lobner P. Nuclear Power Plant Damage Control Measures and Design Changes for Sabotage Protection, NUREG/CR-2585, SAND82-7011, 1982

INTECH