Spent fuel reprocessing system security engineering capability maturity model

LIU Ya-chun[1,2,3], ZOU Shu-liang[1,2] ,YANG Xiao-hua[4], OUYANG Zi-gen[2,3], and DAI Jian-yong[2]

1.College of Nuclear Science and Technology, University of South China, Hengyang 421001, China (liuyachun65@yahoo.com.cn)
2. Nuclear Economy and Management Research Center, University of South China, Hengyang 421001, China
3. College of Mathematics and Physics, University of South China, Hengyang 421001, China
4. College of Computer Science and Technology, University of South China, Hengyang 421001, China

Abstract: In the field of nuclear safety, traditional work places extra emphasis on risk assessment related to technical skills, production operations, accident consequences through deterministic or probabilistic analysis, and on the basis of which risk management and control are implemented. However, high quality of product does not necessarily mean good safety quality, which implies a predictable degree of uniformity and dependability suited to the specific security needs. In this paper, we make use of the system security engineering - capability maturity model (SSE-CMM) in the field of spent fuel reprocessing, establish a spent fuel reprocessing systems security engineering capability maturity model (SFR-SSE-CMM). The base practices in the model are collected from the materials of the practice of the nuclear safety engineering, which represent the best security implementation activities, reflect the regular and basic work of the implementation of the security engineering in the spent fuel reprocessing plant, the general practices reveal the management, measurement and institutional characteristics of all process activities. The basic principles that should be followed in the course of implementation of safety engineering activities are indicated from "what" and "how" aspects. The model provides a standardized framework and evaluation system for the safety engineering of the spent fuel reprocessing system. As a supplement to traditional methods, this new assessment technique with property of repeatability and predictability with respect to cost, procedure and quality control, can make or improve the activities of security engineering to become a serial of mature, measurable and standard activities.
Key words: spent fuel reprocessing; system security engineering; process ability; maturity degree

1 Introduction

In nuclear safety engineering, deterministic methods have been applied by the pro-conservative assumption for the computation of safety features. When a large nuclear installation deviates from its normal condition, the system can be brought back to a controllable status, or the consequences of an accident can be limited to an acceptable degree. With the publication of WASH-1400[1], especially after the TMI accident, the US Nuclear Regulatory Commission (NRC) decided to carry out further research in probing into the probability of initial events and failure modes by means of probabilistic safety analysis (PSA). They analyzed the interplay among several systems, and assessed various hypothetical accident scenarios as well as their effect on overall engineering safety standards by means of factual rather than pro-conservative computation modules together with system, equipment and human reliability data collected in the course of design, construction, debugging, operation and maintenance. In recent years, the American Nuclear Society (ANS) and the International Atomic Energy Agency (IAEA) applied the risk analysis method to safety management decision-making and gradually incorporated it into the system of nuclear safety regulations [2-4].

The combination of probability theory, the deterministic method and the correct engineering judgments provide a strong guarantee for the design and implementation of nuclear safety engineering projects. However, the design, operation, maintenance and assessment of safety engineering rely heavily on the relation between personnel and techniques. Modern statistical process control theory shows that product quality to a large extent depends on the maturity of the production process [5, 6]. From 1993 to 2003, thanks to the support of the U.S.

Received date: July 28, 2010
(Revised date: November 14, 2010)

National Security Agency (NSA), the U.S. Department of Defense, and Canada's Communications Security Bureau, after the joint efforts of dozens of companies, the system safety engineering capability maturity model (SSE-CMM 3.0) geared to process capability assessment came into being and developed into the general method and international standard for developed western countries to organize and implement the safety engineering process. In recent years, it was applied to China's information security and other risk control fields [7-12].

The present paper intends to combine knowledge about SSE-CMM and the spent fuel reprocessing system in order to build a security engineering capability maturity model for spent fuel reprocessing systems (hereafter abbreviated as SFR-SSE-CMM), which will offer a new way to evaluate and improve safety of the spent fuel reprocessing system from the perspective of maturing process capability and serve as a useful complement to the traditional method.

2The basic ideas and structural features of the SSE-CMM

2.1 Overview of security engineering process

All successful companies share the same feature: a set of strictly defined, well managed, and measurable work procedures. The CMM model integrates the idea that accompanies with maturity of high capability can continually turn out high quality products while limiting the engineering risks to a low level. The SSE-CMM[6] abstracted the system safety engineering task into eleven sub-tasks with salient features. The engineering practice required in the accomplishment of each sub-task is referred to as a process area. The SSE-CMM divides the 11 process areas into 3 categories: the risk process area, the engineering process area and the assurance process area. The security engineering process works with the other engineering disciplines to determine and implement solutions to the problems presented by the dangers. Finally, the assurance process establishes confidence in the security solutions and conveys this confidence to insiders. The hierarchy and logical relationships between the three basic process areas are illustrated by Figs. 1 to 4.

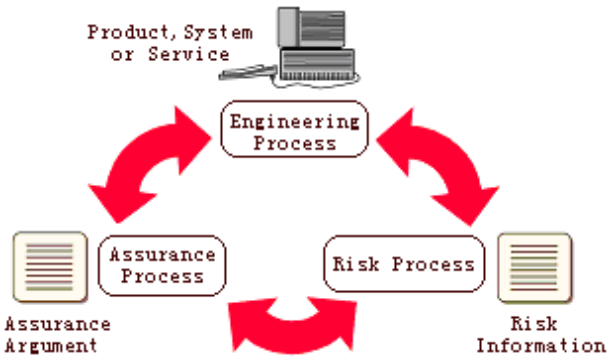

Fig. 1 Three basic areas of the security engineering process.

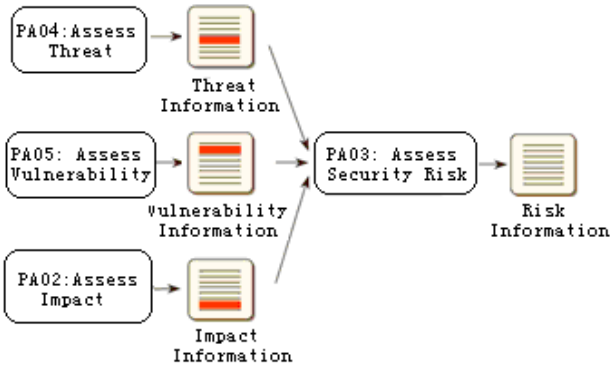

Fig. 2 The risk area includes threats, vulnerabilities and impact.

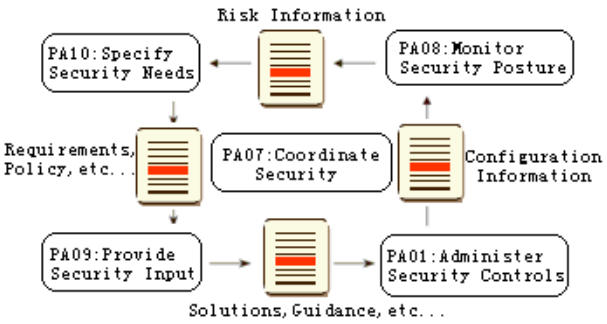

Fig. 3 Components of the engineering process area.

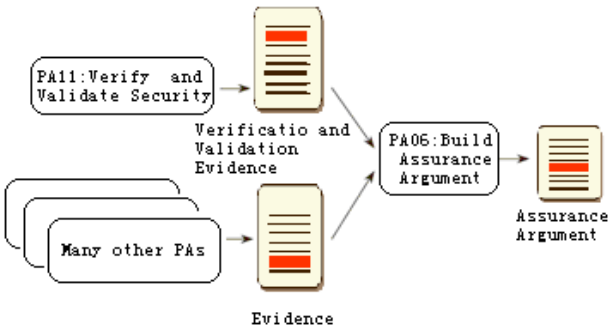

Fig. 4 The assurance process builds confidence in the solutions.

2.2 Determining the capability level for each process areas

As shown in Table 1, the SSE-CMM architecture is designed to determine a security engineering organization's process maturity across the breadth of security engineering. The goal of the architecture is to clearly separate basic characteristics of the security engineering process from its management and institutionalization characteristics. In order to ensure this separation, the model has two dimensions, which are called "domain" and "capability" dimension respectively. The domain dimension simply consists of all the practices that collectively define security engineering. These practices are called "base practices." The capability dimension represents practices that indicate process management and institutionalization capability. These practices are called "generic practices" as they apply across a wide range of domains. The generic practices represent activities that should be performed as part of doing a base practices.

The domain dimension simply consists of 61 "base practices" (BP) that collectively defines the security engineering process areas PA01 to PA11. For example, PA04 threat assessment involves 6 base practices (BP), namely, BP.04.01 "identify natural threats", BP.04.02 "identify man-made threats", BP.04.03 "identify threat units of measure", BP.04.04 "assess threat agent capability", BP.04.05 "assess threat likelihood", and BP.04.06 "monitor threats and their characteristics". The generic practices are used in a process appraisal to determine the capability of a process. Each capability level is identified and distinguished by a set of common features, each of which is described by a set of generic practices. A total of 29 generic practices are subordinated to the logical areas of 12 common features (CF), which belong to 5 different capability levels. The latter are in order of increasing ability level: (1) Performed informally, (2) Planned and tracked, (3) well defined, (4) Quantitatively controlled, and (5) Continuously improving. An organization with low capability would experience wide variations in achieving cost, schedule, functionality, and quality targets.

Table 1 Model structure and usage

5	CF5.2	GP.5.2.3				
		GP.5.2.2				
		GP.5.2.1				
	CF5.1	GP.5.1.1				
		GP.5.1.1				
4	CF4.2	GP.4.2.2				
		GP.4.2.1				
	CF4.1	GP.4.1.1				
3	CF3.3	GP.3.3.3				
		GP.3.3.2				
		GP.3.3.1				
	CF3.2	GP.3.2.1				
		GP.3.2.1				
		GP.3.2.1				
	CF3.1	GP.3.1.2				
		GP.3.1.1				
2	CF2.4	GP.2.4.2	√			
		GP.2.4.1				
	CF2.3	GP.2.3.2				
		GP.2.3.1				
	CF2.2	GP.2.2.2				
		GP.2.2.1				
	CF2.1	GP.2.1.6				
		GP.2.1.5				
		GP.2.1.4				
		GP.2.1.3				
		GP.2.1.2				
		GP.2.1.1				
1	CF1.1	GP.1.1.1				
Capability / Domain			BP.01.01	BP.01.02	…	…
			PA01			PA02…

Unlike the base practices of the domain dimension, the generic practices of the capability dimension are ordered according to maturity. Higher levels of process capability are located at the top of the capability dimension. The common features are designed to describe major shifts in an organization's characteristic manner of performing in the security engineering domain. Each common feature has one or more generic practices. The lowest common feature is CF1.1 "Base Practices are performed". This common feature simply checks whether an organization performs all the base practices in a process area. Other common features and generic practices are listed in Table 2.

Table 2 The composition of capability dimension

Capability Level	Common Features	Generic Practices
1	CF1.1 Base Practices are Performed	GP 1.1.1 Perform the Process
2	CF 2.1 Planning Performance	GP 2.1.1 Allocate Resources
		GP2.1.2Assign Responsibilities
		GP2.1.3Document the Process
		GP 2.1.4 Provide Tools
		GP 2.1.5 Use Plans, Standards, and Procedures
		GP 2.1.6 Plan the Process
	CF 2.2 Disciplined Performance	GP 2.2.1 Ensure Training
		GP2.2.2Do Configuration Management
	CF 2.3 Verifying Performance	GP2.3.1 Verify Process Compliance
		GP2.3.2 Audit Work Products
	CF 2.4 Tracking Performance	GP2.4.1 Track with Measurement
		GP2.4.2 Take Corrective Action
3	CF 3.1 Defining a Standard Process	GP3.1.1 Standardize the Process
		GP3.1.2 Tailor the Standard Process
	CF 3.2 Perform the Defined Process	GP 3.2.1 Use a Well-Defined Process
		GP3.2.2 Perform Defect Reviews
		GP3.2.3 Use Well-Defined Data
	CF 3.3 Coordinate the Process	GP 3.3.1 Perform Intra-Group Coordination
		GP 3.3.2 Perform Inter-Group Coordination
		GP3.3.3Perform External Coordination
4	CF 4.1 Establishing Measurable Quality Goals	GP 4.1.1 Establish Quality Goals
	CF 4.2 Objectively Managing Performance	GP 4.2.1 Determine Process Capability
		GP 4.2.2 Use Process Capability
5	CF 5.1 Improving Organizational Capability	GP 5.1.1 Establish Process Effectiveness Goals
		GP 5.1.2 Continuously Improve the Standard Process
	CF 5.2 Improving Process Effectiveness	GP 5.2.1 Perform Causal Analysis
		GP 5.2.2 Eliminate Defect Causes
		GP 5.2.3 Continuously Improve the Defined Process

The relationship between base practices and generic practices is illustrated by Table 1. Putting the base practices and generic practices together provides a way to check an organization's capability to perform a particular activity. For example, a fundamental part of security engineering in PA01 is to establish responsibilities and accountability for security controls and communicate them to everyone in the organization. This activity is captured in BP.01.01, "Establish Security Responsibilities." One way to determine an organization's ability to do something is to check whether they have a process to take corrective action as appropriate when the progress varies significantly from what was planned for the activities they claim to be doing. This "characteristic" of mature organizations is reflected in GP.2.4.2, "Take Corrective Action". The person in charge might be asked: "does your organization take corrective action for establishing security responsibilities?" If the answer is "yes," the interviewer learns a little about the organization's capability. Additional information and evidences could be obtained from the supporting documentation or work products. According to the evaluation standard，an expert can make a proper judgment by marking with "√" , " ×" or a weight value in the relevant cell of Table 1. Answering all the questions raised by combining all the base practices with all the generic practices will provide a good picture of the security engineering capability of the organization. These data and supporting evidences from the questionnaire are collated, and the appraisal results are collated. Basic learning of the assessment can then be summarized in a table as illustrated by Fig. 5. A capability level ranging from 0 to 5 is attributed for each process area and displayed simply by a red bar chart. The actual results of an appraisal may include significant details about each of the areas.

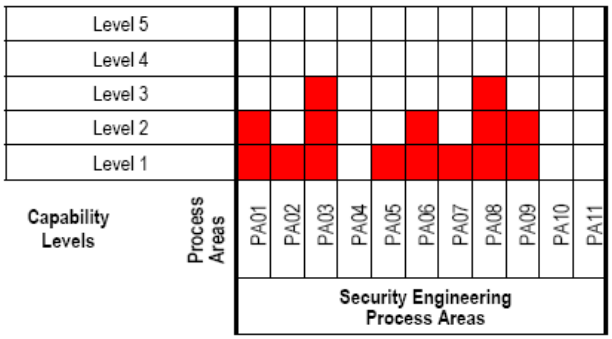

Fig. 5 Determination of the capability levels for some process areas.

3 Outline of the SFR-SSE-CMM

The base practices of the SFR-SSE-CMM are aimed at the essential safety engineering operations of spent fuel reprocessing plants. They represent the practices of the best safety engineering teams of the industry. The combined implementation of certain basic practices can enable an organization to achieve safety targets. Such series of activities aimed at accomplishing the given objectives are called "process areas". A process area is made up of basic practices, which are not only compulsory, but also are essential

for reaching the goals of a process area. Figure 6 shows the structure of the process areas of the SSE-CMM.

PA01 – Process Area Title (in verb-noun form)
Summary Description – An overview of the process area
Goals – A list indicating the desired results of implementing this process area
Base Practices List – A list showing the number and name of each base practice
Process Area Notes – Any other notes about this process area
BP.01.01 – Base Practice Title (in verb-noun form)
Descriptive Name – A sentence describing the base practice
Description – An overview of this base practice
Example Work Products – A list of examples illustrating some possible output
Notes – Any other notes about this base practice
BP.01.02...

Fig. 6 Process area description format.

The key issue in building an SFR-SSE-CMM is to render the basic practices for safety engineering in the field of spent fuel reprocessing. For the sake of conciseness, in the following lines we will only exemplify the threat assessment process area to explore how to project the basic practices of the SSE-CMM into the corresponding safety engineering implementation activities in the SFR-SSE-CMM so as to cover the major fields of spent fuel reprocessing systems security engineering. In accordance with the format of Fig.6, the PA04 threat assessment process area (as an example) in the SFR-SSE-CMM is demonstrated as follows.

PA04 threat assessment process area

Summary description of PA04

Threats refer to the external factors that may cause danger or harm to the system, which could not be controlled but could be relieved partly or nipped in the bud. Threats can be divided into threats from the natural world (such as earthquakes) and threats from human activities (such as explosions). The latter can be further divided into intentional human threats and unintentional human threats. The violations of operating rules and regulations, negligent acts, and operational errors by the operating staff, which can be avoided to a certain degree, are defined as vulnerability of the personnel within the system and are not included in the scope of threat assessment.

The purpose of threat assessment is to identify threats to the spent fuel reprocessing system and understand their nature and characteristics to ensure that the basic process control system (BPCS) can perform the continuous regulation and sequential control of the production process and that the safety instrument system (SIS) can ensure safety functions such as interlock protection and emergency shutdown.

The main content of threat assessment for spent fuel reprocessing systems consists in identifying and assessing the source of a hazard. The identification of the latter is the basis of the selection of initiating events. It describes the location, characteristics and the mechanism of hazard sources, evaluates, classifies and grades the risk of hazard sources, and gives adequate attention to those hazard sources that may cause major casualties, huge losses of property and severe environmental damages or pollution.

Goals of PA04 (The desired results of implementing this process area)

The goals of PA04 is to identify and characterize the threats in spent fuel reprocessing systems, protect the safety of the operating staff and the general public, describe other issues related to safe operation, and come to corresponding conclusions so that quality control can be better implemented in the relevant practices of the engineering process area.

Base practices list of PA04

The base practices of PA04 are listed in Table 3.

Table 3 Base practices of PA04

BP.04.01	Identify applicable threats arising from natural source.
BP.04.02	Identify applicable threats arising from man-made sources.
BP.04.03	Measurement of the threat arising from natural source or external unintended human activities
BP.04.04	Assess the agent capability and motivation of intentional human threats.
BP.04.05	Assess the likelihood of an occurrence of a threat event.
BP.04.06	Monitor ongoing changes in the threat spectrum and changes to their characteristics.

Process area notes for PA04

（1）The threat information produced by this process area is intended for use in PA03, along with the vulnerability information from PA05 and impact information from PA02. While the activities involved with gathering threat, vulnerability, and impact information have been grouped into separate process areas, they are interdependent. The goal is to find combinations of threat, vulnerability, and impact that are deemed sufficiently risky to justify action.

（2）The combination of threat and vulnerability is called an event or working condition. If an event causes harmful results to the system's assets, life safety of the staff and the environment, then it is called an accident.

（3）Since threats may change, monitoring should be conducted regularly. In the phases of site selection, construction, debugging, operation and retirement, spent fuel reprocessing plants must submit the "Site safety evaluation report", "Construction Application and preliminary safety analysis report", "First loading application and final safety analysis report", "Operation application and the amended final safety analysis report", and the "Retirement safety analysis report" to the State Bureau of Nuclear Safety. The specific content of all the basic practices in the assessment of the threat process area comes from these reports or other industry standards [13].

3.1 BP.04.01 Identify applicable threats arising from natural source

3.1.1 Description

Describe the site of plants and the landscape features and meteorological, hydrological, geological and seismological features in its vicinity, analyze such features from the perspective of safety in accordance with the related rules of the state and the competent department for nuclear industry, and identify the possible threats that the plant may face from the natural world, including earthquake, landslide, surface uplift, hurricane, sandstorm, flood, debris blow, tsunami, etc.

3.1.2 Example work products

- Geographical threat

Point out the location of the plant site and mark it out in latitude and longitude, provide related maps or aerial photographs indicating towns, water bodies, transport routes and nearby architecture in the vicinity of 80 km, mark out the plant's borderlines in a map of a proper scale, highlight the possible influence of land drainage and surface winds by means of proper hypsographic map.

- Meteorological threat

Describe the historical meteorology around the site and its vicinity and point out the seasonal meteorology and the extreme meteorology such as severe cold, intense hot, heavy rains and snows, hails, rainstorms, lightning strikes, hurricanes and tornadoes, *etc*.

- Surface and underground hydrologic threat

Describe the noticeable hydrological features around the site and its vicinity. Provide the drainage system graph, hydrology safety fixtures and position, upstream and downstream flow control structures position, the flow variation rules and influence factors, the management and operation standards. Describe the layers of underground water, their formation and the status of seepage flow in the site; provide data concerning grads, penetrability, dispersion, dilution, ion exchange, and channeling.

- Geological and seismological threat

Describe geological and seismological features and their attributes, draw conclusions, and mark out the provenance of data. Regional geological data include regional natural geography, geological background and geological history, and site geological data include petrology and formational geology. Detailed analyses must be made in terms of possible ground subsidence, uplift or subsidence damage. The site seismological data include the relationship between the site's natural geography and the regional natural geography, the lithological stratum and formational-geological features of the site, surface geology and seismological history, and the strongest earthquake ever recorded in the region.

- Natural background radiation threat

The stream of high-energy, fast-moving particles or waves that is found in our environment is called natural background radiation. It is required to provide data about the natural background radiation of the site in a radius of 80 km.

3.2 BP.04.02 Identify applicable threats arising from man-made sources, either accidental or deliberate

3.2.1 Description

Describe the site of the spent fuel reprocessing plant and the nearby conditions in terms of population, industry, agriculture, transportation, water conservancy and military facilities. Identify the threats related to human activities from the perspective of safety in accordance with the rules and regulations of the state and the competent department for nuclear industry concerning radioprotection. These threats come from outside the system, including collision, falls, fires, pipeline accidents, toxic gas, explosion, radiation, pollution, hydropower interruption, etc.

3.2.2 Example work products

- Threats brought by population change

Provide demographic data for the area within a radius of 80 km, predict the dynamic change of population, and analyze the potential effects of population change on the reprocessing plant's safety such as resource exploitation, civil and criminal cases, *etc*.

- Threats brought by the utilization of land and water bodies

Describe the utilization of land and water bodies in the vicinity of 80 kilometers and its potential effect on the reprocessing plant's safety, such as water depletion, land desertification, *etc*.

- Threats brought by industry, agriculture, transportation and military installations

Mark out on the map the industrial, agricultural, transportation and military installations in the vicinity of the plant site, point out their relationships to the spent fuel reprocessing plant as well as possible hazards linked to them, such as plane crash, projectile impact, pipeline accidents and reservoir breach, *etc*.

- Threats brought by plant effluent

Describe the form, type and nature of the effluent of the spent fuel reprocessing plant and its nearby factories, analyze the hazard mechanism of the effluent for the staff and the environment, such as harmful gas leakage, air and water pollution, and so on.

- Man-made threats in the process from input to output

Mark the input of staff, equipment, raw materials, hydroelectricity, and the output of staff, products, side products and other tangibles. Mark the source, destination, application, storage location, mode, specification, and physical, chemical and radioactive features of all the items. Pay attention to the movement and evolution of inflammable, explosive, toxic and radioactive materials [14-16], such as camphor brown oil explosion, concentrated unary nitrate solution leakage, interruption of cooling water, and loss of radioactive sources, etc.

3.3 BP.04.03 Measurement of the threat arising from natural source or external unintended human activities

3.3.1 Description

Natural and man-made threats have their corresponding measurement units and sphere of application. A proper measurement unit should be selected to measure the various threats in a given environment and figure out the degree of threats. For instance, for the measurement of earthquakes the Richter scale can be used as a measurement unit of the intensity.

3.3.2 Example work products

- Choose a set of proper measurement units according to the natural threats and man-made threats.
- Measure the attributes or the degree of threats by means of the selected measurement units according to the natural threats and man-made threats so as to provide relevant data for the engineering process area to determine the design basis event.

3.3.3 Notes

If a given threat has no acceptable measurement unit, an acceptable one should be put in place. If possible, testability description should be made for the relevant range and measurement unit.

3.4 BP.04.04 Assess the agent capability and motivation of intentional human threats

3.4.1 Description

This process area focuses on the determination of a

potential human adversary's ability and capability of executing a successful attack against the system. By "ability" we mean the adversaries' knowledge to perform attacks (*e.g.* do they have the training knowledge), whereas by "capability" we refer to a measure of the likelihood that an able adversary can actually execute the attack (*e.g.* do they have the resources).

3.4.2 Example work products

- Threat agent capability assessments and descriptions
- Pre-arranged planning for a meeting in case of the emergency of a terrorist attack

3.4.3 Notes

Deliberate man-made threats are to a large extent dependent upon the capability of the threat agent and the resources that the adversary has at his disposal. In addition to the agent capability, an assessment of the material resources that the agent has available should be considered along with his motivation and breakthrough points for performing the act. This may be affected by the agent's likely assessment of the attractiveness of the target or asset. The effect of multiple attacks occurring in sequence or concurrently needs to be considered.

3.5 BP.04.05 Assess the likelihood of an occurrence of a threat event

3.5.1 Description

Assess the possibility of various marked threats by means of mathematical statistics based on historical data and prior experience.

3.5.2 Example work products

- Assessment report on the possibility of the occurrence of various threats

3.5.3 Notes

Gather statistics and analyze the frequency of occurrence of various threats according to their classification, and illustrate their degree of uncertainty or an approximate range.

3.6 BP.04.06 Monitor ongoing changes in the threat spectrum and changes to their characteristics

3.6.1 Description

In any case, threats will be dynamic. Due to the change in environment and the update of equipment, staff and technology, new threats may arise and the nature of the current threats may also change. Therefore, current threats and their characteristics should be monitored and new threats should be examined. This basic practice is closely connected to the safety status monitoring in the engineering process area.

3.6.2 Example work products

- Threat surveillance report
- Threat change report

3.6.3 Notes

Since threats may vary, multiple assessments can be carried out in a given environment. The cycle of assessment can be decided depending on the nature of the different threats. For example, the assessment of earthquakes can be performed every 5 years while the assessment of threats brought by plant effluent can be made on a monthly basis. However, repeated threat assessment can never replace threat monitoring. Besides, threat monitoring doesn't necessarily have to be conducted by insiders; it can be entrusted to relevant organizations or data can be retrieved from them (for example for the monitoring of earthquakes and weather).

4 Conclusions

SFR-SSE-CMM is an experiment aiming at applying SSE-CMM to China's spent fuel reprocessing system. More than sixty basic practices have covered the main fields of spent fuel reprocessing safety engineering. Such basic practices, in combination with the generic practices of SSE-CMM, constitute a standards system for the safety engineering capability assessment of spent fuel reprocessing systems. Such a system is conducive to standardizing enterprise engineering implementation activities and discovering ways to upgrade process capabilities. In order to get a lot of effective evaluation data, simplify the assessment process, we have developed special assessment software: "Appraisal Tool of Systems Security Engineering Capability Maturity". The evaluation experts input data shaped like Table 1 by the Brower/Server interface independently, the computer system will output a figure similar to Fig. 5 through

the rapid information processing, displaying the ability level in an intuitive way that the evaluation process has determined, meanwhile, giving the probative value of direct or indirect evidences and suggestions how to improve the process area. Clicking on the corresponding red square by moving the mouse, the implementation situation and execution characteristics of generic practices that reflect the process capability, can be further displayed. Now, the spent fuel reprocessing systems security engineering capability maturity model, have been become one of enterprise standards of implementing safety engineering in China, and the software copyright has been declared. Only through the proper ontology conversion, the model will be promoted to use in nuclear industrial systems including nuclear power plants.

Acknowledgement

This research project has benefited from the State Administration of Science, Technology and Industry for National Defense, China National Nuclear Corporation, and Department of Education of Hunan Province. We are honored to express our deepest gratitude to them for their funding and support (Grant No. A3720060121, CX2009B187, supported by Hunan Provincial Innovation Foundation for Postgraduate). Moreover, I would like to take this opportunity to thank my graduate friends in the nuclear economy and management research center of Nanhua University for their encouraging and good advices.

References

[1] US NRC WASH-A1400, Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants, 1975.

[2] IAEA Safety Standards Series No.NS-R-1, Safety of Nuclear Power Plants: Design, 2000.

[3] IAEA Safety Standards Series No.NS-R-2, Safety of Nuclear Power Plants: Operation, 2000.

[4] US NRC NUREG-0800, Chapter 19, Use of Probabilistic Risk Assessment in Plant-specific, and Risk-informed Decision-making: General Guidance, 2002.

[5] DEL, C. E.: Statistical Process Adjustment: A Brief Retrospective, Current Status, and Future Research, STATISTICA NEERLANDICA, 2006, 60(3): 309-326.

[6] PAULK, M. C.: Process Improvement and Organizational Capability, Generalizing the CMM, Proceedings of the ASQC's 50th Annual Quality Congress and Exposition, Chicago, IL, 1996, May 13-15: 92-97.

[7] System Security Engineering Capability Maturity Model, Model Description Document. Version 3.0, June 15, 2003: http://www.SSE-CMM.org.

[8] QIAN, G., and DA, Q.: Management OF Info-Security Engineering Based on SSE-CMM Model，Journal of Southeast University (Natural Science Edition), 2002, 32 (1): 32-36.

[9] CHEN, J, and GONG ,Y.: Model of Information System Security Engineering Based on SSE-CMM, computer Engineering, 2003, 29(16): 35-36.

[10] SONG, R., QIAN, G., and YU, L.: Information Security Management and Control Based SSE-CMM, Journal of computer Engineering and Application, 2000, 36 (12):128-129.

[11] LIU, X., and CUI, L.: Research on Security Risk Assessment for Electric Power Communication System Based on the SSE-CMM, Telecommunications For Electric Power System, 2005, 26(156): 49-51.

[12] XIAO, R., MEI, L., and HUILAN Z.: Information Security Evaluation of E-Government Systems, Proceedings of 2007 International Symposium on Distributed Computing and Applications to Business, Engineering and Science, August 14-17, 2007, Hubei, China.

[13] Nuclear Industry Standard of the People's Republic of China, EJ/T 681-92：The Standard and Content of Safety Analysis Report for the Spent Fuel Reprocessing Plant.

[14] LUO, Y., FAN, Y., and MA, X.: Risk Analysis and Safety Evaluation, Beijing：Chemical Industry Press，2004: 144-185.

[15] JIANG, S., and KE, Y.: Reprocessing Plant Design for Power Reactor Nuclear Fuel, Beijing: Atomic press，1996.

[16] ZHENG, H., and ZHAO, B., and LI, R.: Exploration of Probabilistic Safety Analysis Method FOR Nuclear Fuel Reprocessing Plant, Nuclear Project Research and Design, 2008, 69:30-35.