Security vulnerability of spent fuel reprocessing system based on SSE-CMM

YU Ying[1,2], YANG Xiao-hua[1,2], ZOU Shu-liang[1] , LIU Zheng-Hai[1,2], LIU Zhi-Ming[1,2], and BAI Xiao-feng[3]

1. Research Center for Economic & Management of Nuclear Power, University of South China, Hengyang 421001 (yyingu@sina.com, xiaohua1963@yahoo.com.cn, zoushuliang@yahoo.com.cn, ehaizh@163.com, nhdxlzm@sohu.com)

2. Computer Science & Technology School, University of South China, Hengyang 421001

3. The Safety Protection Department of the 404 Company Limited，CNNC，Lanzhou 732850，China (baifeng98@163.com)

Abstract: Reprocessing of spent fuel is the favored strategy for the end step of the fuel cycle. In order to set up a comprehensive framework for evaluating the security engineering practices for reprocessing systems, this paper proposed to refine the security vulnerability processes of SSE-CMM, which are part of one of the three aspects (threat, vulnerability and impact) of security risk, to fit reprocessing systems. We define security vulnerability in reprocessing systems by comparing definitions of vulnerability in several different domains, and we discuss its meaning in SSE-CMM. Separately, we analyze the specific content of the five basic practices of the vulnerability assessment process by describing the actual activities undertaken in reprocessing systems.

Keyword: vulnerability; spent fuel; reprocessing; SSE-CMM; security engineering

1 Introduction

Spent fuel management is one of the most important factors influencing the future of nuclear energy. While reprocessing of spent fuel is the favored strategy for the back end of the fuel cycle, in the long term, the recycling of nuclear fuel may play an important role both in global energy supply and as technical basis for the partitioning and transmutation of minor actinides to reduce environmental stress and contribute to the sustainable use of nuclear energy. In preparation for such a future possibility, reprocessing is a desirable option. It is also recognized that continued work is required to further develop safety standards. But security considerations now mainly depend on security analysis reports, which focus on the technical process. A comprehensive framework for evaluating the security engineering practices of reprocessing systems is lacking.

The most widely accepted security engineering principle is the Systems Security Engineering Capability Maturity Model (SSE-CMM), which has been accepted as an ISO standard [1]. The basic ideas and structural features of the SSE-CMM and the outline of applying SSE-CMM specifically for spent fuel management has been presented elsewhere by some authors of this paper [2]. In this paper, we try for the first time to refine the vulnerability process area for the SSE-CMM for the use in the Spent Fuel Reprocessing (SFR) domain. Based on this refinement, we propose a security vulnerability assessment process for SFR systems to further integrate processes and infrastructures relevant to security. Section 2 discusses background knowledge and previous works related to the current study. Section 3 defines vulnerability for SFR by contrasting the definitions in different other fields. Section 4 elaborates the results of mapping the vulnerability process area to the SFR domain. Section 5 discusses the challenges and lessons learned in the mapping and process development. Section 6 summarizes the conclusions and proposes future works.

2 Background and related work

2.1 SFR status and trends

Spent Fuel Reprocessing can be regarded as the only currently proven option for spent fuel management with an end point, namely disposal in a geological repository. Reprocessing using the Purex process has become a mature technology with considerable experience gained from the operation of civil

Received date: February 26, 2011
(Revised date: May 31, 2011)

reprocessing plants in several countries handling a wide variety of fuel types (see Table 1) [3].

Civil reprocessing has been carried out on a commercial scale for over four decades in several countries (see Fig.1)[4]. Today all commercial reprocessing plants are collecting material from civil nuclear reactors to recycle them and convert the unwanted wastes into a safe form for disposal.

Table 1 Current and planned reprocessing capacities in the world

Country	Site & Plant	Start operation	Capacity (tons/year)	
			Present	Future
China	Jiuquan: RPP LWR	——	——	60
	Lanzhou: CRP LWR	2020	——	800
France	LaHague: UP2 LWR	1994	800	800
	LaHague: UP3 LWR	1990	800	800
India	Trombay: PP Research	1964	60	60
	Tarapur: PREFRE1 PHWR	1974	100	100
	Kalpakkam: PREFRE2 PHWR	1998	100	100
	Kalpakkam: PREFRE3A PHWR	2005	150	150
	Tarapur: PREFRE3B PHWR	2005	150	150
Japan	Tokai-mura: PNC TRP LWR	1977	90	90
	Rokkasho-mura: RRP LWR	2010	800	800
Russian Federation	Chelyabinsk: RT1 WWER440	1971	400	400
	Krasnoyarsk: RT2 WWER1000	2020	——	1500
UK	Sellafield: Thorp LWR/AGR	1994	900	900
	Sellafield: B205 GCR	1967	1500	——
	Total Capacity(tons/year)		5850	6710

In the long term, however, with the implementation of advanced reactors and fuel cycle systems, such as partitioning and transmutation, novel reprocessing technologies with total actinide recycling may have to be implemented. This is mainly due to the long term implications associated with the storage and disposal of minor actinides and fission products, as well as the fissile materials, contained in the spent fuel.

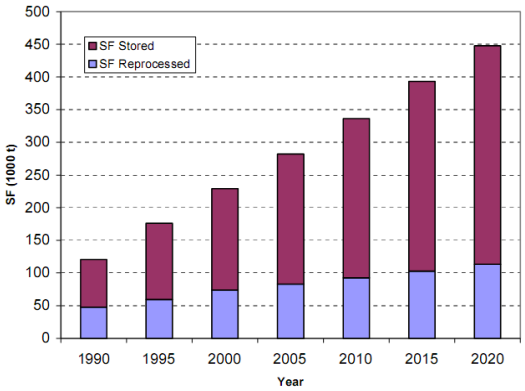

Fig.1 Global statistics in spent fuel management.

In China, spent fuel is arising. It is estimated that, after 2005, about 199 tons of heavy metal (tHM) PWR spent fuels and 198 tHM CANDU spent fuels will be produced each year [5]. At present, the centralized wet storage facility planned is the Lanzhou Nuclear Fuel Complex with a capacity of 550 tHM, which is part of the pilot reprocessing plant.

It is clear that reprocessing will in the future provide a technical basis for the partitioning and transmutation of minor actinides, and it will thereby contribute to the reduction of environmental stress as part of the sustainable utilization of nuclear energy. The economics and environmental impacts of reprocessing should be analyzed. However, security is the most important thing. Spent fuel reprocessing plants have been operating at industrial scale for several decades. During this time much knowledge has been accumulated, which has resulted in significant improvements in plant safety and radiological protection.

2.2 Security engineering and SSE-CMM

SSE-CMM addresses security engineering activities that cover the whole life cycle of the product, including concept definition, requirements analysis, design, development, integration, installation, operations, maintenance, and decommissioning. To define, improve, and assess the capability of security engineering is the goal of SSE-CMM. Only if the security engineering organization achieves a high maturity, the implementation process of the organization can be reliable and its product can be accepted in the long term.

The SSE-CMM is a process reference model. It has been mainly applied to evaluate the level of maturity of security maturity in IT organizations. The SSE-CMM is originally focused on the processes used to achieve information security, most specifically on the maturity of those processes [6]. However, experience with the Model has demonstrated its utility and applicability to other security domains other than the IT domain. The SSE-CMM Model does not dictate the use of a specific process, let alone a specific methodology. An organization making use of the SSE-CMM Model should use its existing processes.

The security of fuel reprocessing mainly depends on the security analysis reports based on international standards or national standards. The International Atomic Energy Agency (IAEA) has developed a system of international safety standards [7] for fuel cycle facilities. A safety guide on spent fuel reprocessing facilities is also in preparation, which defines series of standards for security of fuel reprocessing. China's legal system of spent fuel management consists of relevant laws, regulations, national standards (GB), and trade standards (EJ) [8], which are a set of best practices (framework) for spent fuel management. They are result-oriented but not process-oriented towards security risk assessment. So, the reports focus on the technical processes and nuclear safety culture mostly. They are not geared toward an assessment in a security engineering way which is more systematic and process-based.

A gap needs to be bridged in order to implement this model in the reprocessing domain, in which rigorous standards must be met. It would help to understand what practical activities are undertaken in the reprocessing domain and to set up a framework of maturity assessment.

2.3 Assess vulnerability process

Managing risk is an important part of the management of security. The process of assessing the vulnerability belongs to the risk process, which is the most important one of the Model's security engineering three main areas: Engineering Process, Risk Process and Assurance Process. There are four process areas (PA) in the Risk Process, *i.e.*, assessing security risk, threat, vulnerability and impact. And the last three PAs of threat, vulnerability and impact are the three main factors to support assessing the security risk by providing relevant information. They interact with each other. Risk is an unwanted incident made up of the three components (see Fig. 2).

The purpose of the assessment of vulnerability is to identify and characterize system security vulnerabilities. This process includes analyzing system assets, defining specific vulnerabilities, and providing an assessment of the overall system vulnerability.

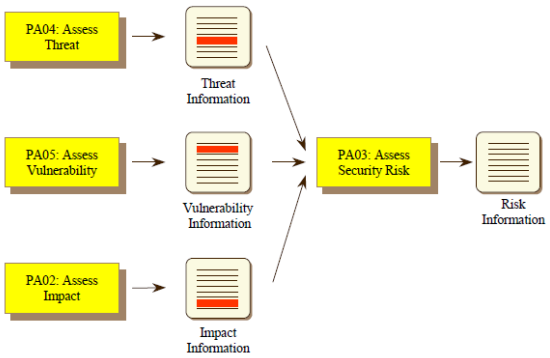

Fig. 2 The security risk process involves threat, vulnerability, and impact

It includes five Base Practices:

BP.05.01 Select a vulnerability analysis method

BP.05.02 Identify vulnerabilities

BP.05.03 Gather vulnerability data

BP.05.04 Synthesize the system's vulnerability

BP.05.05 Monitor vulnerabilities and their characteristics

The base practices for security were gathered from a wide range of existing materials, practices, and expertise. The practices selected represent the best existing ones in use in the security engineering community, not untested practices. Those five base practices above are mandatory characteristics that must exist within the implementation of a vulnerability assessment process.

3 The definition of vulnerability

The "vulnerability of spent fuel" has been discussed in nuclear domain mainly from the nuclear security aspect of radiological terrorism to the spent fuel

pools in nuclear facilities. Therefore, the vulnerability of spent fuel reprocessing is one of the issues to be discussed from security aspect. However, as far as the authors know, there has been no studies to deal with this issue from the SSE-CMM model. The authors of this paper try to define "vulnerability" of spent fuel reprocessing from the frame of SSE-CMM.

3.1 Vulnerability in different domain

Even if vulnerability originates from the study of natural disasters, the concept now often appears in papers related to ecology, environmental sciences, computer science, networking, information systems, economics and other related fields, in order to describe the components of a system vulnerable to damage and lacking the ability to resist interferences and resume their normal functioning. Vulnerability in different domains has different connotations.

3.1.1 Ecological vulnerability [9]

Vulnerability in ecological terms is the variability shown by an ecological system in a specific space or region when subject to natural or anthropogenic activities. The trend of the variations is often disadvantageous to the viability and development of the system.

3.1.2 Vulnerability in computer systems

Vulnerability, also known as security hole, is the defect or deficiency that exists in a computer system's hardware, software, design and implementation or in related system security policies. It represents a weakness in the security of automated systems and their management. An illegal user can make use of security vulnerabilities in computer systems to gain additional privileges, without having been previously granted access, and thereby damage the system [10, 11]. Especially in network systems, the direct consequence of the existence of vulnerability is the potential illegal access or increase of authority of non-authorized users. Consequently, an attacker can get the opportunity to damage the network system [12].

3.1.3 Power system vulnerability

The vulnerability of a power system stands for the possibility of catastrophic accidents caused by large area blackout. Dangerous conditions due to human interventions, internal components failures, protection control systems, and other factors appear when an accident happens in the system [13]. The outcome depends on whether the system can maintain stability and keep the normal capacity of power supply, that is, the risk level through which a system may maintain stable operation and normal power supply under faulty conditions.

3.2 The definition of vulnerability in SSE-CMM

In the frame of SSE-CMM, "vulnerability" refers to the aspect of a system that can be exploited for purposes other than those originally intended, such as weaknesses, security holes, or implementation flaws within a system that are likely to be attacked. These vulnerabilities are independent of any particular threat or attack. We can compare the various connotations of vulnerability used in different domains. Ecological vulnerability focuses on the system itself, on its instability. On the other hand, vulnerability in computer systems has the same meaning as security holes or flaws in SSE-CMM, whereas the meaning of vulnerability in power systems relies on the consideration of threats pending on the system.

In general, vulnerability includes three meanings:
(1) It is an inherent property of the system, which has nothing to do with a specific threat.
(2) The existence of the vulnerability makes the systems, facilities, or internal components more sensitive to changes or interferences of the outside world.
(3) Under the force of external interferences and environmental changes, the system, facilities or internal components can be damaged to a certain degree.

3.3 Vulnerability of SFR based on SSE-CMM

To identify vulnerabilities, at first we need to analyze system assets that are objects that we can identify by their internal properties. In SSE-CMM, assets are broadly construed to include the people, environment, technology and infrastructure in a system. So the inherent properties to SFR focus on three aspects: human, equipment and implement technology. All the three aspects are the assets of SFR system. There are

human errors that may happen during the reprocessing process. Equipment failures are factors that can impact reprocessing process too. And the implementation of technologies has unavoidable limitations, which depend on the development of science and technology.

4 Mapping vulnerability process of SSE-CMM to SFR domain

As mentioned above, vulnerability process of SSE-CMM has five Base Practices. Mapping the vulnerability process of SSE-CMM to the SFR domain is to explain each practice based on the actual practices in SFR domain (see Table 2).

The practice called "select vulnerability analysis method" means to select the methods, techniques, and criteria by which the system security vulnerabilities in a defined environment are identified and characterized. As regards SFR, the three aspects of system vulnerability have different reasonable and effective analysis methods. Human Reliability Assessment (HRA) [14], Human Error Assessment and Reduction Technique (HEART) [15] and Human Cognitive Reliability (HCR) [16] are used to analyze the human error. Root Cause Analysis (RCA) [17] and the Fault Tree Analysis (FTA) [18] are general methods to analyze equipment failure. Experimental test method is the way to find out the limitation of implementations of technologies. In this practice, the methods used to analyze vulnerabilities must be defined to establish security vulnerabilities of the system in a way that allows for them to be identified and characterized.

"Identify vulnerabilities" means that all system vulnerabilities discovered should be identified. The ordering of such vulnerabilities may be prioritized in accordance with threat analysis, which would assess in another process. All possible human errors, equipment failures and technological limitations must be listed out, human errors ordered by the risk they could bring to the system, equipment failures ordered by their functional significance, technological limitations ordered by their impact on the implementation of the system.

Vulnerabilities have properties associated with them. "Gather vulnerability data" is to gather data associated with these properties of the vulnerabilities. For example, the number of times that a human error or equipment failure emerged is information related to human error or equipment failure; the limit parameters about a given technology are the properties to describe technological vulnerability. All the reliable data about vulnerability of a system need to be recorded.

Aggregated vulnerabilities could result in problems for the system too. "Synthesize system vulnerability" means to analyze which vulnerabilities or combinations of vulnerabilities

Table 2 Mapping between vulnerability process BPs and SFR system

Vulnerability process BPs	BP Description	SFR practices	Product/Check point
BP.05.01	Select vulnerability analysis method	Define methods for analyzing human error, equipment failure and technology limitation	Indication HRA, HEART, HCR, FTA, RCA *et al*. in the analysis report
BP.05.02	Identify vulnerabilities	List all possible vulnerability and order them	Human error list, equipment failure list, Notes of technology
BP.05.03	Gather vulnerability data	Record the times of occurrence of each human error or equipment failure. List the important limit parameters of implement technology.	Statistics of human errors, Statistics of equipment failure list of parameters
BP.05.04	Synthesize system vulnerability	The analysis of the probabilities of human error and equipment failure. The analysis of the likelihood of exceeding technology limitation conditions.	Human Error Probability tables, Equipment failure probability tables, Exceeding conditions likelihood table
BP.05.05	Monitor vulnerabilities and their characteristics	Check the equipment and conduct staff appraisal regularly. Focus on the change of the limitation parameters. Record new problem.	The logs of the equipment application and parameters, staff appraisal result report, abnormal conditions analysis report

result in problems for the system and determine the likelihood of vulnerabilities and the chance for successful exploitation. In SFR, Probability Safety Assessment (PSA) is the main method used to perform a synthesized analysis. The likelihood of vulnerabilities combination can be represented by the probability analyzed by PSA and FTA. Failure probability is characterizes equipment failures; human error probability characterize human error.

The vulnerability spectrum applicable to any location and situation is dynamic. New vulnerabilities can become relevant and the characteristics of existing vulnerabilities can change. In terms of SFR, new implementation technologies or new equipments can bring new vulnerabilities. Equipment failure probability can become larger after a period of use. "Monitor vulnerabilities and their characteristics" is to monitor both existing vulnerabilities and their characteristics, and to check for new vulnerabilities on a regular basis. So, it is important to check the equipment regularly, conduct staff appraisal periodically, focus on the change of the limitation parameters, and record new problems that occur in the reprocessing implementation process.

5 Challenges and lessons learned

The mapping encountered a number of challenges. To create the mapping, the understanding of both SSE-CMM and the SFR regulations must be gained to make sure to interpret the terminologies and concepts accurately. The success of the mapping needs to draw the attention and win the acceptance of reprocessing plants. Although the terminologies can be learned during the development, it is still difficult to fit them in the appropriate context. Thus, it is important to get feedback from plants to improve the accuracy of our mapping results. Thus, it is imperative that we formulate a method to communicate the SSE-CMM concepts with experts in an effective manner.

6 Conclusion and future work

The mapping from the vulnerability process of SSE-CMM to the spent fuel reprocessing domain enables us to develop a set of quantitative metrics to assess the security vulnerability in an SFR system. It facilitates the development of the security vulnerability assessment process for SFR systems. Based on our mapping results, we found that, although there is no definition of vulnerability in spent fuel reprocessing, most practices about vulnerability assessment have been done actually. This means that its security engineering process reached capability maturity level 1 in PA05 – "assess vulnerability process". To confirm whether it reaches the higher level, we need to figure out the implementation of generic practices. Also, the administrative policies and requirements still need to be defined in the spent fuel reprocessing era.

It is the first step to assess the risk of spent fuel reprocessing. We will further refine the SSE-CMM to fit the SFR domain step by step. Firstly, we will refine the base practices of the security risk process in SFR. It is essential to identify emerging security needs, threats/vulnerability/risks, and to develop adaptive processes and methods to coordinate and verify security. Then we will map the other two main area of the Model (i.e. threat and impact) to SFR. At the same time, the generic practices about each process will be analyzed and put forward. Setting up a whole SFR Maturity Assessment Model based on SSE-CMM is the final goal.

References

[1] SSE-CMM Project& ISSEA Team: System Security Engineering Capability Maturity Model Description Document-Version3.0[S], 2003.(In Chinese)

[2] LIU.Y., ZHOU,S., YANG Xiao-hua, OUYANG Zi-gen, and DAI Jian-yong: Spent Fuel Reprocessing System Security Engineering Capability Maturity Model, Nuclear Safety and Simulation, Vol.2, No.1, March 2011: 83-91

[3] Deng, G.: Overview of Spent Fuel Management in China[R] , International Conference on Management of Spent Fuel from Nuclear Power Reactors, 2010.6.3

[4] International Atomic Energy Agency: Status and Trends in Spent Fuel Reprocessing[R], IAEA-TECDOC-1467, Vienna, 2005.

[5] China National Nuclear Corporation: The National Report under the "Convention on Nuclear Safety" of the People's Republic of China[R], 2005. (In Chinese)

[6] PRC National Standard: Information Technology − Systems Security Engineering[S], GB/T 20261-2006 Capability Maturity Model. (In Chinese)

[7] International Atomic Energy Agency: Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management[R], INFCIRC/546, 1997.

[8] China National Nuclear Corporation: Safety Design Rule for Radiation Protection of Nuclear Fuel reprocessing Plant[S], EJ849-94, 1994. (In Chinese)

[9] ZHOU, J., HUANG,X.: A Review on The Assessment Methods of Ecological Vulnerability[J], YUNNAN GEOGRAPHIC ENVIRONMENT RESEARCH, 2008,20(1):55-71. (In Chinese)

[10] KRSUL, V.: Software Vulnerability Analysis[R], Department of Computer Sciences, Purdue University, 2000.

[11] LIU, B., XIAO, X., ZHANG,G.: Vulnerability Assessment Method of Information System Based on Analytic Hierarchy Process[J], Computer Science, 2006,33(12):62-64. (In Chinese)

[12] Sushil Jajodia, Steven Noel and Brian O'Berry : Topological Analysis of Network Attack Vulnerability[C], Springer US, 2005:247-266.

[13] WANG, L.: Application Study on Vulnerability Assessment in Power System Security Defense System[J], North China Electric Power University, 2005. (In Chinese)

[14] XIE, H., SUN,Z., LI,X., *et al*: An Overview of Typical Methods for Human Reliability Analysis[J], Journal of National Universityof Defense Technology, 2007,29(2):101-107. (In Chinese)

[15] WILLIAMS,J.C.: A Data-based Method for Assessing and Reducing Human Error to Improve Operational Performance[C], Proc. IEEE 4th Human Factor and Power Plants , 1988 :436 - 453.

[16] ZHANG, L., HUANG,S., HUANG,X.: THERP+HCR-based Model for Human Factor Event Analysis and Its Application[J], Nuclear Power Engineering, 2003,24(3):272-276. (In Chinese)

[17] GAO, L., LV,Q.: Application of Root Cause Analysis on Equipment Failure to Improve the Safety Performance of Key Equipments in Nuclear Power Station[J], Nuclear Power Engineering, 2005, 26(6(S1)):82-86. (In Chinese)

[18] CAO, X., HU,L., LI,Y., *et al*: Fault Tree Analysis of East Cryogenic System[J], Chinese Journal of Nuclear Science and Engineering, 2009,29(2):170-175. (In Chinese)

Intentionally Blank