

**Military Technical College
Kobry El-Kobbah,
Cairo, Egypt**



**11th International Conference
on Electrical Engineering
ICEENG 2018**

Analysis of Nuclear Safety Measures Associated with Nuclear Power Plants Programs

Salem ElKhodary*, Hassan Mahmoud**, Saied Qotb*** and Emad El-Din Sharouda****

ABSTRACT

This paper discusses one of the most important issues that impedes nuclear energy expansion, and this issue is the nuclear safety measures which must be verified and fulfilled in the nuclear power plant. Egypt is considered one of the newcomers that start to produce electricity dependent on the nuclear energy. Egypt signed an Intergovernmental agreement (IGA) on 19 November 2015 with Russian Rosatom company, specialized in nuclear energy sector, to establish the first nuclear power plant (4 VVER reactors of Gell+) located in Al-Dhabaa City, north of Egypt. The proposed nuclear power plant would be consisted of four 1200-MWe pressurized water reactor (PWR) to provide the Egyptian unified grid with total power 4800-MWe. This nuclear power plant will be in operation case within four stages. It is planned for nuclear share in the Egyptian energy mix to be 10% by 2030. The thought of nuclear energy danger is the main cause that prevents some governments to introduce the first nuclear power plant in their land or to expand their nuclear power plants programs. The advanced intelligent techniques which are concerned with nuclear passive and active safety systems in nuclear power plants will be analyzed and recommendations would be delivered in this paper.

KEY WORDS: Nuclear power plant NPP / Risk assessment / Unified security / critical digital assets CDA / safety security and emergency preparedness SSEP/ hazards /threats / initiating events / vulnerabilities.

1. Introduction

Humanity must face the unexpected indefinitely consumption of energy which depends on the fossil fuel energy generation like coal, oil, and natural gas. Increasing the world demand in energy, the world motivates the researchers who work in field of

* Faculty of Engineering, Ain Shams University, Cairo, Egypt.

** Egyptian Electricity Holding Company, Cairo, Egypt.

*** Atomic Energy Authority, Cairo, Egypt.

**** Middle Delta Electricity Production Company, Talkha, Dakahlia, Egypt.

energy generation to obtain an optimum solution can absorb this rate of energy demand. So, the energy generation technique based on fossil fuel must be replaced by another type of energy generation. Then, many researches have been applied and it is found that the technique of nuclear fission energy produces economic, large scale, safe and clean energy with no emissions of greenhouse gases. Therefore, the world started to change the dependent on energy generation technique of fossil fuel to nuclear energy generation. France is the best example of the world countries which follows the nuclear fission energy generation. Also, some of Middle East countries like Egypt, UAE and Jordan started to use the world of nuclear energy [1].

The first step of global energy transformation is converting the energy generation from fossil fuels to nuclear fission energy technique. This process can be achieved throughout certain stages like that has been done in France from 1970 to 1980. Dependence of France on energy generation technique helps to reduce emissions of carbon dioxide and preventing greenhouse gases [2]. Other industrial countries should take this transition step in their considerations. Methane is considered the major greenhouse gas and replacing the coal-fired power plant with the gas-fired power plant is not optimum solution to reduce the high rate of greenhouse-gas emissions even the low rate of pollutant emissions into the atmosphere [3]. Renewable energy such as wind and solar will be applied to supply the economic and sustainable energy, but they are very expensive to purchase and require specified environment to be established. So, nuclear energy technique is considered the best solution to generate clean large-scale energy. Figure (1) shows the percent of the produced energy in all the world of nuclear energy compared with other types of energy generation [4].

2. History of Safety Issues Associated with Nuclear Power Plants Comparing with Fossil Fuel Power Plants

Although the misconceptions in media about the nuclear fission, it would be considered among the safest energy technologies in terms of health impact and fatalities, notwithstanding there are great nuclear accident occurred three times throughout the history of nuclear energy generation. The first nuclear accident occurred at Three Mile Island (TMI) in the U.S.A, **1979**., the second occurred at Chernobyl in Ukraine, **1986** and the last nuclear accident was at Fukushima in Japan, **2011** [5].

In Chenoby1 nuclear accident, there were **35** fatalities cases, namely some of these fatalities that were directly exposed to high radiation during the clean-up operation. However, the fatalities numbers due to the nuclear accidents, less than one hundred, are considered relatively small comparing to numbers of annually fatalities in the coal, gas and oil-fired power plants [6].

The statistics which was studied by the World Health Organization (WHO) show that the global values of the mortality rate per billion kWh for different types of energy generation due to all reasons and it was that nuclear energy generation type has the lowest mortality rate among other types of energy generation. Table 1 shows the mortality rate per billion kWh for different types of energy generation [7].

3. Safety Systems Supplied to Nuclear Power Plants NPPs

Safety is considered the most important factor during choosing the type of reactor. All reactors must satisfy the minimum level of the safety requirements to be more inherently safe reactors. In case of trouble existence in the reactors to prevent occurrence of great accident, safety systems of the reactors are safely shutdown of the reactor, cool the reactor core and operate all auxiliary systems that responsible for the reactor safely operation and shutdown [5,7].

3.1 Control of the Reactor in Normal and Shutdown Conditions

The reactor must be under control during its operation to avoid the excessive thermal energy produced by an abnormal rate of nuclear fission reaction. However, in a reactor trouble case, it is necessary to immediately stop the reaction of nuclear fission. Therefore, the control system of the reactor must maintain the rate of nuclear fission reaction constant, and the reactor shutdown facilities can be provided by inserting control rods immediately [7].

3.2 Safety Systems to Cool the Reactor

Thermal energy is generated even the reactor is completely shut down in the decay process for the radioactive materials to become stable nuclei. This process is called decay heat. So, the continuity of cooling of the reactor core is necessary after shutdown as the reactor core cooling during reactor operation. If there is a loss in the cooling system in the reactor, an emergency cooling system must be provided not to cause the reactor core dry and reach high temperature and resulting the core melt-down or damage [7].

3.3 Facilities to Contain Radioactive Materials

The required radioactive materials to the nuclear power plants must be provided with the multiple barriers such as fuel clad, pressure vessel and the containment to prevent the accident of radioactive materials releasing from the reactor core to the environment. So, the containments are airtight and can prevent any abnormal events or accidents. It is also used against the terroristic attack [7].

3.4 Facilities to Enhancement the Safety Facilities

The most important facilities, required to enhance the safety conditions in the nuclear power plants, are supply continuity of power distribution system, control and instrumentation system must be valid and the cooling system never to be interrupted at any circumstances [7].

4. Safety Risk Assessment and Unified Security of Nuclear Power Plants NPPs

Safety risk assessment method and unified security are proposed and applied to be studied in that case. This proposed method adopts an approach like method of security risk estimation NIST 800-30. However, unlike NIST 800-30, the proposed

method would consider both safety risks and security as shown in Figure (2), and the nine steps in this method are illustrated in the figure as shown below. The nine steps can be described in the following subsections [8, 9].

A. The System Characterization

The hardware and software of the target system are detected and identified to get the related system boundary, data properties and functionalities [9].

B. Identification of hazards, threats, initiating events and vulnerabilities

Hazards are the system components malfunctions that may result in the system failure. Threats are the possible sources of malicious attack on the system. Initiating events are the circumstances which could cause the hazards. Vulnerabilities are the system weaknesses that can be exploited by the attackers.

We can denote the relationship between safety and security as a Boolean parameter $\pi(v, t, h)$, where v is the vulnerability, t is the threat and h is the hazard. The parameter value is 1, if the vulnerability v is exploited by threat t and triggering initiating events that cause hazard h . Otherwise, the parameter value is 0 [10].

C. Control Analysis

The target of risk assessment is called *critical digital assets* (CDA), which could be any software, hardware or documents related to safety, security and emergency preparedness (SSEP) of the given target system such a nuclear power plant NPP. Adapting the levels of state-of-the-art safety integrity can be defined in IEC 61508 and NEI 08-09 to this proposed method and the safety levels are numbered from 1 to 4. Similarly, the three classes A, B, and C of the control and instrumentation systems in IEC 61226 are mapped to the security levels 4, 3 and 2, respectively. Other classes are mapped to security level 1. *The control risk* (CR) can be defined as the risk level associated with security and safety design of the critical digital assets (CDA) and is defined as the following.

$$CR(c) = \text{Max}\{(CR_{\text{security}}(c)), CR_{\text{safety}}(c)\} \quad (1)$$

$$CR_{\text{security}}(c) = \text{Max}_{\text{sec}} + 1 - L_{\text{sec}}(c)$$

$$CR_{\text{safety}}(c) = \text{Max}_{\text{saf}} + 1 - L_{\text{saf}}(c)$$

For example, for VDU, *the control risk* would be $CR(\text{VDU}) = \text{Max}\{4+1-4, 4+1-3\} = 2$. Then, for *the remote multiplexing unit* (RMU), *the control risk* $CR(\text{RMU}) = \text{Max}\{4+1-3, 4+1-2\} = 3$. This means that control risk of RMU is higher than that of VDU. These results indicate quite intuitive because (VDU) is much well protected in terms of both safety and security when compared to *the remote multiplexing unit* (RMU) [11].

D. Determination of Threat Likelihood

The classification scheme based on Klinke and Renn approach is adopted in that work for determination of threat likelihood as shown in Table 2. The values in the brackets are the *Threat Level* (TL).

We consider the VDU in nuclear power plant NPP as an example. Then, we suppose that VDU is open to the signal masquerading threat. Since the threat will have a serious consequence on safety of nuclear power plant NPP, the consequences seriousness is categorized as high for the VDU. However, since the VDU is often well protected, located in security level 4 and safety level 3, as mentioned previously, then uncertainty of consequences is low. Thus, based on classification scheme, we can obtain that signal masquerading threat t of VDU has a medium threat level, i.e., $TL(t) = 2$ [12].

E. Determination of Hazard Likelihood

If a hazard h occurs independently of a threat t , then the likelihood $p(h)$ of the hazard h occurring in the nuclear power plant NPP is proposed to be the Poisson distribution with small average value in the range from 10^{-5} to 10^{-11} . Thus, the four levels of likelihood are defined based on this range, namely $[0, 10^{-9})$, $[10^{-9}, 10^{-7})$, $[10^{-7}, 10^{-5})$, and $[10^{-5}, 1]$ which are assigned to levels $HL(h) = 1, 2, 3,$ and $4,$ respectively.

If a hazard h occurs independently of a threat t , then the likelihood $p(h)$ of the hazard h is a conditional probability $p(h|t) = p(h \cap t) / p(t)$. Since $p(h|t)$ can take any value from 0 to 1, thus the occurrence of the four hazard levels $HL(h, t)$ are defined as $[0, 0.25), [0.25, 0.5), [0.5, 0.75),$ and $[0.75, 1],$ and assigned to levels 1, 2, 3 and 4, respectively [9].

F. Asset Impact Analysis

The four possible values of *the asset impact* (AI) of *the critical digital assets* (CDA) c can be mentioned as the following.

(1) $AI(c) = 4,$ when *the critical digital assets* (CDA) performs *safety, security and emergency preparedness* (SSEP) functions. A failure of such a CDA results in the direct failure of SSEP functions.

(2) $AI(c) = 3,$ when *the critical digital assets* (CDA) can affect critical system/function and pathway. A failure of CDA results in the degraded performance of *safety, security and emergency preparedness* (SSEP) functions.

(3) $AI(c) = 2,$ when *the critical digital assets* (CDA) supports critical systems. A failure of such a CDA will not affect the performance of *safety, security and emergency preparedness* (SSEP) functions. However, the auxiliary or optional functionalities related to SSEP functions might be affected.

(4) $AI(c) = 1,$ when *the critical digital assets* (CDA) protects critical systems. A failure of such a *critical digital assets* (CDA) does not harm any *safety, security and emergency preparedness* (SSEP) functions. However, the unprotected SSEP functions might be more vulnerable to attacks [10, 11].

G. Determination of Risk

The given *critical digital assets* (CDA) c with the *vulnerability* (V) that may be exploited by *the threat* (t), which may lead to *the hazard* (h), *the security safety risk of that incident* $R(c,v,t,h)$ can be defined as follows [10].

$$R(c,v,t,h)=\pi(v,t,h) \times \max\{CR(c),AI(c)\} \times \max\{TL(t),HL(h,t)\} \quad (2)$$

H. Control Recommendations

This method assessed the risk levels into four levels. The corresponding measures of the design basis threat (DBT) must be obtained. For example, the critical risk level immediate and strict control mechanisms to mitigate the risk which would be employed. For the high-risk level, some strict measures, but the non-urgent ones must be applied. For the medium risk level, some monitoring must be used. For the low risk level, the logging is only required [10, 11].

CONCLUSION

There are many factors influencing the nuclear power plants safety. These factors are mainly passive and active safety systems, training, scientific knowledge of the staff, safety culture of the workers and organization and capability of supervision needed for the plants operation and maintenance. Therefore, to promote the organizational performance and safety, specific measures must be applied. For example, enhancement of safety culture of the plant workers, regular on-job training, improvement of procedure and the enforcement of supervision requirements, etc. The classification scheme based on survey and interview is high specific and comprehensive tools to be effective.

The combined safety- security risk level is estimated, and the integration of independent risk level must be considering the maximum significant actual rate. When the risk level which is assessed by the proposed method reaches its maximum value, then the suggested countermeasures to eliminate the risk occurrence would be more complete, intensive and efficient.

Tables

Table1. Mortality rate per billion kWh for different types of power plants

Type of power plant	Rate of Mortality per billion kWh
Nuclear Power Plant	0.04
Oil-fired power plant	36
Natural gas-fired power plant	4
Coal-fired power	100
Hydro power plant	104
Wind power plant	0.15
Solar energy power plant	0.44
Biomass/Biofuel energy generation	24

Table2. Threat Level in the Proposed Method

Seriousness of consequences	Uncertainty of consequences		
	Low	Medium	High
Low	Low (1)	Low (1)	Low (1)
Medium	Low (1)	Medium (2)	High (3)
High	Medium (2)	High (3)	Very High (4)

Figures

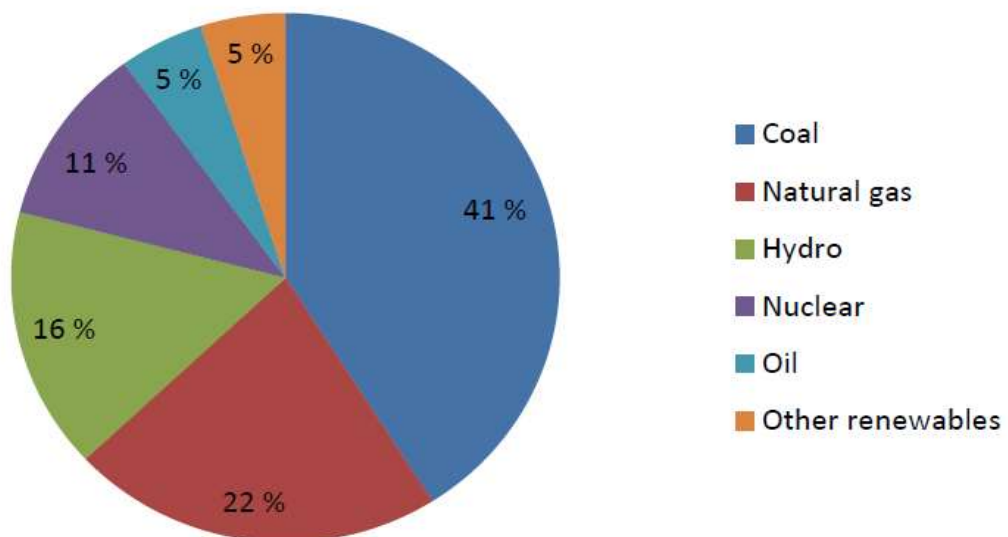


Fig. 1. Percent of each energy generation type in all over the world

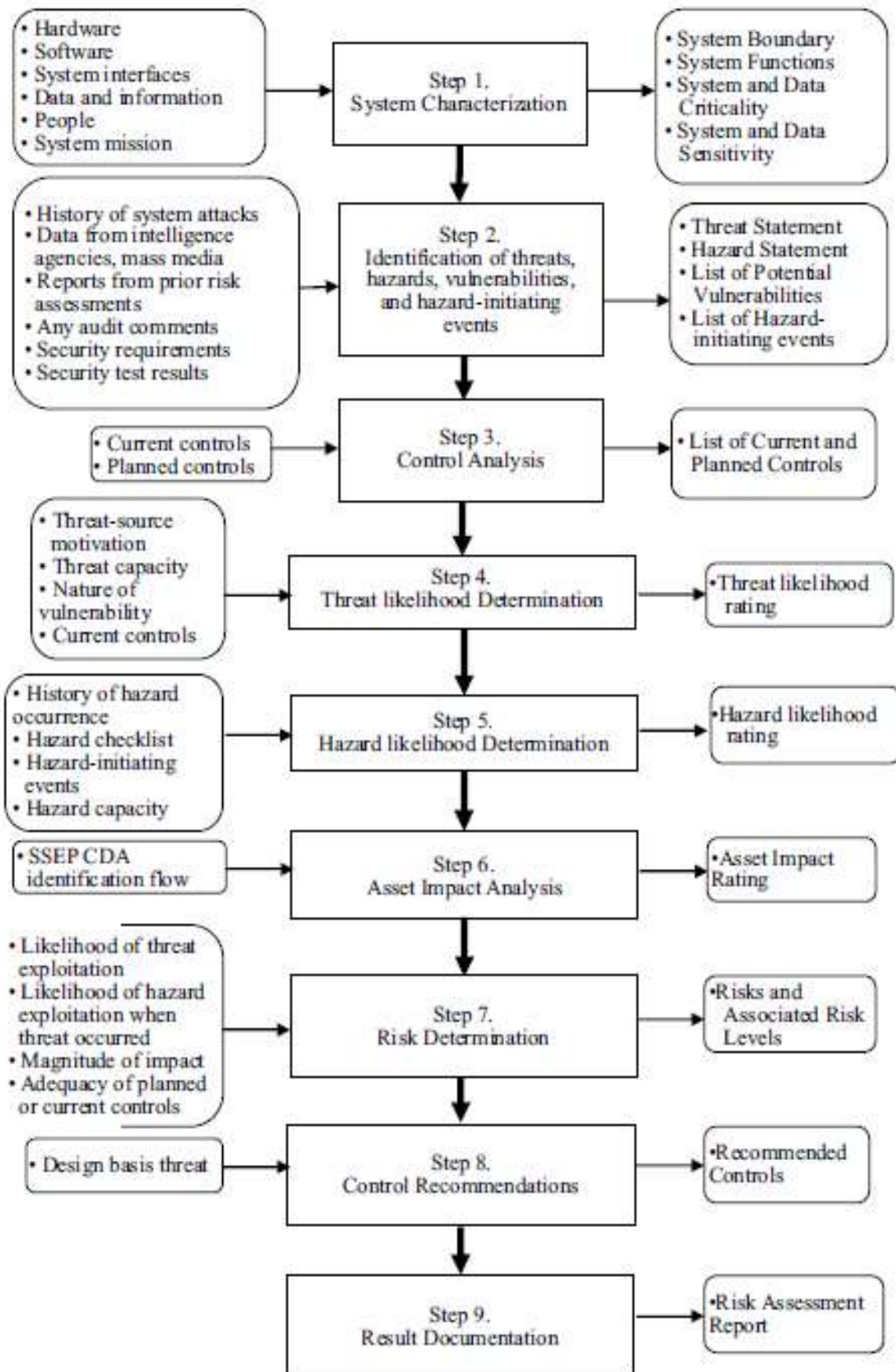


Fig. 2. Safety Risk Assessment Method and Unified Security

ACKNOWLEDGEMENT

The authors would to thank all members of the organizing team of the 9th International Scientific Conference 2018, and the rapporteur of the 11th International conference on electrical engineering ICEENG 2018, Maj. Gen. R. Assoc. Prof. Ahmed E. Abdalla, Military Technical College, Cairo, Egypt, for their great efforts to organize this beneficial and interesting conference. They also would to thank all authors in the conference for their scientific adding and valuable participation.

REFERENCES

- [1] Hannah Green, Radiological and Environmental Impact of Nuclear Accidents - a Case Study of Japan's Fukushima Daiichi Nuclear Power Plant, Master of Science in Radiation and Environmental Protection, School of Physics, University of Surrey, September 2011.
- [2] D. Lightfoot, et al., Nuclear fission fuel is inexhaustible, CNS Climate Change Technology Conference, May 10–12, 2006, Ottawa, Ontario, Canada, 2006.
- [3] Charles E. Till, Yoon Il Chang, Plentiful Energy – The Story of the Integral Fast Reactor, Amazon, 2011.
- [4] Jarkko Ahokas, Kristiina Söderholm, The Role of Nuclear Power in the Future Energy System, International Journal of Contemporary Energy, Vol. 2, No. (1), 2016.
- [5] Jarkko Ahokas, Kristiina Söderholm, The Role of Nuclear Power in the Future Energy System, International Journal of Contemporary Energy, Vol. 2, No. (1), 2016.
- [6] Ramón A. Alvareza, Stephen W. Pacala, James J. Winebrake, William L. Chameides, Steven P. Hamburg, Greater focus needed on methane leakage from natural gas infrastructure, Proc. Natl Acad. Sci. U.S.A. 109 (2012) 6435–6440.
- [7] IPCC, Climate Change 2013, The Physical Science Basis, Glossary, World Meteorological Organization (WMO), United Nations Environmental Program (UNEP), Geneva, 2013.
- [8] NEI 08-09 “Cyber Security Plan for Nuclear Power Reactors,” Nuclear Energy Institute, 2011.
- [9] L. Pietre-Cambacedes and M. Bouissou, “Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes),” in Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC), Turkey, pp. 2852-2861, October 2010.
- [10] T. Aven, “A unified framework for risk and vulnerability analysis covering both safety and security,” Reliability Engineering & System Safety, Vol. 92, No. 6, pp. 745-754, 2007.
- [11] C.-F. Chuang and H.P. Chou, “Investigation of Data Communication Systems in Lungmen Nuclear Power Plant Project,” IEEE Transactions on Nuclear Science, Vol. 53, No. 3, pp. 1443-1449, June 2006.
- [12] O. Renn and A. Klinke, “A New Approach to Risk Evaluation and Management: Risk-based Precaution-based and Discourse-based Strategies,” *Risk Analysis*, Vol. 22, pp. 1071-1094, 2002.