ANNALS of the ORADEA UNIVERSITY.
Fascicle of Management and Technological Engineering, Volume X (XX), 2011, NR2

PROBABILISTIC SAFETY ANALYSIS (PSA) IN SAFETY MANAGEMENT OF CRITICAL INFRASTRUCTURES

Olga Bucovetchi, Petronela Cristina Simion, Cristian-Aurelian Popescu
University "Politehnica" of Bucharest,
olgabucovetchi@yahoo.com, cristinas_upb@yahoo.com, crispopescu_12@yahoo.com

Keywords: safety management, critical infrastructure, nuclear power plant

Abstract: Safety management is a process in which industries and producers, societal representatives and the public interact in finding a balance between the benefits, costs and risks of products, activities and processes. The purpose of the present paper is to provide a theoretical framework for studies of safety management in high-risk industries or activities with safety as an important concern. Safety functions for preventing or mitigating the accidents, and the associated systems necessary to carry out the safety functions are evaluated by probabilistic safety analysis (PSA).

1. Introduction

Successive federal US government reports, laws, and executive orders have refined, and generally expanded, the number of infrastructure sectors and the types of assets considered to be "critical" for purposes of homeland security.
If vulnerabilities in these infrastructures are exploited, our nation's critical infrastructures could be disrupted or disabled, possibly causing loss of life, physical damage, and economic losses (Simion and Popescu, 2009).
Nuclear power plants (NPP) are considered critical infrastructures by most countries, and they spent a lot of efforts for identifying and implementing the appropriate measures to eliminate or reduce the risk impact involved in their operations (Simion *et. al.*, 2010).
Safety management is a process in which industries and producers, societal representatives and the public interact in finding a balance between the benefits, costs and risks of products, activities and processes.
Over the past decade managers of utilities and nuclear power plants (NPPs) have been confronted with a number of new challenges. Especially aging plants and equipment (OECD/NEA 2000), the ongoing generation turnover (OECD/NEA 2001), and the deregulation of the electricity market (Bier et al. 2001) have been shaping the aim and nature of managerial concerns and responsibilities. The managers have responded in different ways. For example, outsourcing and the use of subcontractors in general have accelerated as a means of optimising the use of resources and introducing cost savings (Kettunen et al. 2004a).
The purpose of the present paper is to provide a theoretical framework for studies of safety management in high-risk industries (nuclear power plants) or activities with safety as an important concern. Safety functions for preventing or mitigating the accidents, and the associated systems necessary to carry out the safety functions are evaluated by probabilistic safety analysis (PSA).

2. Safety management of the NPP critical infrastructures

Safety management of nuclear power plants (NPPs) raises concerns that are more demanding than for many other industries. For example, issues associated with information management are of crucial importance because public confidence in nuclear power influences the survival possibilities of the industry. Another strategic issue concerns the high requirements attached to systems for quality management – a subject that needs much effort and attention and also exposes the nuclear sector for extensive regulatory

demands. External political uncertainties also present obstacles for the selection of long-term investments strategies. Moreover, and the most important in this context, the deregulation of the energy market forces a need for more cost-effective production. To be able to direct attention and manage issues such as those mentioned above is not an easy task given various resources constrains. Consequently, management groups are looking for concepts, tools and techniques that can support and optimize safe and efficient operation (Rollenhagen, 2006).
For an effective safety management it is also imperative to acknowledge the nature of the organizational culture. In order to maintain internal cohesion, "culture" forms routines, preconceptions and rules of thumb, and hence it inherently resists outside change. Furthermore, inputs from the outside are interpreted within the existing cultural framework of thinking. Organizational culture acts as much as a blindfold as an asset if not reflected upon actively. (Alvesson 2002 p. 119; Kunda 1992; Trice & Beyer 1993) Managers are as much a part of the culture as the workers. Their ability to become aware of and question the cultural assumptions is thus limited. Actually, some characteristics of the culture may better be perceived at "lower" levels of the organization, were e.g., the financial pressures and outside influences do not "distort" the picture as much. Especially in light of the current (perceived) increase in economic pressures it is imperative for managers to better grasp the realities and constraints of work at the shop-floor level (Reiman and Oedewald, 2006).

3. Probabilistic Safety Analysis (PSA) – important tool in safety management of NPP

An important tool while managing the safety of the NPP critical infrastructures is probabilistic safety analysis (PSA). PSA supports both the design of a nuclear power plant (NPP) and the safety management and control of a NPP all through its service life. PSA methodology integrates information about operating practices, operating histories, component reliability, human behaviour, thermal response of the hydraulic plant, accidents and associated phenomena, potential environmental and health side-effects (Simion and Popescu, 2009). There are three levels of PSA as presented below.

Level 1 is the first part of PSA. The level 1 PSA should identify the accident sequences leading to the damage of the NPP core, and to determine their probabilities. PSA is documented in such a way that at least the following matters can be logically traced from the assumptions to the final results (STUK, 2003):

- overall description of the plant
- determination, description, categorization and frequency estimation of initiating events
- success criteria for the safety and support systems, and descriptions of physical assessment methods used for their determination
- event trees for each of the initiating event categories (Event Tree Analyses)
- description of accident sequences and procedures used for their determination
- human reliability analysis
- analysis of dependencies and common cause failures
- fault tree analysis including descriptions of systems and functions (Fault Tree Analyses)
- reliability data including expert judgment with necessary arguments

- importance measures for basic events and systems
- uncertainty analysis
- results and their evaluation with conclusions.

The level 2 PSA is to determine the amount, probability and timing of radioactive substances to be released out from the containment. The assessment should cover the leaks, damage, controlled releases of radioactive substances and bypass sequences of the containment.

The level 2 PSA introduces the interface between level 1 and 2: description of the plant damage states used at level 2, division of level 1 minimal cut sets to level 2 plant damage states, and the model of dependences of the level 2 systems and functions from the level 1 systems.

Also, the level 2 (STUK, 2003) embraces:

- estimation of the amounts of radioactive substances released from the damaged reactor core into the containment and estimation of the transportation and retention of radio-nuclides
- estimation of the amounts, quality, altitude and lifetime of various radioactive substances released to the environment, and the respective probability estimation
- assessment of the appropriateness and efficiency of the strategy of accident management.

The level 3 PSA analyses the risk to the people and environment – caused by the release of radioactive substances.

PSA is one of the most efficient and effective tools to support the decision making process for the safety and risk management of nuclear power plants.

4. Conclusions

The nuclear power industry as a whole makes a rather unique and consistent community. One factor connecting utilities, licensees, contractors, regulators as well as researchers world-wide is the recognition of the paramount importance of safety. In practice this means that most technical modifications as well as major organizational change initiatives are usually subjected to a rigorous safety analysis before their implementation is approved, and that the relative weight of safety clearly exceeds that of other matters – such as sole technical or economic considerations – in the decision-making process.
The recent literature is rich in methods and instruments used to analyse the threats, risks, vulnerabilities, and safety of the critical infrastructures. Considering the specific strengths of the PSA method, it currently looks like one of the most effective and efficient instruments for the NPP risk and safety management, decision making process. It should be continuously applied, developed and improved, mainly for the PSA levels 2 and 3.

Generally speaking, safety management entails the establishment of a management process committed to determining the threats to a system or its environment, the risk level of a particular activity or product, and instances in which deviations from normal or desired processes can be associated with risks.

REFERENCES

1. Alvesson, M. (2002). Understanding organizational culture. Sage, London.
2. Bier, V.M., Joosten, J.K., Glyer, J.D., Tracey, J.A., Welch, M.P. (2001). Effects of deregulation on safety: Implications drawn from the aviation, rail, and United Kingdom nuclear power industries (NUREG/CR-6735). Washington DC: U.S. Nuclear Regulatory Commission.
3. Kunda, G. (1992). Engineering culture: Control and commitment in a High-Tech corporation. Temple University Press, Philadelphia.
4. Kettunen, J., Mikkola, M., Reiman,T. (2004a). When availability counts – Key concepts, constraints and challenges of outsourcing in the nuclear power industry. In K.S. Pawar, C.S. Lalwani, & J. Shah (eds.) Proceedings of the 9th International Symposium on Logistics: Logistics and global outsourcing (pp. 552-558). Nottingham: Centre for Concurrent Enterprise, University of Nottingham.
5. OECD/NEA (2000). Nuclear power plant life management in a changing business world. Workshop proceedings, Washington DC, USA, 26-27 June 2000. Issy-les-Moulineaux: OECD Nuclear Energy Agency.
6. OECD/NEA (2001). Assuring future nuclear safety competencies. Specific actions. Issy-les-Moulineaux: OECD Nuclear Energy Agency.
7. Rollenhagen, C. (2006). Nordic perspectives on safety management in high reliability organizations: Theory and applications. Chapter 7. Edited by Ola Svenson et al. Stockholm University, Sweden.
8. Reiman, T., Oedewald, P. (2006). Organizational Culture and Social Construction of Safety in Industrial Organizations. Edited by Ola Svenson et al. Stockholm University, Sweden.
9. STUK (2003). Probabilistic Safety Analysis in Safety Management of Nuclear Power Plants. Guide YVL 2.8. Radiation and Nuclear Safety Authority (STUK), Helsinki.
10. Simion, C., Popescu, C.A. (2009). Considerations Regarding Risk Management Of Nuclear Power Plant As A Critical Infrastructure. Proceeding of the 4th International Conference Of Management And Industrial Engineering, Management In The Worldwide Contemporary Challenges, Bucharest, Romania.
11. Simion, C.P., Gheorghe, A., Popescu, A.C., Scarlat, C., Alexe, C.M. (2010). Defining nuclear power plants as critical infrastructures. Proceedings of the International World Energy System Conference (WESC 2010). July 1-3, 2010. Targoviste, Romania.
12. Trice, H.M., Beyer, J.M. (1993). The cultures of work organizations. Englewood Cliffs, NJ:Prentice Hall.