INTEGRATING RISK MANAGEMENT AND SAFETY CULTURE IN A FRAMEWORK FOR RISK INFORMED DECISION MAKING

William R. Nelson
Det Norske Veritas (U.S.A.), Inc.
1400 Ravello Drive
Katy, Texas 77449 USA
Bill.Nelson@dnv.com

Abstract

Operators and regulators of nuclear power plants agree on the importance of maintaining safety and controlling accident risks. Effective safety and risk management requires treatment of both technical and organizational components. Probabilistic Risk Assessment (PRA) provides tools for technical risk management. However, organizational factors are not treated in PRA, but are addressed using different approaches. To bring both components together, a framework of Risk Informed Decision Making (RIDM) is needed. The objective tree structure of the International Atomic Energy Agency (IAEA) is a promising approach to combine both elements. Effective collaboration involving regulatory and industry groups is needed to accomplish the integration.

1. Introduction

Risk management and safety culture are both receiving significant attention and development in the commercial nuclear power industry, both from the regulatory side and the industry side. Formal PRAs are being extensively used to help guide operational and regulatory decisions, for example, to establish maintenance and surveillance intervals for critical safety-related equipment. However, much work remains to be done to effectively utilize and communicate the results produced by risk professionals so that they can be put to practical use at the management level in nuclear utilities and regulatory bodies. In addition, more work is needed to develop ways to combine probabilistic risk information with other types of information to support safety, economic, and operational decisions.

At the same time, significant attention is being given to the identification and implementation of principles for effective safety management at nuclear utilities. It is now recognized that once issues of equipment reliability are addressed, an additional level of increased safety can be gained by the implementation of effective safety management and human performance systems. In particular, there is increased recognition in the nuclear industry and other high-risk industries (e.g. aviation, petrochemical and health care) that one of management's greatest responsibilities is to cultivate an effective safety culture within their organization. To address this need, regulatory bodies and utilities are expending significant effort to develop instruments for measuring safety culture, and best practices for addressing perceived deficiencies in safety culture. Unfortunately, industry-wide consensus regarding the optimal way to address safety culture has been exceptionally difficult to obtain, especially in the United States.

To reach maximum levels of nuclear safety, both technical risk management (as captured in a PRA) and organizational safety management (as represented by safety culture assessment) need to be improved and integrated so that the full spectrum of risk information can be communicated, understood, and utilized. This integration is necessary in order to make the regulatory and operational decisions that are required for safe and efficient generation of energy from nuclear power, and for the overall health of the commercial nuclear power industry.

This paper presents concepts for combining risk management and safety culture to form a framework for risk informed decision making that can be used to maximize the use of all kinds of risk information for effective operation and regulation. In addition, the RIDM framework can be helpful in mutual understanding and alignment of industry and regulatory perspectives regarding effective operation and regulation of nuclear power plants. To help achieve these goals, Det Norske Veritas (DNV) is working to facilitate the development of next-generation risk management methods for the nuclear industry and we are actively soliciting partners for this important effort.

2. Essential elements of effective safety and risk management

Before addressing RIDM in depth, some background on the overall foundation of effective safety and risk management is helpful for establishing context. There are some fundamental principles that seem to apply across multiple high-risk industries.

This work was initially stimulated by questions such as:

- Why do catastrophic accidents continue to happen in some industries?
- Why haven't safety and risk management tools been more effective in preventing and mitigating accidents?
- Are such events the inevitable remnant of our inability to identify and manage accident risks, or is there a fundamental problem with our safety and risk management methods?
- What are the critical components of an effective safety and risk management system at the facility, national, and international level?
- What are the critical success factors necessary to ensure that organizational performance objectives are achieved while controlling accident risks?

To help address these questions, DNV reviewed the responses of different industries to catastrophic accidents that influenced the entire industry. Included in this review were the nuclear industry response to the accident at Three Mile Island (TMI), the National Aeronautics and Space Administration's (NASA) response to the Challenger and Columbia accidents, and the oil industry response to the Texas City refinery accident. Based on the review, DNV believes that certain components are necessary for effective safety and risk management, and in turn are essential for organizational success:

1. **Effective risk management culture –** Safety and risk organizations and systems should be integrated with management and operational cultures.

2. **Effective paradigm or "map" of the system –** This is used to guide design, define safe operations, and select corrective actions during accidents. An example is the critical safety function concept developed in the nuclear industry following the accident at TMI.
3. **Effective tools for decision making –** Procedures, flow charts, and/or software are needed to guide information gathering and risk informed decision making.
4. **Effective measures of process performance –** Meaningful measures of process performance must be defined and communicated in a language understood by all the communities (e.g. engineering, management, operations and regulators).
5. **Effective lessons learned systems –** Lessons learned should be identified and applied to continuously improve safety and risk management, prevent the recurrence of events, and share experience within the organization, across the industry, and even between industries.

One of the most important (and often neglected) of these factors is the paradigm or map of the system. The proper selection of the paradigm can make the difference between success and catastrophe in an emergency situation, and the change of paradigm can lead to significant gains in safety and performance. An example is the transition of nuclear power plants in the US from a failure-oriented, event-based paradigm with the addition of a success-oriented, critical function-based paradigm following the accident at TMI. The subsequent improvement of performance of nuclear power plants in the US, and the lack of a TMI-class accident in the intervening years, suggests that there is much to be gained by adding a success perspective to the typical approach to risk management.

3. Sample applications of operational risk management in the nuclear industry

Following TMI, a period of soul-searching occurred across the entire US nuclear industry. It was readily apparent that a failure to effectively address the root cause of the accident, or the occurrence of a similar accident at a nuclear power plant elsewhere, would likely lead to the closure of all US plants and the demise of the entire US nuclear industry. As it was, the US nuclear industry suffered a financial setback and loss of public confidence from which it is only now beginning to emerge.

Following the TMI accident, Bill Corcoran of Combustion Engineering Inc., one of the US reactor vendors, introduced a success-oriented paradigm for accident management that he referred to as Critical Safety Functions [1]. The concept is based on the premise that there are a small number of critical safety functions (e.g. core heat removal, reactivity control and containment integrity) that must be maintained at all times during normal and emergency operations. These critical safety functions are concise descriptions of the key barriers for defense in depth in the nuclear power plant. During an accident the focus is to assess the health of the critical safety functions, and to select actions that can prevent the safety function from being lost or to restore it if it is already compromised. The function-based emergency procedures are then organized to provide guidance for assessing the health of the critical functions and selecting a "success path" using available resources to protect or restore the challenged functions. This approach does not require the correct diagnosis of the event that

resulted in the current situation, and therefore can provide guidance for corrective actions across the full spectrum of possible events.

In more recent years, there have been many significant activities in the US nuclear industry to develop risk informed applications and to institute risk informed regulatory processes. For example, the South Texas Project (STP) nuclear power plant has instituted risk informed applications in support of many major operational and maintenance decisions, and developed a risk management infrastructure for integrating risk management processes into the overall organization [2]. Anecdotal evidence suggests that the working environment at STP has become significantly more relaxed since these measures have been implemented, "because we always know where we are in risk space."

The US Nuclear Regulatory Commission is making steady progress towards incorporating the risk informed perspective into regulatory and licensing processes, and in developing a totally new risk-informed, performance-based licensing process for future plant designs [3].

Overall, the TMI accident led to fundamental changes in the way the US nuclear industry views and manages nuclear safety, including the introduction of the success-oriented critical function approach. While it is difficult to conclusively prove a direct link, it appears that these changes have had a significant influence on improving plant performance and safety. As an example, the average capacity factor of US nuclear power plants has increased from approximately 56% to more than 90% in the years since the TMI accident [4] [5].

4. NASA example of operational risk management

NASA has an inherent interest in risk informed approaches to mission planning and operation, as their primary objective is to successfully complete a variety of space missions while minimizing risks for loss of mission or crew. Until recently, their approach to risk management had been primarily failure oriented, using the same methods of PRA made popular by the nuclear industry. However, in recent years NASA has increased the emphasis of real-time risk management for on-orbit applications, which included an examination of the potential benefits of success-oriented approaches. One of these efforts led to the development of a concept called the Mission Success Framework.

The Mission Success Framework was developed in work for application of real-time risk management in the Mission Evaluation Room for the International Space Station (ISS) [6]. The Mission Success Framework is built upon the critical safety function approach described above, and other applications including emergency procedures for a test reactor [7] and identifying the information needs of nuclear reactor operators for responding to severe core damage accidents [8]. The critical function-based logic tree structures developed in these earlier studies were adapted for application to the ISS.

The major features of the Mission Success Framework are as follows:

- A clear definition of the mission of the system and the measures of mission success

- A complete catalog of the hardware, software, human, and organizational resources available to achieve the mission
- A description of the critical functions that must be maintained to achieve mission success
- Identification of the types of challenges that may endanger the critical functions
- Identification of the "success paths" that can be used to maintain or restore the critical functions when the challenges occur
- Rules and guidance for selecting the best success paths for responding to any combination of critical function challenges
- Identification of the information required to monitor the health of the critical functions and the performance of the success paths

Some benefits of the mission success framework include:

- It can serve as the foundation for group decisions in real-time risk and fault management.
- It provides a powerful tool for modeling system interdependencies, and the effects of those interdependencies on any number of real or hypothetical accident scenarios.
- It can be combined with a systematic information requirements analysis to help identify additional tests needed to isolate the root cause of an event.
- It serves as a fundamental "map" of the problem solving space for anomaly resolution.
- It explicitly compensates for the fact that not all possible scenarios can be pre-analyzed.
- It provides a means to derive corrective actions for the full range of events that could challenge the mission-significant critical functions.
- It provides a means to incorporate information from multiple disciplines and place it within a common framework for evaluation. In this way, all disciplines can be represented and systematically considered in light of mission success.
- It provides a natural means to integrate both success- and failure-oriented risk models for effective risk management. Failure-oriented models can focus on event diagnosis, and success-oriented models can focus on event mitigation and achieving overall mission success.

It seems that the mission success framework is applicable to organizations as well as hardware systems. DNV is currently exploring application of the concept to combine technical risk and management systems (including safety culture) within an integrated tool for effective risk informed decision making.

5. Risk informed decision making

Efforts are underway in the worldwide nuclear industry to develop RIDM concepts to combine probabilistic risk information with many other types of information (e.g. deterministic, financial, political and environmental) to support effective, collaborative decision making. According to the International Atomic Energy Agency [9]:

> "RIDM is a discipline. It starts with a need, an issue or situation for which a decision is required. It involves considering, weighing, and integrating often complex inputs and insights from traditional engineering (deterministic)

> analyses, probabilistic analyses, operational experience, compensating or mitigating measures, or other pertinent considerations. It considers each aspect in context with each other aspect and with the whole. It assesses conformance to guidance or criteria. It involves assessing safety or risk. It involves a way of thinking to integrate such inputs, insights, and assessment to result in safe, sound, and optimum management or operational actions or decisions. The discipline, while having static aspects, is fundamentally dynamic or fluid and is sensitive to responsible long term and near term feedback; it is ongoing. Responsible feedback can and should influence management or operational decisions or actions, previous decisions or actions, or the implementation of the discipline itself."

While such a definition is obviously very imprecise, it provides a useful starting point to stimulate the development of techniques to more effectively utilize risk information in the overall management processes for complex process facilities. Towards this end, DNV is exploring the application of the Defense in Depth objective tree structure developed by IAEA [10] as a vehicle for implementing effective RIDM. The objective tree structure is a hierarchy that defines the critical functions that must be maintained to protect defense in depth barriers, the challenges that may compromise the critical functions, the mechanisms which could induce the challenges, and the risk management strategies that can be used to prevent the challenges and thereby protect or restore the critical safety functions. Figure 1 is an example of a portion of a defense in depth objective tree for maintaining reactor coolant system (RCS) cooling.

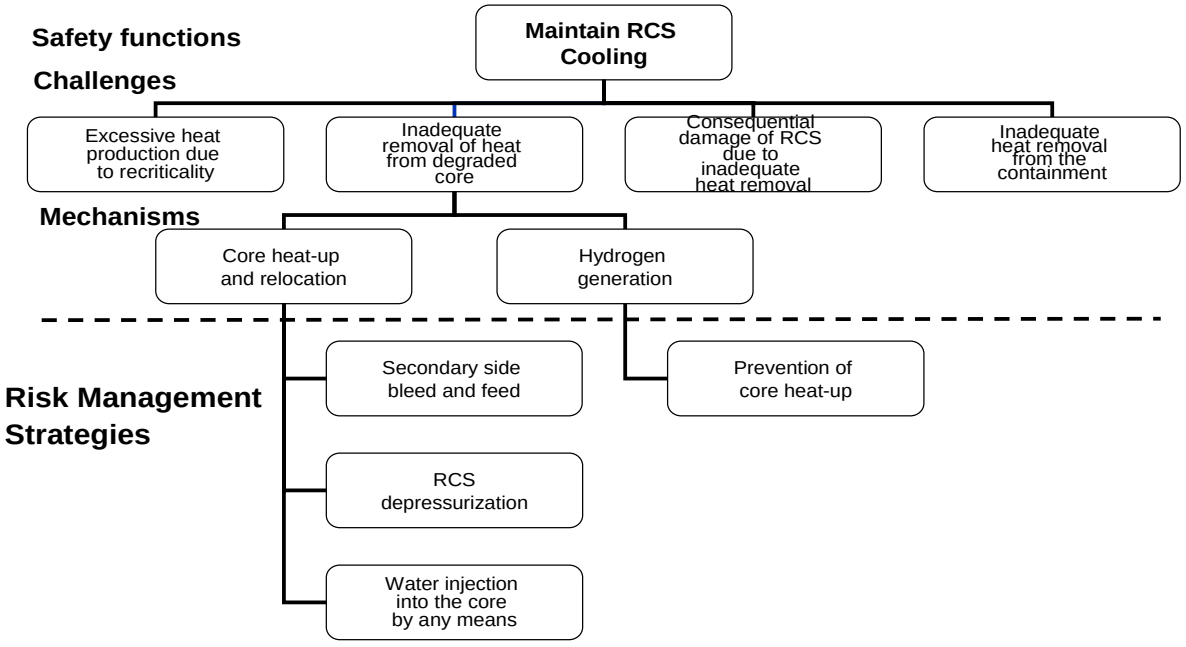

Figure 1 Sample objective tree for maintaining RCS cooling [10]

Benefits of the defense in depth objective tree structure include:

- It provides a common, goal-oriented language to integrate diverse sources of information to support risk informed decision making.
- It allows treatment of management systems and safety culture along with technical risk, and provides a direct link between them.
- It shows how any combination of failures affects the critical safety functions, and how mitigation strategies can address multiple risks.
- It can be directly linked to probabilistic risk assessment fault tree and event tree models and quantitative results.
- It allows systematic evaluation of potential risk management strategies.
- It aligns with operational decision making and accident management.
- It allows the evaluation of operational experience and formulation of lessons learned.

NASA is using a very similar framework in their program for RIDM [11]. The approach uses an "objectives hierarchy" to organize information regarding the objectives that must be accomplished to guarantee mission success. The objectives hierarchy includes technical, financial, safety, and stakeholder support components, thus providing the basis for integration of technical and non-technical components of mission success. Supporting the objectives hierarchy are the performance measures that are used to monitor and achieve mission success and the failures or challenges that can occur that could endanger mission success. Figure 2 shows the NASA framework for RIDM.

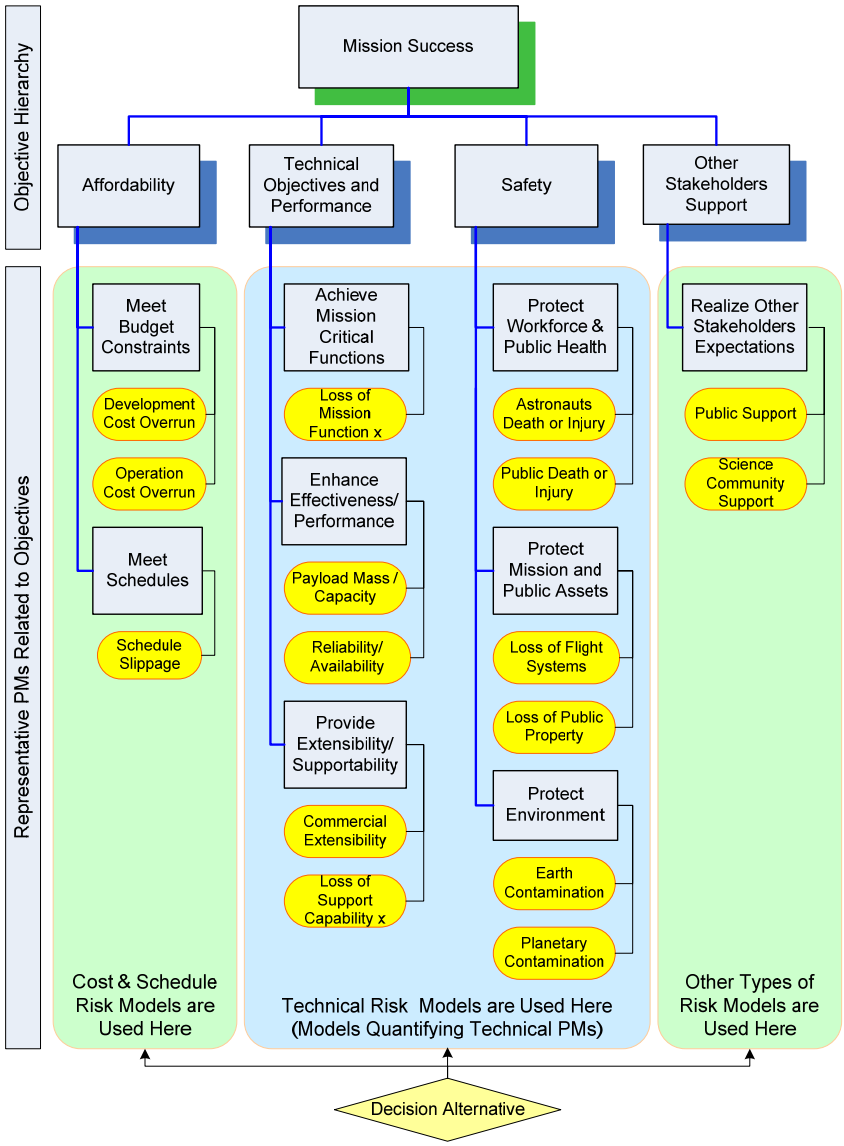

Figure 2 NASA Framework for risk informed decision making [11]

6. Developing a risk management culture

As described above, one of the critical elements of effective safety management and RIDM is an effective risk management culture. By this is meant an organizational culture in which effective risk management practices are integrated with the operational and management systems and decision processes. While there is a significant overlap with the more commonly used term "safety culture," an effective risk management culture does not attempt to capture the more elusive concepts regarding the attitudes and opinions of an organization's employees. In this

sense risk management culture should be somewhat easier to define and measure, and the assessment of its influences on safety and risk should be easier to establish.

The Electric Power Research Institute is engaged in a program called Risk Management Effectiveness Assessment (RMEA) [12] that attempts to define the attributes of an effective risk management culture. While full application of this concept has not been tested, it appears that organizations that have an effective risk management culture do benefit from corresponding improvements in operational safety and performance. It will be very important to further explore the assessment of risk management culture and to implement the experience gained. This provides a more direct route to safety improvement than waiting for the research that will be required to fully understand and implement effective safety cultures.

7. Development needs for risk informed decision making

Now that many of the essential tools of safety and risk management have been developed and demonstrated, additional work is necessary to integrate them into an effective framework for RIDM. For example, a framework should be developed that effectively integrates probabilistic information with other types of risk information (e.g. deterministic calculations, regulatory, plant performance, and financial). Methods should be developed to present and visualize risk information to support collaborative decision making by stakeholders. The framework should also be capable of combining management systems and safety culture with the technical risk information so that the risk influence of safety culture changes can be understood and communicated.

The RIDM framework should be based on performance and risk measures that are directly tied to process safety, critical safety and economic functions, and organizational goals. The framework should be usable both to pre-analyze and develop strategies for events that might occur, and then to evaluate and manage events that are in progress. Finally, a common language is needed that can communicate risk across discipline boundaries, at all levels of the organization, and with external stakeholders. This language should also align with operations including real-time risk management.

8. Integrating risk management and safety culture for risk informed decision making

It is certainly not an easy task to effectively integrate risk management and safety culture in order to enable RIDM, but it is essential for the next level of improvements in safety and risk management. Part of the difficulty comes from the inherently different viewpoints of the underlying disciplines (i.e. engineering vs. the social sciences). The following is the outline of a strategy that DNV is pursuing to address these issues.

The first step is to develop an objective tree structure that includes all the organizational goals and critical functions, including safety, performance, and economic considerations. Then, all of the resources and strategies – hardware, software, management systems, safety culture, etc. – that contribute to the protection of the critical functions are identified. Next, the measures for

assessing the health of the critical functions and the performance of the risk management strategies are identified. Selection criteria are defined for selecting a mitigation strategy for each real or hypothetical challenge to the critical functions. Finally, the objective tree structure is maintained and exercised throughout the system lifecycle (i.e. concept development, design, operation, performance monitoring, incident investigation, and development of lessons learned).

Figure 3 shows how technical risk and safety culture elements can be incorporated into a common safety objective tree.

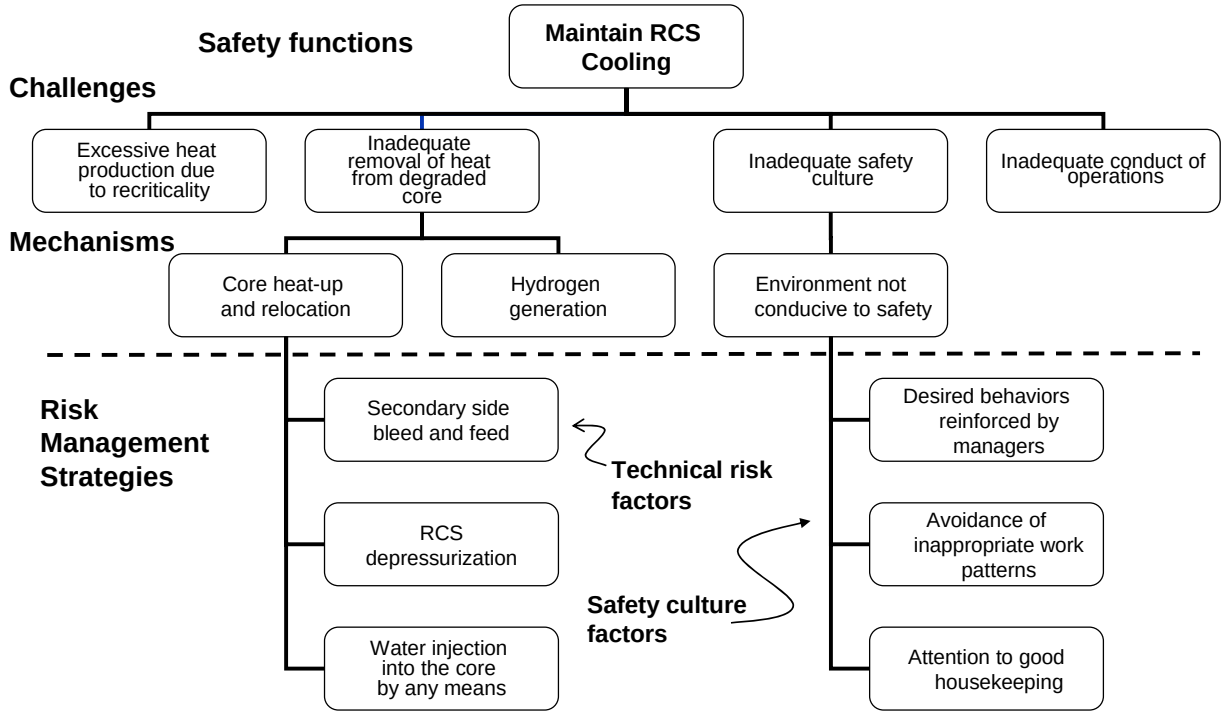

Figure 3 Objective tree combining technical risk and safety culture factors

9. The need for regulatory and industry alignment for risk informed decision making

There is a significant need to align industry and regulatory treatment of risk information for making operational and regulatory decisions. In the US, the parallel paths taken by industry and the regulator are illustrated by the risk informed applications that have been developed by many utilities, and by the risk-informed, performance-based Reactor Oversight Process used by the Nuclear Regulatory Commission to monitor a plant's safety performance and determine the degree of regulatory oversight that is required. Development of a common framework for RIDM can help align these approaches for currently operating plants. This need for alignment will be even more critical to enable the licensing and regulatory processes to meet the demands for the

coming generation of new plants. Not only will the number of license applications stretch the ability of the regulatory process to accommodate the workflow, the use of new plant designs and technologies will require that a flexible RIDM framework be developed so that the regulation and operation of such a diverse fleet of new and existing plants can be managed in a coherent and consistent manner.

10. Concepts for cross-industry collaboration on risk informed decision making

DNV is actively working to facilitate cross-industry collaboration aimed at understanding and testing the concepts of effective RIDM, using a combination of failure- and success-oriented analysis tools. The following steps are envisioned to carry out this collaborative effort:

- Identify the requirements for effective application of RIDM.
- Develop a framework and methods to integrate probabilistic information with other types of risk information (e.g. deterministic, regulatory, performance and economic); present and visualize risk information to support collaborative decision making; and tie management systems and safety culture to technical risk.
- Develop performance and risk measures that are tied to process safety, critical functions, and organizational goals that can be clearly understood across disciplines and be directly manipulated.
- Develop a common language that communicates risk across discipline boundaries, at all levels of the organization and with external stakeholders, and that aligns with operations including real-time risk management.
- Test methods and tools in pilot projects with participating organizations.
- Develop a guide for the implementation of effective RIDM.

DNV has begun making contact with organizations in the nuclear, space, commercial aviation, and oil and gas industries to identify areas of common interest and to develop a framework for collaboration to make progress towards these important goals. A similar effort is already underway in the commercial aviation industry in the US. The Federal Aviation Administration and other US government agencies are working together to develop the Next Generation Air Transportation System (NextGen). A key component of this program is the development of a framework for safety management that will combine the technical aspects of safety and risk management with the organizational factors including safety culture.

11. Conclusions

In recent years significant advances have been made in the development and application of methods to assess the technical aspects of risk in nuclear power plants. At the same time, progress has been made in methods for assessing the organizational factors that must be controlled for effective safety and risk management. One of the organizational factors that is currently receiving much attention is safety culture. Many approaches have been suggested for assessing and managing safety culture, although consensus has not yet been reached between industry and regulatory bodies on the most effective ways to address these issues.

To fully experience the benefits of safety and risk management for nuclear power plants, the technical and organizational factors that influence risk should be integrated in a common framework for RIDM. The safety objective tree structure developed by the IAEA shows promise as a potential foundation for this integrated treatment of technical risk and safety culture. A concentrated effort involving both regulatory and industry organizations is needed to fully define the optimal approach and to test the benefits of this integrated framework for RIDM. To help achieve these goals, DNV is working to facilitate the development of next-generation risk management methods for the nuclear industry and we are actively soliciting partners for this important effort.

12. References

[1] W. R. Corcoran et al., "Nuclear Power-Plant Safety Functions," *Nuclear Safety*, Vol. 22-2, March/April 1981, pp. 179-191.

[2] C. R. Grantom, "Risk Manager Infrastructure Elements for Nuclear Power Stations," American Nuclear Society Utility Working Conference, Amelia Island, Florida, August 2008.

[3] US Nuclear Regulatory Commission, Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing, NUREG-1860, December 2007.

[4] Nuclear Energy Institute, http://www.nei.org/resourcesandstats/documentlibrary/reliableandaffordableenergy/graphicsandcharts/usnuclearindustrycapacityfactors/

[5] John Gaertner, Ken Canavan, and Doug True, "Safety and Operational Benefits of Risk-Informed Initiatives," Electric Power Research Institute White Paper, February 2008.

[6] W. R. Nelson and S. D. Novack, "Real-Time Risk and Fault Management in the Mission Evaluation Room for the International Space Station," NASA Contractor Report INEEL/EXT-03-00661, May 2003.

[7] W. R. Nelson, "Response Trees for Emergency Operator Action at the LOFT Facility," ANS/ENS Topical Meeting on Thermal Reactor Safety, Knoxville, TN, April 7-11, 1980.

[8] W. R. Nelson, D. J. Hanson, and D. E. Solberg, "Identification of the Operating Crew's Information Needs for Accident Management," American Nuclear Society Meeting, Washington, D. C., Oct. 31 - Nov. 4, 1988.

[9] International Atomic Energy Agency, Risk Informed Decision Making, IAEA Safety Standard DS 365 (Draft), April 2008.

[10] International Atomic Energy Agency, Assessment of Defense in Depth for Nuclear Power Plants, Safety Reports Series No. 46, 2005.

[11] Homayoon Dezfuli, Robert Youngblood, and Joshua Reinert, "Managing Risk Within a Decision Analysis Framework," Second International Association for the Advancement of Space Safety Conference, Chicago, IL, May 2007.

[12] Electric Power Research Institute, Risk Management Effectiveness Assessment Application Guide, EPRI Report 1011761, December 2005.