AN APPROACH FOR RISK INFORMED SAFETY CULTURE ASSESSMENT FOR CANADIAN NUCLEAR POWER STATIONS

William R. Nelson
Det Norske Veritas (U.S.A.), Inc., Katy, Texas USA

Abstract

One of the most important components of effective safety and risk management for nuclear power stations is a healthy safety culture. DNV has developed an approach for risk informed safety culture assessment that combines two complementary paradigms for safety and risk management: loss prevention – for preventing and intervening in accidents; and critical function management – for achieving safety and performance goals. Combining these two paradigms makes it possible to provide more robust systems for safety management and to support a healthy safety culture. This approach is being applied to safety culture assessment in partnership with a Canadian nuclear utility.

1. Introduction

It is widely recognized that a healthy safety culture is a critical component of effective safety and risk management for nuclear power stations. Unfortunately, there is substantial disagreement about what constitutes an effective safety culture, and accidents and near misses continue to occur even when substantial efforts are exerted to institute safety management and safety culture programs. It is therefore apparent that something is missing in standard safety management and safety culture programs.

There is an urgent need for a safety culture assessment approach that effectively combines technical and organizational risk factors together, and which can be tied directly to objective measures of safety and risk. This is essential to ensure that safety culture assessment has a real and positive effect on safety and risk, and to ensure that risk mitigation investments are focused where they will have the maximum benefit.

The overall objectives of the DNV risk informed safety culture assessment process are the following:

- Develop a measure of safety culture that is grounded in objective measures of safety and risk
- Prevent individual events from progressing to serious accidents by slipping through the holes in the “Swiss cheese”
- Support the assessment of operational experience to identify lessons learned that will prevent not only “identical” accidents but broader categories of similar events
- Support achievement of organizational objectives for safety and performance
- Develop a common awareness of safety and performance across disciplines and at all levels of the organization

- Integrate the full spectrum of management systems on a common foundation of safety and performance objectives
- Redefine the utility-regulator engagement to enable an effective partnership for achieving safety objectives

2. Combining two complementary dimensions for safety management

Classical methods for safety management are often based on a loss prevention paradigm – that is, intervening in the progression of events to prevent the occurrence of serious accidents that would result in financial loss due to equipment damage, loss of production, injury to personnel or the public, or loss of reputation. A complementary paradigm focuses on the achievement of organizational goals including production and safety.

2.1 Loss prevention

Figure 1 shows a common graphic that illustrates the loss prevention approach – the "Swiss cheese" model developed by James Reason [1]. The diagram illustrates a number of "pathways" that are followed (e.g. by people, equipment or processes) as an event progresses from "hazards" (i.e. potentially dangerous conditions) to an accident – where significant losses to the organization may occur. The diagram also shows that the primary strategy to prevent events from progressing to accidents is to establish and maintain barriers that intervene in event progression, either physically or procedurally. Safety management then becomes an exercise to ensure that the proper barriers are in place and maintained. The primary goal for safety culture in the loss prevention paradigm is to maintain awareness of the barriers and to actively intervene in accident progression when the situation requires it.

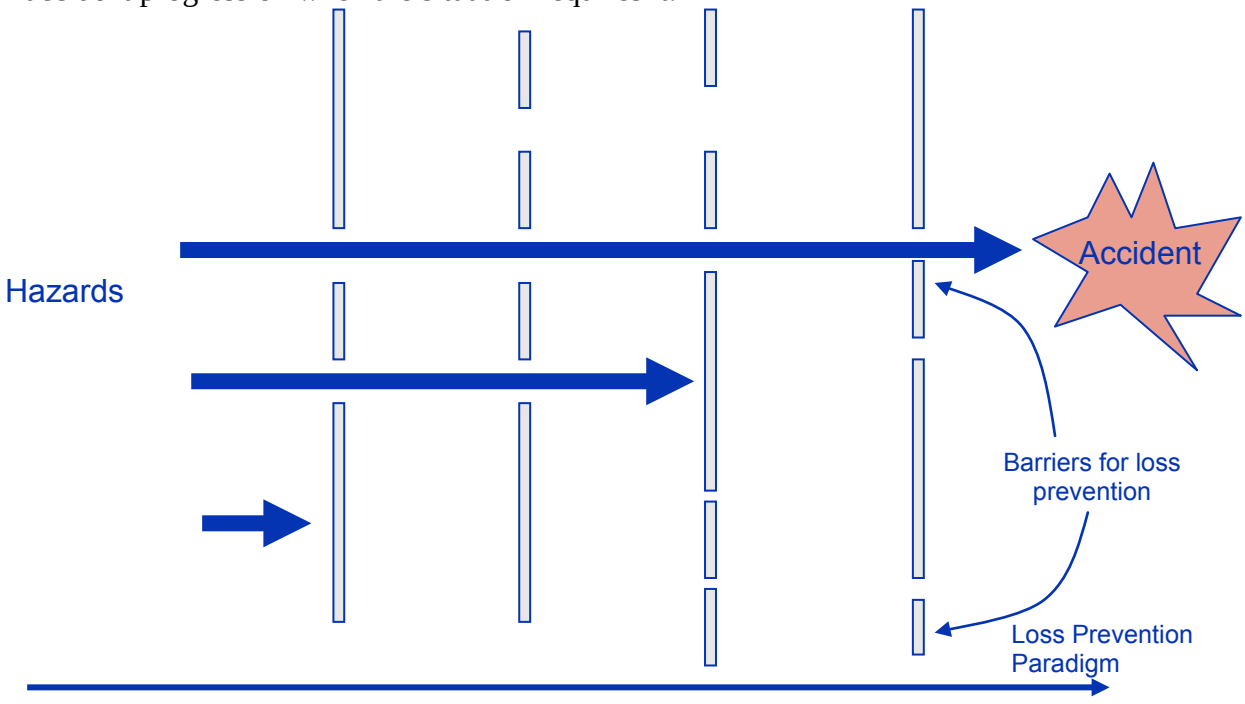

Figure 1 Loss prevention paradigm

2.2 Critical function management to achieve safety and performance goals

The concept of critical safety functions was developed in the nuclear industry following the accident at Three Mile Island. [2] Critical safety functions can be extended to the more generic term, "critical functions", to cover broader objectives – for example, production goals for a nuclear power station. Critical functions are used to ensure that the proper equipment, systems and procedures are in place to enable organizations to achieve their goals.

Figure 2 shows how the addition of the critical function perspective can be used to supplement the loss prevention perspective. In this case the goal is to move towards the top of the diagram, i.e. to achieve the organization's production and safety goals. Resources are made available to help the organization achieve these goals, and information systems are used to help personnel understand the critical functions and the current situation relative to the achievement of the goals. In this paradigm, safety culture is concerned with awareness of the health of the critical safety functions and effective decision making to support the achievement of the organization's safety goals.

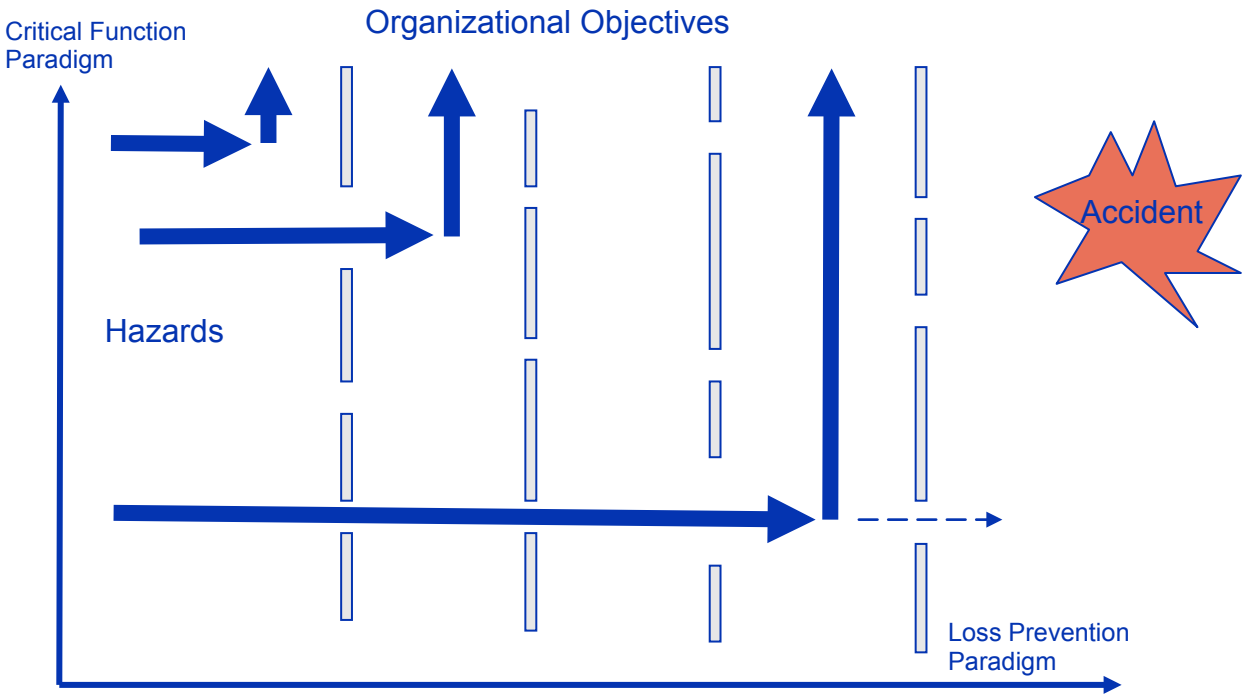

Figure 2 Combining the loss prevention and critical function paradigms

By combining the loss prevention and critical function paradigms, a very robust system for safety and performance management becomes possible.

3. Attributes of a healthy risk informed safety culture

The DNV approach to risk informed safety culture assessment is based on the concept that effective safety management and safety culture can be described by the attributes described in the following sections.

3.1 Awareness of barriers and critical functions

People at all levels of the organization and across disciplinary boundaries must have adequate awareness of the barriers and critical functions. This includes awareness of the function and health of the critical functions and barriers, and the implication of individual actions on the critical functions and barriers.

3.2 Commitment to safety and performance goals

Another important component of risk informed safety culture is the commitment at all levels of the organization to prevent accidents and to achieve organizational and safety objectives.

3.3 Information systems and tools to enable risk informed decisions

Organizations must provide effective systems and tools that allow employees to make effective risk informed decisions for preventing accidents and to achieve organizational safety and performance goals.

4. The importance of healthy regulatory engagement – “going the second mile”

Regulatory relations are sometimes viewed only as a necessary cost of doing business. However, nuclear utilities should recognize that healthy relations with regulatory organizations play a vital role in maintaining safety and achieving performance goals. By providing a complementary perspective and set of eyes for monitoring processes for safety and risk management, effective partnership between the regulator and utility can help both organizations achieve their respective responsibilities towards shareholders and citizens. Effective utility–regulator engagement is analogous to the statement, “If someone forces you to go one mile, go with him two miles.” Going the first mile under duress is hallmark of standards-based compliance. Compliance is only the starting point for excellence in safety and plant performance. Effective collaboration between regulatory and industry groups is needed to ensure that effective measures for safety management and safety culture are implemented in the Canadian nuclear industry. The key to “going the second mile” is to agree on the destination.

5. Tools for risk informed safety culture assessment

The DNV approach for risk informed safety culture assessment uses two basic analytic tools to organize safety and risk management information: objective trees and bow tie diagrams. These tools are described in the following sections.

5.1 Bow tie diagrams

Bow tie diagrams are very effective tools for representing information regarding the loss prevention paradigm for safety management. Bow tie diagrams were developed in the offshore oil and gas industry, and were originally applied primarily to identify physical barriers for preventing and mitigating catastrophic events such as fires and explosions. More recently however, they have been applied to a broader spectrum of potential events and to cover organizational barriers as well as physical barriers.

Figure 3 shows the basic structure of a bow tie diagram. The circle at the center of the diagram shows the "top event" – i.e. the occurrence of a serious accident resulting from a specific type of hazard. On the left side of the diagram are the potential causes of the top event and the barriers (either technical or organizational) that could prevent it from occurring. On the right side of the diagram are the potential consequences of the top event, barriers that can be used to mitigate or control the consequences, and the overall effects that could result from the occurrence of the accident.

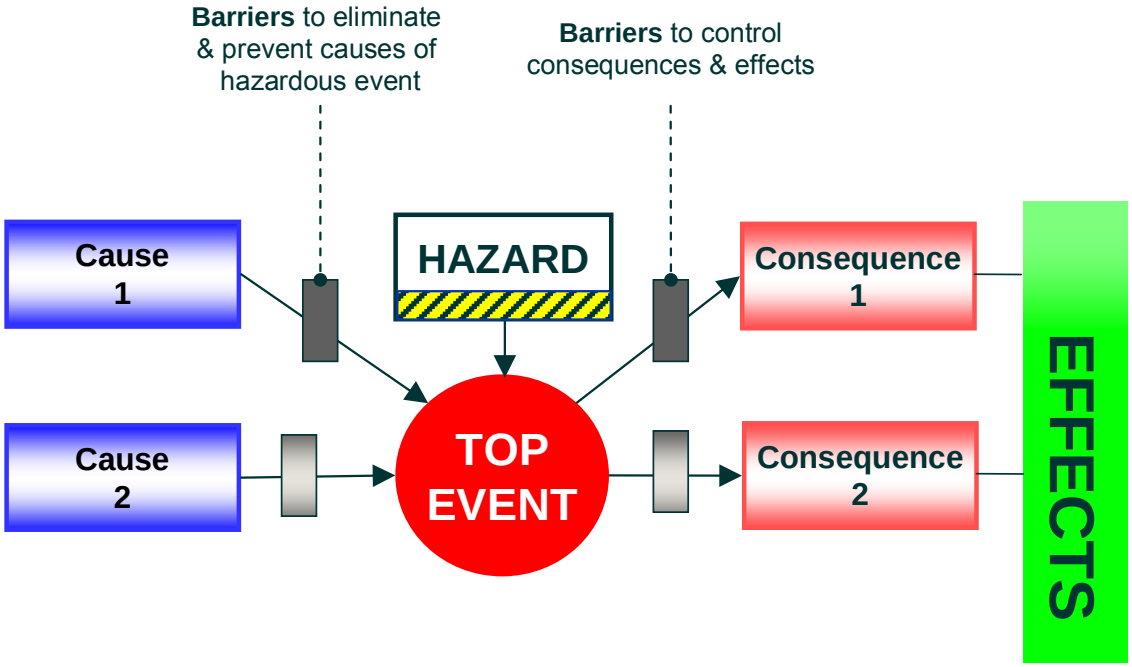

Figure 3 Example bow tie diagram

Bow tie diagrams and other forms of barrier analyses have been used successfully for many years in the offshore oil and gas industry, and are increasingly accepted by regulatory bodies as

an effective means to document and maintain safety management systems. New methods are being developed to incorporate processes and tools into ongoing barrier management to ensure that barriers are continuously maintained and to facilitate communication of critical safety information throughout the organization.

5.2 Objective trees

Various forms of objective trees for critical function management have been developed and applied since the accident at Three Mile Island (TMI). Even prior to the TMI accident the Idaho National Engineering Laboratory (INEL) developed a form of objective trees called response trees that were used to organize the emergency procedures for the Loss of Fluid Test (LOFT) facility, a test reactor that was used to test the performance of emergency core cooling systems during a loss of coolant accident (LOCA). [3] Following the TMI accident the Combustion Engineering (CE) Owner's Group created a variation of response trees called Resource Assessment Trees to organize information in the Emergency Procedure Guidelines for CE nuclear power plants. The INEL developed a more generic version called safety objective trees to study information requirements for Severe Accident Management in a study for the US Nuclear Regulatory Commission. [4] Finally, the International Atomic Energy Agency (IAEA) developed another variation called defense in depth objective trees to illustrate strategies for maintaining defense in depth for nuclear power plants. [5] The defense in depth objective trees showed that organizational factors could be treated together with technical risk factors in the same objective tree structure.

Figure 4 is an example of the basic defense in depth objective tree structure that we are using in our approach for risk informed safety culture assessment. It includes levels that describe the critical safety functions; the challenges that could endanger the critical safety functions; specific mechanisms that could lead to the critical function challenges; and risk management strategies that can be used to prevent or mitigate the challenges and thus protect the critical safety functions.

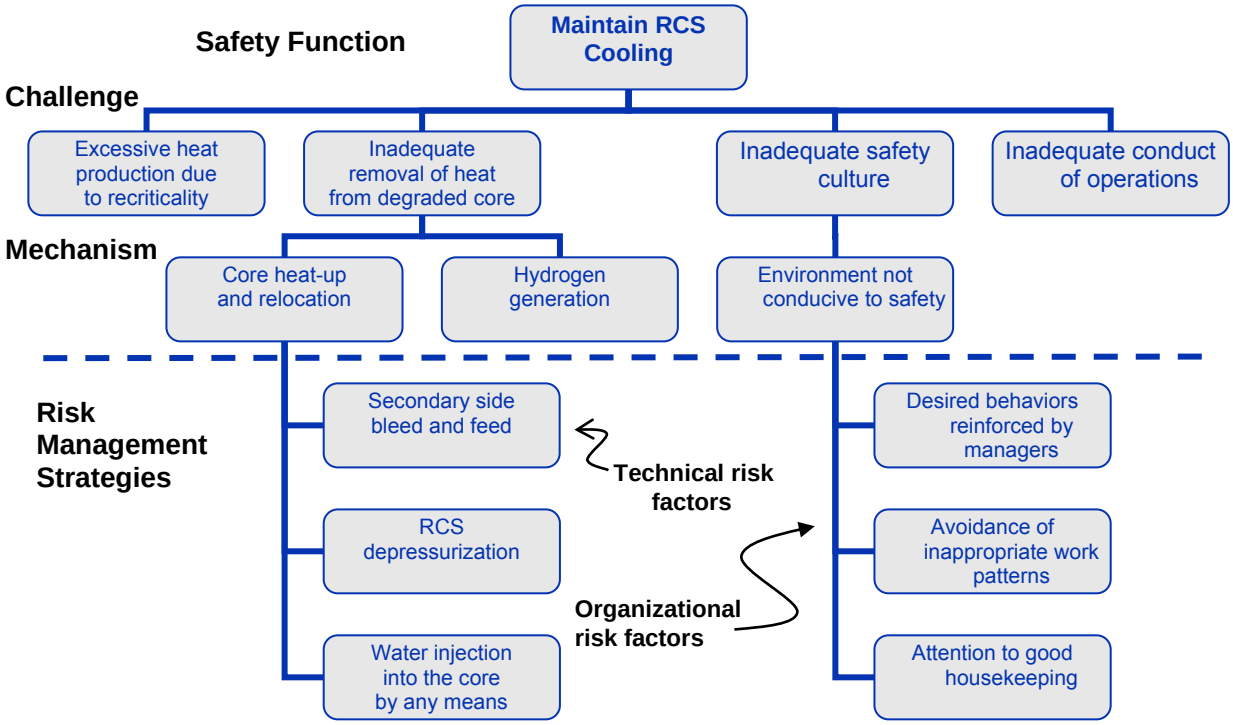

Figure 4 Example defense in depth objective tree

5.3 Combining objective trees and bow tie diagrams for safety and performance management

Figure 5 shows how bow tie diagrams and objective trees can be linked together to provide integrated treatment of both the critical function and loss prevention paradigms for safety and performance management. Events at the Challenge and Mechanism levels of the objective trees can be linked directly to bow tie diagrams that illustrate how these events can be prevented and/or mitigated through the application of technical or organizational barriers. These events can also be directly linked to quantified risk assessment methods such as Probabilistic Safety Assessment (PSA).

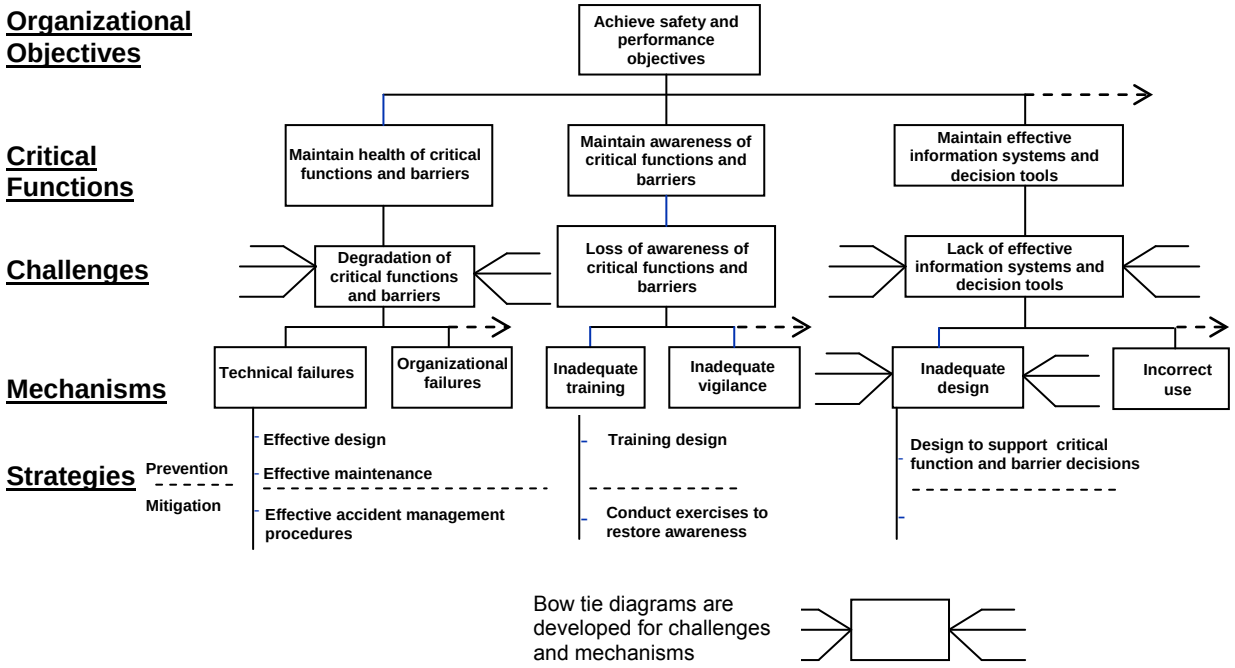

Figure 5 Combining objective trees and bow tie diagrams for risk informed safety culture assessment

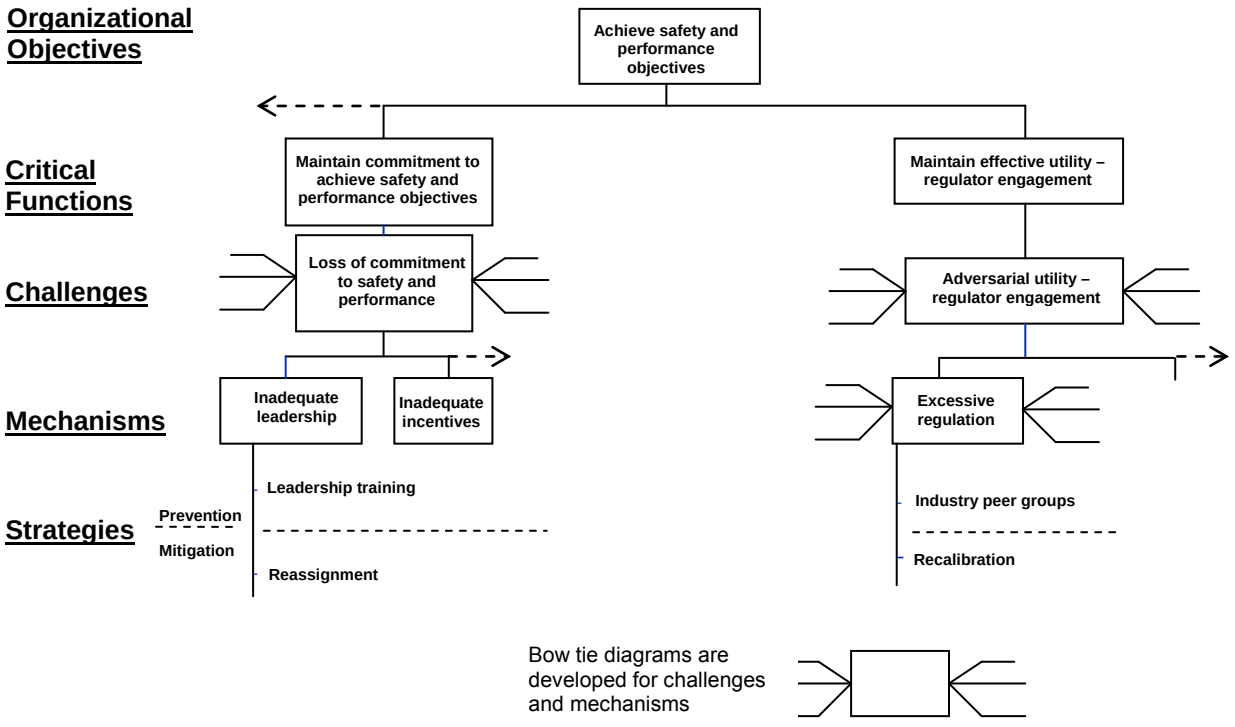

Figure 5 (cont.) Combining objective trees and bow tie diagrams for risk informed safety culture assessment

6. Application of the tools for safety culture assessment

The bow tie diagrams and objective trees provide a systematic way to organize knowledge regarding accident prevention and mitigation as well as the critical functions required to achieve organizational performance and safety goals. The next step is to define the measures that determine how well this knowledge is utilized in the operation of the nuclear power station. The fundamental metrics are focused on:

- Measures of the health of the critical function
- Measures of the health of the barriers for accident prevention and mitigation
- Employee awareness of the barriers and critical functions
- Employee awareness of how their actions influence the performance of the critical functions and barriers
- Employee and management commitment to maintain the critical functions and barriers
- Availability and effectiveness of information systems and tools for maintaining the critical functions and barriers

A protocol is then developed for interviewing a cross section of employees across disciplines and all levels of the organization to evaluate the current status of the measures and identify steps necessary for improvement.

7. Benefits of risk informed safety culture assessment

Some of the benefits of the bow tie-objective tree approach for risk informed safety culture assessment include the following:

- The approach can be applied in a consistent manner across all components of the management system and to identify risk mitigation measures across functional, technical and operational boundaries
- Management attention can be focused on the most critical areas for maintaining the barriers and critical functions
- Balanced attention can be given to both technical and organizational factors
- Lessons learned can be interpreted and summarized across events to help prevent similar accidents and not just identical ones
- Owners can be assigned to barriers and critical functions to ensure that they are maintained in a healthy condition
- Measurement of the health status of critical functions and barriers can be a reliable “leading indicator” of safety and process performance
- The approach aligns well with World Association of Nuclear Operators (WANO) and Institute of Nuclear Power Operations (INPO) safety culture assessment processes, while focusing attention on the most risk critical areas

8. Conclusions

DNV has developed an approach to risk informed safety culture assessment that combines two complementary perspectives for safety and performance management: the loss prevention

paradigm and critical function paradigm. By combining these two paradigms it is possible to provide effective processes and tools that enable a healthy safety culture and to provide objective means for safety culture assessment. We are currently working in partnership with a Canadian nuclear utility to apply risk informed safety culture assessment as part of their overall management systems assessment. We are also working to organize a Joint Industry Project to fully explore the potential of the approach.

9. References

[1] James T. Reason, Managing the Risk of Organizational Accidents, Ashgate Publishing, 1997.

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

[3] 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.

[4] 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.

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