INL/CON-11-21720
PREPRINT

Assessing Risk and Driving Risk Mitigation for First-of-a-Kind Advanced Reactors

ASME SMR 2011

John W. Collins

September 2011

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint should not be cited or reproduced without permission of the author. This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this paper are not necessarily those of the United States Government or the sponsoring agency.

Proceedings of the ASME 2011 Small Modular Reactor Symposium
SMR2011
September 28-30, 2011, Washington, DC, USA

6585

ASSESSING RISK AND DRIVING RISK MITIGATION FOR FIRST-OF-A-KIND ADVANCED REACTORS

John W. Collins
Idaho National Laboratory
Idaho Falls, ID, USA

ABSTRACT

Planning and decision making amidst programmatic and technological risks represent significant challenges for projects. This presentation addresses the four-step risk assessment process needed to determine a clear path forward to mature needed technology and design, license, and construct advanced first-of-a-kind nuclear power plants, including Small Modular Reactors. This four-step process has been carefully applied to the Next Generation Nuclear Plant.

INTRODUCTION

This paper defines the scope and methodology for identifying and quantifying risks and for developing the risk handling and risk workoff strategy to enhance project success. This methodology was used for the Next Generation Nuclear Plant and can be applied to all projects including other advanced reactor concepts. This paper also describes the NGNP Risk Management System (RMS). The RMS is a relational database developed in Microsoft® Access, which provides conventional database utility as well as a number of unique capabilities specifically designed to facilitate the development and execution of activities outlined in this paper. These include the capability to establish the risk baseline; document and analyze the risk reduction plan; track the current risk reduction status; and organize risks by reference configuration area, system, subsystem, and component. Opportunities can also be identified, tracked, and evaluated for the potential to enhance plant efficiency, reduce cost, or accelerate schedule.

Risk management is a key discipline for making effective decisions and communicating the results within and across organizations. It is used to determine the feasibility of project plans, identify potential problems that may affect life-cycle activities and the quality and performance of products, and improve the active management of projects. The purpose of risk management is to identify potential programmatic and technical problems before they occur so that actions can be taken to reduce or eliminate the probability of occurrence and/or the impact of these problems should they occur.

The structured approach defined in this paper is intended to be executed in a step-wise, iterative manner that is coordinated with established project phases and milestones.

RISK MANAGEMENT PROCESS EXECUTION

Risk management provides the structured, formal, and disciplined approach to identify and control (i.e., reduce or mitigate) above normal risks to acceptable levels using appropriate response actions. DOE Order 413.3A and its attendant DOE G 413.3-7, *Risk Management Guide*, establish a clear expectation that project personnel identify and analyze risks as early as possible in the life of a project and continue this analysis through succeeding project stages. Implementation of the process will enhance the probability of project success by improving project performance and decreasing the likelihood of unanticipated cost overruns, schedule delays, and compromises in quality and safety**.** The approach consists of the following functions and planning actions:

- Risk identification
- Risk quantification
- Risk handling strategy
- Residual risk workoff

Integration of these steps into the overall risk management process is shown in Figure 1. Tailoring of the risk management steps and associated activities, including execution guidance, is provided in the following sections. ISO Guide 73 and the INCOSE *Systems Engineering Handbook* were used for risk management vocabulary guidelines, and the process outlined in ISO/IEEE 16085 is referenced for the management of risk in the life cycle of the project.

Copyright © 2011 by Battelle Energy Alliance, LLC.
Published and used by ASME with permission

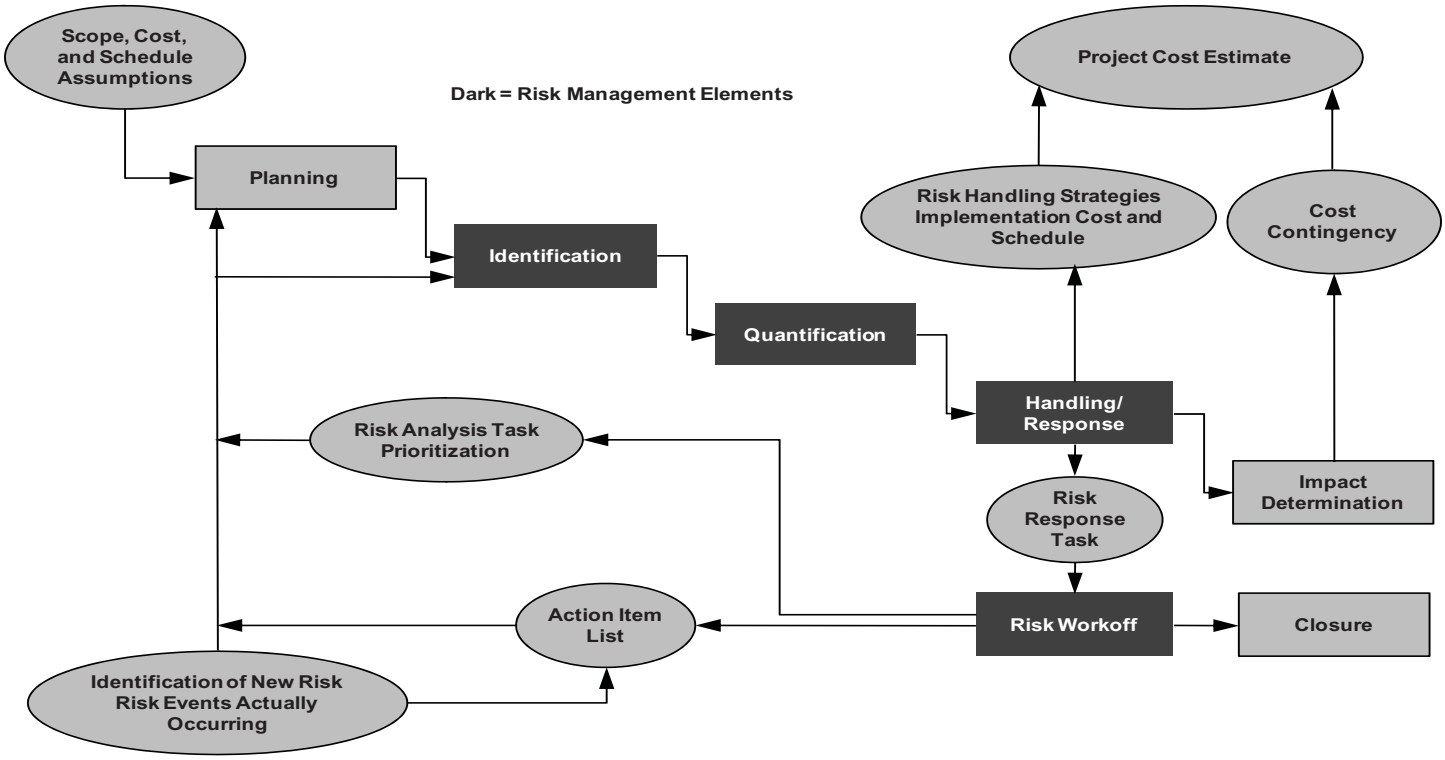

FIGURE 1. RISK MANAGEMENT FUNCTIONAL FLOW DIAGRAM

Risk Identification

The purpose of the risk identification function is to capture risk events likely to prevent the project from achieving its objectives and to document specific characteristics with a basis describing why these events are considered a risk. All identified above-normal risks are entered into the project risk management system and tracked through closure. Subsequently, risks are identified and documented, and tracking is initiated in this phase.

Because risks change as the project matures, with new risks developing or anticipated risks disappearing, risk identification is a repetitive process. Such risks include but are not limited to:

- Risks arising from the use of technologies not previously demonstrated in a relevant application or environment
- Normal and accident scenarios, including events that cause the disablement of engineered safety features (typically documented in Phenomena Identification Ranking Tables [PIRT] as produced with the Nuclear Regulatory Commission)
- Design needs that must be addressed to further detail the design.

Risks are captured in the project risk register and contain attributes that allow for ranking and understanding of each risk. The risk register is managed as part of the Risk Management System (RMS) and is available through the NGNP project. When possible, risks are assigned to specific critical areas, systems, subsystems, and components. Other key attributes are detailed below.

Risk Types. Risk types include both technical and programmatic risks and are defined in the International Council on Systems Engineering (INCOSE) *Systems Engineering Handbook*, version 3.2.1, as follows:

- ***Technical Risk*** – the possibility that a technical requirement of the system may not be achieved in the system life cycle. Technical risk exists if the system may fail to achieve performance requirements; to meet operability, producibility, testability, or integration requirements; or to meet environmental protection requirements. A potential failure to meet any requirement that can be expressed in technical terms is a source of technical risk.

- ***Programmatic Risk*** – produced by events that are beyond the control of the project manager. These events often are produced by decisions made by personnel at higher levels of authority, such as reductions in project priority, delays in receiving authorization to proceed with a project, reduced or delayed funding, changes in onrganization or national objectives, etc. Programmatic risk can be a source of risk in any other risk category.

These risks types may be further broken down and defined, as necessary, to encompass identified risks.

Product: Project Risk Register that contains:

- Risk title
- Risk description
- Affected system or structure
- Risk type (e.g., technical or programmatic).

Copyright © 2011 by Battelle Energy Alliance, LLC.
Published and used by ASME with permission

Risk Analysis and Quantification

The risks contained in the risk register are scored for probability of occurrence and severity of consequence, if realized. Here the scoring methodology is established and the basis for the scoring is well documented. Risk analysis is completed so that risks are prioritized and assigned an appropriate risk handling strategy. Risks are evaluated for each applicable scenario.

At early project stages, risks are analyzed using qualitative or semi-quantitative methods. In the case of NGNP, a semi-quantitative method was used involving calculation of a numerical risk number for each event. This risk number is based on a relative numerical value assigned to the likelihood (event probability or P_E) that a risk event will occur, the associated impacts of the risk (consequences or C), and the likelihood (P_C) that the event will result in the consequence identified. These factors are used to calculate the risk number according to the following equation:

$$Risk\ Number = (P_E \times P_C) \times C \times W \qquad (1)$$

Where:

P_E = Probability of occurrence
P_C = Probability that consequence occurs at level of severity noted
C = Consequence of occurrence (loss if event occurs)
W = Weighting factor (used to emphasize consequence of occurrence).

Values are assigned to all four factors according to the criteria in Table 1 and Table 2. In general, the discrete values shown in the tables are used in the calculation; however, exceptions can be made to increase dispersion and discriminate between risks. In this case, an appropriate basis and annotation must be provided. For the factors P_E & C, the value assigned should reflect the risk condition before implementation of the risk handling strategy. Factor P_C is set to one for the initial consequence evaluated. As other severity levels are evaluated, P_C will be varied appropriately.

TABLE 1. PROBABILITY DEFINITION

Probabilities	Range	Technology Criteria	Scale Criteria	Use for Calculation
Improbable	**< 10^{-6}**		Not evaluated since it is improbable	**N/A**
Very Unlikely	**10^{-6} to <0.1%**	Technology is well understood and is routinely used in similar, integrated applications and conditions	The scale of the system/ component needed is similar to existing successful applications.	**0.1**
Unlikely	**0.1% to <1%**	Technology is understood and has been used in applications and conditions close to, but not identical to, required conditions. A small amount of development is needed before deployment.	Majority of the components are similar in scale to existing applications.	**0.3**
Somewhat Likely	**1% to <10%**	Technology needs a moderate amount of research, development and design before deployment at required operating conditions.	About half of the components are similar in scale to existing applications	**0.5**
Likely	**10% to 50%**	Technology needs a major amount of research, development and design before deployment at required operating conditions.	Some of the components are scaled similar to existing applications, with the remainder needing significant design changes to achieve deployment.	**0.7**
Very Likely	**> 50%**	Low maturity, complex, unclear development path; multiple unproven technology must work together.	All needed components have never been attempted at the necessary scale.	**0.9**

TABLE 2. CONSEQUENCE DEFINITION

Consequence	Technical	Schedule	Use for Calculation (risk units)
Negligible	Minimal or no impact.	Schedule delays that do not affect milestones or the critical path.	**1**
Marginal	Small change needed to design or path forward. Minor damage to equipment or facilities. Minor, temporary loss of capabilities.	Schedule delays that may affect external milestones or are threatening a slip along the critical path.	**3**
Significant	Moderate change needed to design or path forward. Moderate, but repairable damage to equipment or facilities. Moderate, temporary loss of capability	Schedule delays that will slip the critical path end date by up to 6 months.	**5**
Critical	Major change needed to design or path forward, workaround available. Significant, repairable damage to equipment or facilities.	Schedule delays that will slip the critical path end date by more than 6 months but less than 1 year.	**7**
Crisis	Major change needed to design or path forward, no workaround available now. Loss of equipment or facilities.	Schedule delays that will slip the critical path end date 1 year (schedule slips in excess of 1 year are anticipated to cause a loss of the program).	**9**

Copyright © 2011 by Battelle Energy Alliance, LLC.
Published and used by ASME with permission

Risk numbers are used to prioritize risks and determine the risk level (i.e., very low, low, moderate, high, or very high) of each event. Risk levels are used to tailor appropriate risk handling strategies and define tracking requirements. Levels can generally be defined by the following criteria:

- ***Very-Low Risk.*** A risk identified as *very low* has virtually no potential for impacting the project or the consequences are exceptionally minor. No oversight is necessary.
- ***Low Risk.*** A risk identified as *low* has little potential for impacting cost, schedule, or performance requirements and is probably mitigated with standard cost or schedule contingency. Minimum oversight is needed to ensure the risk remains low.
- ***Moderate Risk.*** A risk identified as *moderate* has a reasonable probability of impacting cost, schedule, or performance requirements and in turn requires additional management actions above the normal contingency and project controls.
- ***High Risk.*** A risk identified as *high* has a strong possibility of a major impact to the project and will require additional significant action to control risk (e.g., comprehensive analysis and a formal risk handling strategy).
- ***Very-High Risk.*** A risk identified as *very high* is almost certain to occur and/or have a major impact on the project. Like a high risk, it will also require considerable action to control the risk (e.g., comprehensive analysis and formal risk handling strategy).

Assign Risk Level. The risk level is assigned automatically by the RMS. The risk number ranges shown in Table 3 are based on a default value of 1.0 for probability of consequence (P_C).

Product: Quantified project risk register with documented basis for scoring, which adds the following to the risk register:

- Probability Scores and Basis
- Consequence Scores and Basis
- Risk Score.

Risk Handling Strategy

Risks are mitigated by applying a systematic approach to maturing the technology through research and development, modeling, testing, and design. Tasks needed to mature the technology and reduce project technical risk are developed and documented in a Technology Development Roadmap (TDRM).

Risk response (also termed risk handling) identifies the course of action or inaction selected to effectively manage each risk item. The risk response function documents that either a given risk is acceptable to the project (as is) or defines actions that will be taken to make an unacceptable risk acceptable to the project. Risk handling strategies are selected after the probable impact on the project has been determined so that the strategy is appropriate for the level of risk. A risk handling strategy (i.e., accept, mitigate, avoid, or transfer) is selected for all identified above-normal project risks. The risk response is the detailed tasks that are performed to execute the risk handling strategy.

Risk owners are responsible for selecting the risk handling strategy and, when required, for developing the associated risk response approach (including specific actions) for assigned risk items. The handling strategy, response approach (optional), and actions are documented and presented to the risk management team. The assembled risk management team reviews all risk responses and makes any necessary adjustments to reach team consensus. The agreed-upon risk responses are then entered into the risk register and tracked. The following sections provide additional information to be used in performing the risk response planning function.

TABLE 3. RISK LEVEL MATRIX

Probability \ Consequence	Negligible	Marginal	Significant	Critical	Crisis
Very Likely	Low 0.9	Moderate 2.7	High 4.5	Very High 6.3	Very High 8.1
Likely	Low 0.7	Moderate 2.4	High 4.4	Very High 6.1	Very High 7.9
Somewhat Likely	Low 0.5	Moderate 1.9	High 3.8	High 5.3	Very High 6.8
Unlikely	Very Low 0.3	Low 1.2	Moderate 2.6	High 4.2	High 5.4
Very Unlikely	Very Low 0.1	Low 0.5	Low 1.0	Moderate 1.8	Moderate 2.7

Copyright © 2011 by Battelle Energy Alliance, LLC.
Published and used by ASME with permission

Select Risk Handling Strategy. The risk handling strategies employed by the NGNP project and consistent with DOE G 413.3-7, *Risk Management Guide*, are as follows:

- ***Risk Acceptance.*** Acceptance is a deliberate strategic decision by the project based on the understanding that it is more cost-effective to continue the project as planned, with no additional resources (e.g., time and money) being allocated to control the risk. Low risks are typically accepted. When the strategy to accept a risk is employed, the risk level remains the same (i.e., residual risk equals initial risk), but no costs or schedule impacts are incurred for risk response implementation.
- ***Risk Mitigation.*** Risk mitigation involves identifying specific steps or actions that will reduce the probability of the event or lessen the consequence of a risk if the event occurs. Since risk is defined as probability times consequence, reducing the probability or lessening the consequence of occurrence will reduce the project's exposure to a particular risk by reducing the expected value of the outcome. Mitigation can often be accomplished by taking action before the event occurs (i.e., prevention) or by identifying actions to be performed after the event occurs (i.e., contingency or recovery planning). The primary example of risk mitigation for NGNP is developing a TDRM to study, test, design, and mature technologies that will reduce the probability of occurrence as the plans defined in the TDRM are executed.
- ***Risk Avoidance.*** Risk avoidance focuses on total elimination of the potential threat, usually by eliminating the potential that the risk event can occur. This strategy requires a clear understanding of the root cause of the event. Examples of risk avoidance include totally redesigning a system or selecting an alternate technology that is not subject to the same risk. When this strategy is selected, there is a potential for implementation costs and schedule impacts. Other strategies include changing or lowering requirements while still meeting the needs of the project.
- ***Risk Transfer.*** The risk transfer strategy involves shifting the entire risk to a third party, typically after the risk is converted to a monetary amount. Private industry examples of this strategy include requiring performance bonds from subcontractors and purchasing insurance policies. For these two examples, the implementation cost is the incremental cost to the subcontract (if measurable) and the cost of insurance policy premiums, respectively. Typically, no residual risk remains after transfer.

  In DOE, the risk is transferred between federal and contractor entities via contract. Transferred risks are monitored to ensure new risks are not created and do not impact project mission and objectives.

Guidance for Risk Handling Strategy Selection. Selecting good risk handling strategies for project risks is critical, and in some cases, it may be prudent to employ something other than a conventional risk handling strategy. In that case, alternative strategies may be used for the NGNP project. While several strategies can usually be used to control a risk, the simplest and most cost-effective strategy should always be sought. This requires a thorough understanding of the risk and its causes and consequences. Table 4 shows the typical application of risk handling strategies for controlling project risks.

TABLE 4. TYPICAL APPLICATION OF RISK-HANDLING STRATEGIES FOR CONTROLLING PROJECT RISKS.

	Risk-Handling Strategies			
Risk Level	**Accept**	**Mitigate**	**Avoid**	**Transfer**
Very High		✓	✓	✓
High		✓	✓	✓
Moderate		✓	✓	
Low	✓	✓		
Very Low	✓			

The cost associated with implementing the risk response plan is evaluated against the cost and schedule impact should the risk be realized. This evaluation is a consideration used in determining which risks to accept without mitigation. For instance, if the risk response implementing costs are high in comparison to the potential cost and schedule impact of the risk, then the risk is a candidate for acceptance without mitigation. For the NGNP, the risk response plan is documented in the TDRM, the R&D Program Plans, and other planning documents. TDRMs are the high-level representation of the risk response plan and provide a systematic method to increase the technical maturity of the components while decreasing the risk of failure to meet the objective of the component function. As shown in Figure 2, risk reduction is an iterative process where the TDRM tasks (risk handling strategy) are executed, the risk is reassessed to determine risk reduction, if any, and residual risk is recalculated based on the achieved reduction. The technical maturity of the component is periodically reassessed to determine current status of the TDRM.

Product: Risk Handling Strategy which includes:

- Tasks to reduce risk – probability or consequence
- Tasks rolled up into strategies.

Residual Risk Workoff

The risk handling strategy and an evaluation of its ability to reduce the risk are captured in the RMS, a relational database that provides conventional database utility, including data maintenance, archiving, configuration control, and query ability. The tool's Hierarchy Tree allows visualization and analyses of complex relationships between risks, risk mitigation tasks, design needs, and PIRTs. The tool also depicts the planned risk reduction anticipated as the TDRM is executed, as shown in Figure 3.

Copyright © 2011 by Battelle Energy Alliance, LLC.
Published and used by ASME with permission

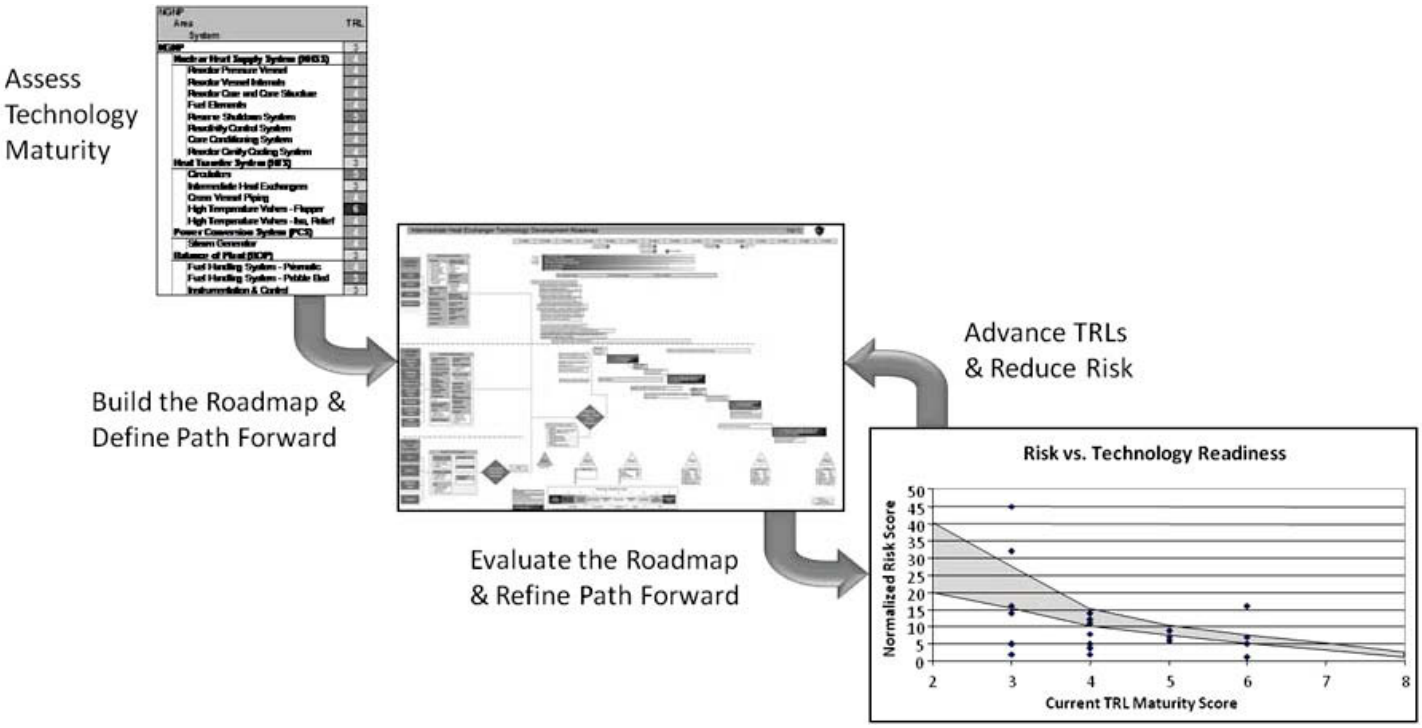

FIGURE 2. ROADMAPPING AND RISK REDUCTION – AN ITERATIVE PROCESS

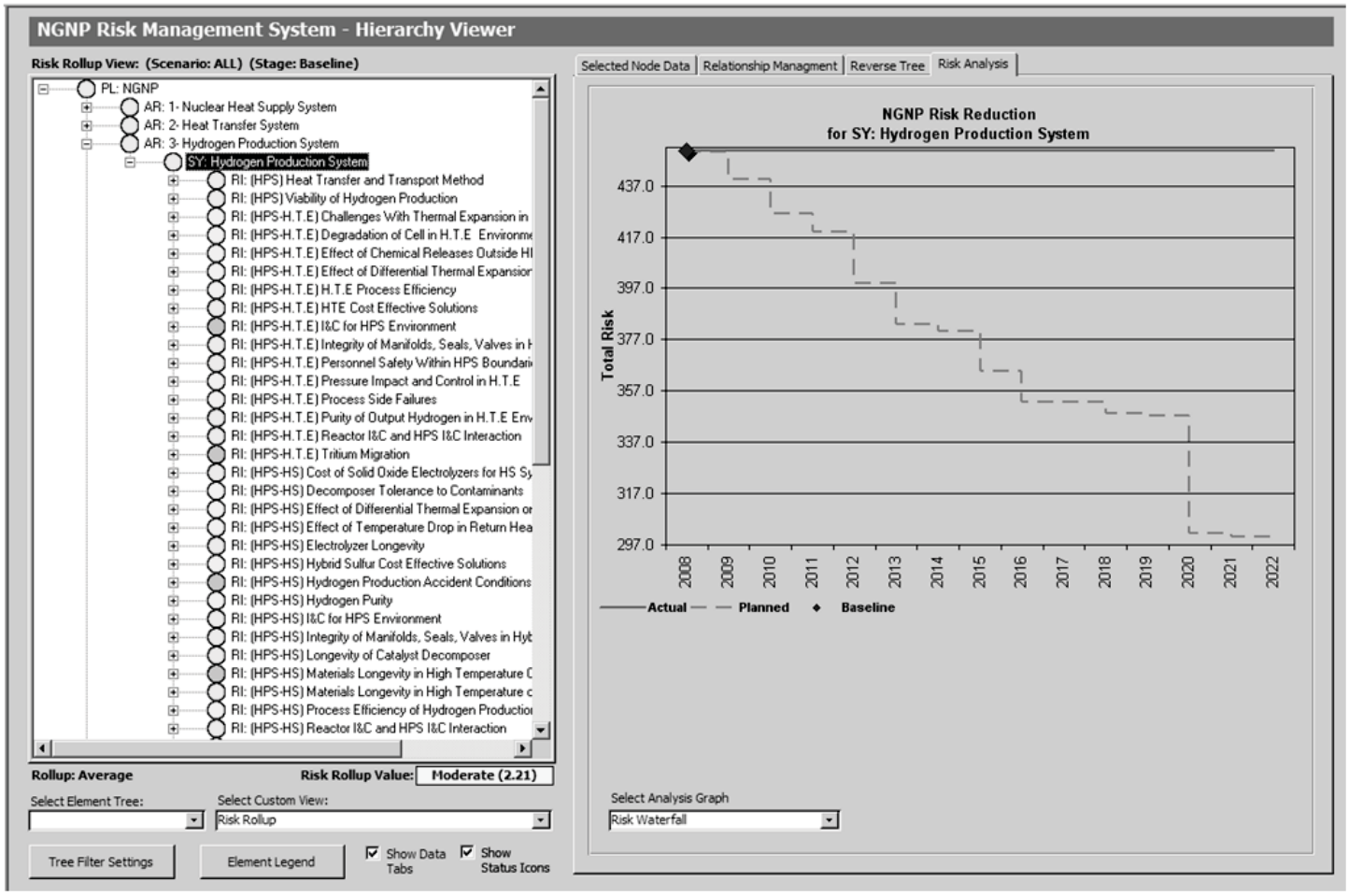

FIGURE 3. RISK REDUCTION DEPICTED BY THE RISK MANAGEMENT SYSTEM

Copyright © 2011 by Battelle Energy Alliance, LLC.
Published and used by ASME with permission

Initiate Risk-Response Action Tracking. After agreement is reached by the risk management team on the risk handling strategy, the response plan, and the residual-risk quantification; the risk response actions are entered into the RMS. The RMS provides a means for assigning action owners and action due dates.

Risks are analyzed to verify that the amount of project risk present at each of the design phases is acceptable. During the pre-conceptual design phase many of the risks will be *Very High*. As the project advances to the conceptual design phase, risk should be reduced such that no risk is higher than *High*. At preliminary design, the risks should be reduced to *Moderate*, and for final design, risks need to be reduced to *Low* and *Very Low*.

A project risk allocation matrix (not shown) was used by NGNP Engineering personnel to evaluate the technical risk associated with deploying each critical area, system, subsystem, and component and determine the risk reduced by performing each task to advance the technical maturity. This tool captures the risk reduction anticipated by each of the R&D, Licensing, and Engineering tasks forecasted in the TDRMs. The risk and risk reduction data captured using this tool was then placed in the RMS for tracking, analysis, and configuration control.

Product: Project Risk Allocation Tool and RMS, which depict the project plan to reduce risk and current progress in doing so.

ACKNOWLEDGMENTS

This manuscript has been authored by Battelle Energy Alliance, LLC under Contract No. DE-AC07-05ID14517 with the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a nonexclusive, paid-up, irrevocable, world-wide, license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes.

REFERENCES

DOE G 413.3-7, *Risk Management Guide*, U.S. Department of Energy, September 16, 2008.

DOE M 413.3-1, *Project Management for the Acquisition of Capital Assets*, Section I, Chapter 14, "Risk Management," U.S. Department of Energy, March 28, 2003.

DOE O 413.3A, *Program and Project Management for the Acquisition of Capital Assets*, U.S. Department of Energy, July 28, 2006.

INL/EXT-07-12967, *Next Generation Nuclear Plant Project Pre-Conceptual Design Report*, Idaho National Laboratory, 2007.

INL/EXT-08-15148, *Next Generation Nuclear Plant Project Technology Development Roadmaps: The Technical Path Forward*, Idaho National Laboratory, January 2009.

INL/EXT-09-16598, *Next Generation Nuclear Plant Project Technology Development Roadmaps: The Technical Path Forward for 750–800°C Reactor Outlet Temperature*, Idaho National Laboratory, August 2009.

PLN-2489, *Next Generation Nuclear Plant Project (NGNP) Preliminary Project Management Plan*, Idaho National Laboratory, October 2008.

Smith, Preston G, and Guy M. Merritt, *Proactive Risk Management*, Productivity Press, 2002.

PLN-3247, *Risk Management Plan for the Next Generation Nuclear Plant Project (NGNP)*, Idaho National Laboratory, September 2009.

Copyright © 2011 by Battelle Energy Alliance, LLC.
Published and used by ASME with permission