Initiative to Address Complex Systems Failure: Prevention and Mitigation of Consequences

June 2011

prepared by

NEXIGHT GROUP
Acknowledgements

ASME’s Initiative to Address Complex Systems Failure: Prevention and Mitigation of Consequences was prepared by Ross Brindle and Lindsay Pack of Nexight Group under the guidance of Reese Meisinger, Managing Director, Strategic Initiatives & External Affairs and Allian Pratt, Director, Strategic Issues. On behalf of ASME, we would like to express our appreciation to the workshop participants (see Appendix c); the Strategic Issues Committee and its chair, Harry Armen; the Innovation Committee and its chair, Chris Pzirembel; the Industry Advisory Board and its chair, Charla Wise; and the ASME staff, including Patti Jo Snyder, Manager, Strategic Initiatives & Innovation, for their input and recommendations.
## Contents

1. **Background**  
2. **Recommended Initiative to Address Complex Systems Failure**  
3. **Communications and Advocacy**  
   - Key Actions  
     - Develop a position statement  
     - Establish an engineering fellow in the Office of Science and Technology Policy  
     - Develop a multi-society position paper  
     - Determine the need for public outreach materials  
   - Resources and Potential Partners  
   - Timeline and Key Deliverables  
4. **Educational Materials Package**  
   - Key Actions  
     - Compile an initial education package  
     - Hold an educator input workshop  
     - Conduct pilot test of materials package  
     - Expand package offering and audience  
     - Develop a communications plan and metrics  
   - Resources and Potential Partners  
   - Timeline and Key Deliverables
v. **Enterprise Risk Management Framework**  
**Key Actions**
- Compile an annotated bibliography of ERM resources  
- Develop a summary graphic of how to conduct the ERM process  
- Compile a set of ERM technique application examples  
- Develop a consensus-driven framework document  
**Resources and Potential Partners**  
**Timeline and Key Deliverables**  

vi. **Risk Analysis Tools**  
**Key Actions**
- Develop a compendium of standard risk analysis tools  
- Develop the business case for diagnostic/prognostic tools  
- Develop a general framework for technical complex systems analysis  
- Hold a symposium on mitigating complex systems failure  
- Develop a mid-level framework and assess the value of industry-specific tools  
**Resources and Potential Partners**  
**Timeline and Key Deliverables**  

vii. **Looking Ahead**  

**Appendix a. March Meeting Raw Results**  

**Appendix b. March Meeting Agenda**  

**Appendix c. List of Participants**  

**Appendix d. Previous Meeting Reports**
In the spring of 2010, the Gulf of Mexico was devastated by a massive oil spill that stretched on for 91 days. Wildlife, ecosystems, and the livelihoods of those who make their living on the water were immediately and negatively impacted and still have not fully recovered. Similar low-probability, high-consequence events—like the gas line rupture in San Bruno, California; the failure of the levees in New Orleans during Hurricane Katrina; the collapse of the World Trade Center buildings in New York on September 11; and the issues at Japan’s Fukushima Daiichi nuclear power plant triggered by the earthquakes and tsunami—have heightened the public’s awareness of the social, economic, and environmental consequences of large-scale complex system failure.

Now more than ever, there is a need to address these dynamic and far-reaching system failures. While natural disasters, terrorist attacks, and human error will occur, engineers can design complex systems and help manage risk to reduce the likelihood of cascading failures while ensuring that these critical systems do not become too expensive to develop. Experience, knowledge, and tools across industries are needed to aid engineers in designing fault-tolerant systems, assessing and managing risks in system operation, and considering the ethical responsibility associated with the management and maintenance of complex systems.

In response to this need, the ASME Strategic Issues Committee and the ASME Innovation Committee convened three meetings that brought together experts and the ASME Industrial Advisory Board (IAB) to identify future initiatives that ASME can undertake in 2011 and beyond to contribute to the understanding of the root causes of complex systems failures, methods to enhance their prevention, and more effective mitigation of their consequences in the event of a catastrophic failure (see Figure 1).
Figure 1

Development of the Initiative Using the Meeting Results

**High-Priority Need**
- A new code, standard, or technical tool (e.g., global methodology for risk analysis in complex systems or new tool on a component basis)

**High-Priority Need**
- Educate students and current engineers to better understand complex systems

**Medium-Priority Need**
- Enable individual companies or agencies to better understand ethical implications and consequences of decisions

**Medium-Priority Need**
- Increase public/political awareness about complex systems

**Low-Priority Need**
- Address human factors (i.e., include the human in the system; address human psychological and organizational issues)

**October 4–5, 2010**
- Expert task force and invited guests

**December 1–2, 2010**
- Industrial Advisory Board and invited guests

**March 28–29, 2011**
- Expert task force and invited guests

**Catalog best practices and enhance methodologies to develop a complex systems risk analysis model**

**Develop an ASME package of educational materials and products**

**Develop a program to help companies assess and manage enterprise risk**

**Risk Analysis Tools**
- Educational Materials Package
- Communications and Advocacy
- Enterprise Risk Management Framework

**ASME Initiative to Address Complex Systems Failure**

---

Initiative to Address Complex Systems Failure: Prevention and Mitigation of Consequences
The first meeting, held at ASME Headquarters in New York on October 4-5, 2010, brought together an expert task force to explore experiences in complex systems management across industries. Participants identified potential areas for ASME action, including the development of standards and tools, educational initiatives, organizational and ethical issues, and the need to increase public awareness of issues associated with complex systems. High-priority areas identified from that meeting were used as a springboard for strategic planning efforts at the subsequent meeting of the ASME IAB.

Held at the Renaissance Mayflower Hotel in Washington, D.C. on December 1–2, 2010, the IAB and invited guests participated in a second meeting to further examine the identified high-priority areas of action where ASME efforts could make a significant impact. The group ultimately developed a set of three initiatives and corresponding action plans for ASME efforts in the next year and beyond.

In the final planning phase, ASME convened another task force meeting to determine pathways for ASME to implement the action plans from the second meeting. At this meeting, held at the St. Gregory Hotel in Washington, D.C. on March 28–29, 2011, the task force determined that ASME would undertake a comprehensive Initiative to Address Complex Systems Failure—one initiative with four essential components: 1) conduct targeted communications and advocacy about complex systems failures; 2) develop an ASME package of educational materials and products for mechanical engineering heads and practicing engineers; 3) produce a compendium of standard risk analysis tools with an accompanying framework for technical complex systems analysis; and 4) develop a framework to help companies understand, assess, and manage enterprise risk. This report summarizes the recommendations by the task force for an ASME Action Plan for this strategic initiative to advance the prevention of complex systems failure and to mitigate their consequences.
ii. Recommended Initiative to Address Complex Systems Failure

ASME units will seek funding for and conduct the activities involved in the four components of its Initiative to Address Complex Systems Failure, outlined in Figure 2. Drawing on the expertise of its volunteer members, ASME has assigned leadership roles to the ASME committees that best align with the goals and objectives of each component. At the same time, ASME will ensure that the components remain aligned and continually inform each other by appointing an oversight committee to periodically check in with the project teams. This approach will ensure that the individual components sustain momentum while addressing the prevention of complex systems failure in a unified way.
Communications and Advocacy
ASME Lead: Strategy and Outreach Council
Strategic outreach materials developed and delivered to set the tone and message for the initiative and raise awareness of the issue of complex systems failure.

Education and Outreach
ASME Leads: Center for Education; Training and Development
A package of existing and newly developed educational materials about complex systems failures that is geared toward mechanical engineering department heads and practicing engineers.

Enterprise Risk Management Framework
ASME Leads: Board on New Development; Standards and Certification Council
A framework that companies can use to develop a comprehensive, integrated approach to assessing and managing their enterprise risk.

Risk Analysis Tools
ASME Lead: Standards and Certification Council
A compendium of standard diagnostic and prognostic risk analysis tools and an accompanying general framework for technical complex systems analysis that industries can tailor to their environment to better assess risk.
iii. Communications and Advocacy

Events like the Deepwater Horizon oil spill and the issues at the Fukushima Daiichi nuclear power plant generate a great deal of press when they happen; but outside of that context, there is little public focus on what can be done to help prevent complex systems disasters before they occur. Such preventive measures will require an initial investment that is generally regarded as a cost whose future return is uncertain. It is human nature for elected officials and the general public to tend to disregard that fact that the ubiquitous complex systems that we rely on in our daily lives operate at a certain level of risk—a likelihood that they may fail, and that their failures need to be addressed proactively. As a result, preventative efforts do not have the attention and resources they need to be effectively developed and implemented.

ASME will conduct communications and advocacy activities to raise awareness about the need for preventative efforts to address complex system failures. Developing and releasing materials such as a position statement, a program initiative plan, and a multi-society position paper will be part of ASME’s plan and its role as a leader in achieving a solution. In addition, continual public outreach will help reinforce the messages that complex systems have a likelihood of failure and, therefore, should have diagnostic and prognostic systems included as part of their design.
KEY ACTIONS

ASME’s Strategy and Outreach Council will lead the development and distribution of strategic outreach materials to set the tone and message for the initiative and raise awareness of the issue of complex systems failure. The timing of these actions and key deliverables that will result from this effort are visible in Figure 3.

Develop a position statement

Developing a clear and direct position statement is a critical first step not only in the communications and advocacy component, but in launching the ASME initiative as a whole. This statement will define a complex system for a more general audience, and emphasize both the need for diagnostic and prognostic systems to be included as part of complex system design and for organizations to conduct risk management operations that take into account the potential for their complex systems to fail. ASME may also use this as an opportunity to establish the intent to lead this effort.

Create and shop around a program initiative plan

Another important part of the communications and advocacy component is developing a program initiative plan that identifies what ASME can do and plans to do to advance the prevention of complex systems failure. This planning document will provide insight to potential partners of ASME’s approach to this initiative and an estimate of the resources it will require to address the issues. As part of this effort, ASME will distribute the program initiative plan and obtain feedback to determine whether it is advisable and feasible to form a coalition to obtain funding.

Establish an engineering fellow in the Office of Science and Technology Policy

The Office of Science and Technology Policy (OSTP) aims to provide the U.S. President and senior staff with accurate, relevant, and timely scientific and technical advice on all matters of consequence; to ensure that the policies of the Executive Branch are informed by sound science; and to ensure that the scientific and technical work of the Executive Branch is properly coordinated to provide the greatest benefit to society. Establishing an ASME engineering fellow who is focused on complex systems to reside within OSTP can assist the science and technology branch of the Executive Office take a stand on this very relevant issue and ensure that enacted policies and regulations do not unintentionally increase the probability or consequences of systems-related failures. This fellow can also help raise awareness of the initiative to other agencies that may want or need to become involved. A first step in this process is meeting with the President’s Science Advisor to advocate for a fellow. The Strategy and Outreach Council plans to propose the idea to the ASME Board on Government Relations at their June 2011 board meeting.
Develop a multi-society position paper

Once the initial steps of the communications and advocacy component have begun and the other components of the initiative are under way, ASME will consider convening other engineering societies and trade associations to develop and release a position paper on the need to address complex systems failure. Jointly communicating this need from a variety of perspectives will effectively convey the interconnected, multifaceted nature of the issue and stress the importance that many fields and industries place on addressing it.

Determine the need for public outreach materials

By definition, communicating about complex systems and failures can be challenging. Many policy makers and members of the public will struggle to understand the complex technical jargon typically associated with dialogues about these systems. ASME will assess and evaluate the need for a public outreach effort in this area that could include developing brief (30- to 120-second) communications pieces that convey ASME messages about complex systems, risks, and options for making improvements released to audiences such as stakeholders, decision makers, and the media. Because this is a later-stage action in the overall initiative, it will be important to include the progress made in the initiative, such as what has been learned in the development of the risk analysis tool and enterprise resource management framework.

RESOURCES AND POTENTIAL PARTNERS

This effort requires $75,000 for funding a fellow at OSTP and another $100,000 to conduct the remaining actions. OSTP is a potential partner in this effort, as they stand to gain a funded fellow who can coordinate this timely issue that is of increasing public concern. A multi-society position paper will require other engineering societies and trade associations as partners. Potentially, a communications partner may also be needed if a public outreach campaign is undertaken.

TIMELINE AND KEY DELIVERABLES

The timing and key deliverables outlined in Figure 3 will help guide ASME’s Strategy and Outreach Council in the development and distribution of strategic outreach materials.
**Figure 3**  
Timeline for Communications and Advocacy

**YEAR 1**
- Develop and release internal ASME strategic management position statement (weeks)
- Develop program initiative plan of what ASME can do to advance field (one month)
- Shop around program initiative plan and get feedback to determine whether or not to form a coalition

**YEAR 2**
- Determine need for and, if needed, conduct public outreach
- Develop multi-society ASME position paper

**YEAR 3**
- Meet with President’s Science Advisor to advocate for engineering fellow focused on complex systems to reside within OSTP

**KEY DELIVERABLES:**
- Initial position statement
- Program initiative plan of what ASME can do to advance field
- Multi-society position paper
- Appropriate public outreach materials (if needed)
iv. Educational Materials Package

While the failure of a complex system often arises from multiple smaller or cascading failures, human factors almost always play a major role. Deficiencies in the specialized education and training that engineers typically receive, in combination with the retirement of the engineers who designed and built today’s most complex systems, have created a gap in knowledge that is critical to the detection, avoidance, and mitigation of complex systems failures. Educating today’s and tomorrow’s early-career engineers about complex systems and risk assessment is necessary to decrease failures in the long term.

ASME will compile a package of educational materials about complex systems failure. The initial package of materials will be geared toward mechanical engineering department heads and practicing engineers, and it will potentially be expanded to include newly developed materials designed to reach out to different audiences. The materials in this package will not only help to ensure that the individuals involved with complex systems know how to react in the correct way during a failure situation, but also that the engineers of today and tomorrow are constantly thinking about new and innovative ways to mitigate failure at all stages of system development and operation.
KEY ACTIONS

The development of the educational materials package will be led by ASME’s Center for Education, with the Training and Development group in the Standards and Certification Council in charge of developing materials for continuing education. The effort aligns well with the Center for Education's Vision 2030, which strives to improve and expand the U.S. engineering curricula to include program areas such as sustainability and systems integration, as well as successful strategies for program development. The timing of these actions and key deliverables that will result from this effort are visible in Figure 4.

Compile an initial education package

A large number of educational materials, such as case studies, modules, and instructional content regarding complex systems, currently exist throughout various industries and academia, but they are not in a readily usable format for different applications and are not broadly shared. A project team of ASME staff and volunteers will begin this effort by reaching out to the extensive ASME membership to gather existing complex systems and risk analysis materials and combine them in a package that is accessible to mechanical engineering department heads and practicing engineers. The package of materials and products is not limited to but could include any of the following components:

- Case studies
- Standards
- Lesson plans
- Student exercises
- Directions on how to use the package based on the audience
- Videos
- Course modules on failure analysis, details of systems, and risk analysis
- A continuing education module
- ASME short courses

Hold an educator input workshop

One of the most important parts of implementing the educational materials package is ensuring that it appeals to educators and is designed so that they actually use it. ASME will conduct a workshop with educators to obtain their input and buy-in on the educational materials package. ASME will then implement these changes prior to a real-world pilot test, and may also use this workshop as a way to encourage educator participation in that test.
**Conduct pilot test of materials package**

With the input from the educator workshop implemented, ASME will conduct a pilot test of the materials package. Select educators will integrate materials into their course for a pilot test that will measure how effectively students were able to learn about the topic based on the materials provided. The results of this study will inform the development of the package before its release.

**Expand package offering and audience**

After conducting pilot tests of the educational materials package, the team will work to develop new materials to expand the audience base of the package. New materials could include a sample course for other educators based on existing courses on complex systems, videos and case studies that show gradation of risk and focus on cascade of small decisions, and case studies that faculty members can use to help students better understand complex systems. Potential new audiences could include students at a variety of education levels, engineering professionals with different amounts and types of experience, and potentially even individuals outside of the engineering field (e.g., business majors).

**Develop a communications plan and metrics**

To ensure broad use of the educational materials package, ASME will develop a communications plan for publicizing its availability and distributing it to the appropriate audiences via the ASME Center for Education and potentially in other societies (e.g., IEEE). This plan will also have an accompanying metrics component based on the expected impacts of the package. The metrics will assess the effectiveness of the materials so that they can be adjusted to better meet the needs of intended audiences as the initiative grows.

**RESOURCES AND POTENTIAL PARTNERS**

Phase 1 of this effort requires $150,000 per year for a three-year minimum. One potential partner for this effort is the National Science Foundation; charged with improving education in science, technology, and math, the foundation could provide expert input early on in the process. The Alfred P. Sloan Foundation is another strong potential partner, whose grants fund science education and technical advances that improve society’s quality of life. Other partners include the Gates Foundation (and other organizations invested in societal improvement) and potentially financier and Open Society Institute founder George Soros.

**TIMELINE AND KEY DELIVERABLES**

The timing and key deliverables outlined in Figure 4 will help guide ASME’s Center for Education, along with the Training and Development group in the Standards and Certification Council, in the development of an educational materials package.
Figure 4

Timeline for Educational Materials Package

YEAR 1
- Establish project team and vet proposal
- Compile initial educational materials package
- Hold workshop to gain educator input and buy-in
- Educators integrate material into their courses for a pilot test

PHASE 1
- Conduct pilot tests

YEAR 2
- Expand package of educational materials
- Develop communications plan to ensure broad use of the package and metrics

PHASE 2

YEAR 3

6 mo. 12 mo. 18 mo. 24 mo. 30 mo. 36 mo.

KEY DELIVERABLES:
- Initial education package geared toward mechanical engineering department heads and practicing engineers
- Expanded package offering
- Communications plan that ensures broad use of the package and metrics
Company organizational structures and internal decision-making processes are integral to how a firm manages risk across an enterprise. Such structures and processes affect the capacity of a company or agency to assess, manage, and mitigate the risks of a complex system failure. Business culture and practices, including how business is conducted with customers, suppliers, and across the tiers of a company, can impact the performance and safety of a complex system; a system failure could result in a tarnished company reputation, litigation, reduced revenues, and other consequences that could jeopardize the future of a company.

ASME will develop a framework that companies can use to develop a comprehensive, integrated approach to assessing and managing their enterprise risk. This easy-to-use, quick-start guide will provide companies with an independent, defensible basis for characterizing enterprise risk that will help them prevent and mitigate the effects of failure events while retaining the company’s reputation and its financial viability. It will include a range of components, such as an annotated bibliography of enterprise risk management (ERM) resources, summaries of common ERM themes and techniques, and a consensus-based process document that provides ERM guidance to companies.
KEY ACTIONS

The Board on New Development will serve as an entry point and, with the help of the Standards and Certification Council, will hire a contractor to develop the materials for inclusion in the framework and then work to develop a consensus-driven document among a committee of ASME volunteers. The timing of these actions and key deliverables that will result from this effort are visible in Figure 5.

Compile an annotated bibliography of ERM resources

ASME will work with an external contractor to develop an annotated bibliography of ERM resources, such as General Electric’s ERM process. This bibliography will include a brief, concise description of what each cited source covers, commentary on where the source is most appropriately used and its limitations, the typical type of inputs needed to use it, suggestions on interpreting outputs, and suggestions on where to find related information. The document should be presented in a user-friendly, searchable format aimed at the typical user. As a model for this effort, the contractor should use the PTB-2 document, the ASME guide that provides a summary of some of the more commonly used codes, standards, recommended practices, specifications, and guidelines produced by organizations based in the United States for maintaining the integrity of fixed pressure equipment in process plants and in general industrial use.

Develop a summary graphic of how to conduct the ERM process

ASME will also hire an external contractor to develop an easy-to-use summary graphic of common ERM themes that demonstrates how the ERM state of the art applies to complex systems. Ideally, this graphic will be a flow chart that describes how to conduct the ERM process and includes decision points along the way. It should also include links to references in a hypertext document format, as well as suggestions on the most important information for companies interested in developing an ERM process to review.

Compile a set of ERM technique application examples

Using the services of an external contractor, ASME will compile a set of examples for how ERM techniques have been applied successfully or unsuccessfully in the past. While these examples should remain as succinct as possible, they will provide lessons learned that could prove extremely valuable to companies as they develop and implement their own ERM processes.

Develop a consensus-driven framework document

To enable companies to take a comprehensive, integrated approach to assessing and managing enterprise risk, ASME will develop a voluntary, consensus-based process document that provides broadly based guidance on building an ERM process. The document, which will include a definition of complex systems, will move beyond just project risk to include the management of operations and the design of the system. It will also consider human factors, legal framework, and business dimensions, recognizing that risk is dynamic and changes over time.
RESOURCES AND POTENTIAL PARTNERS

This effort will require $200,000 for draft documentation in addition to funding volunteer and staff time. While there may be volunteer members from other organizations involved, the development of the enterprise risk management framework is something that ASME can and should do on its own.

TIMELINE AND KEY DELIVERABLES

The timing and key deliverables outlined in Figure 5 will help guide ASME’s Board on New Development, the Standards and Certification Council, hired contractor, and ASME volunteers in developing an enterprise risk management framework.
Timeline for Enterprise Risk Management Framework

Enterprise Risk Management Framework

**YEAR 1**
- Conduct planning activities (find funding, identify volunteers to write RFP, solicit bids, select winner, and contract negotiations)
- External contractor compiles annotated bibliography of ERM resources
- External contractor develops summary graphic of common themes and how ERM state of the art applies to complex systems

**YEAR 2**
- Find volunteers and form a committee to develop a consensus-based process document that provides guidance to companies

**YEAR 3**

**KEY DELIVERABLES:**
- Annotated bibliography of ERM resources that includes GE ERM process
- Summary graphic of common themes and how ERM state of the art applies to complex systems
- Set of ERM technique application examples for how ERM techniques have been applied successfully or unsuccessfully
- Consensus-based process document that provides broadly based guidance
vi. Risk Analysis Tools

The complex nature of large, interconnected systems makes risk inherently difficult to measure. A comprehensive array of tools for assessing risk in complex systems would provide organizations across multiple industries with the capabilities needed to consider the dynamic interactions and economic, personnel, and environmental influences at both a component and systems level.

ASME will utilize its expertise and strength in the development of technical tools to develop a compendium of standard diagnostic and prognostic risk analysis tools and an accompanying general framework for technical complex systems analysis that industries can tailor to their environment to better assess risk. These tools for assessing risk in complex systems will place greater emphasis on failure precursor detection, uncovering hidden failure modes, assessing and assigning appropriate probabilities of failure, and understanding the dynamics of a larger system. In addition to developing a compendium of tools, this effort will also provide a general framework for technical complex systems analysis and seek stakeholder feedback on the need for an industry-level effort at an ASME-hosted symposium.

KEY ACTIONS

The Standards and Certification Council will lead this effort, which will offer value to industries unfamiliar with risk assessment and expand the scope of risk analysis beyond the building to include organizational and environmental impacts. The timing of these actions and key deliverables that will result from this effort are visible in Figure 6.
Develop a compendium of standard risk analysis tools

Using standard risk analysis ensures that companies are monitoring the most essential data for understanding system health. Risk analysis tools enable the measurements of small changes over time so that system operators can understand when the system is headed toward failure. ASME will work with a contractor to develop a one-stop resource where companies can access the available standard software, hardware, sensors, and other tools used for risk analysis. This compendium will contain diagnostic and prognostic tools used in a variety complex systems and sectors, such as the health monitoring system for fatigue cracks in aircraft, damages sustained by gearboxes in helicopters, the transformers that monitor oil composition and assess health risk, and the sensor network built into the I-35W bridge.

Develop the business case for diagnostic/prognostic tools

Using the services of an external contractor, ASME will define the business case for plant engineers to purchase and use risk analysis tools, acknowledging the financial and societal responsibilities of a company and consequences of unmitigated risk. The business case will be presented in a way that specifically communicates to senior management the value that diagnostic and prognostic tools can bring to overall risk management of the business and failure prevention in particular.

Develop a general framework for technical complex systems analysis

An initial stakeholder workshop will provide the non-proprietary industry input needed for ASME to develop a general framework for technical complex systems analysis that offers value to all industries operating complex systems. The framework will encompass a general analytical tool and set of processes that each industry can tailor to their environment (similar to an ISO standard) to help them monitor and predict areas of failure and mitigate risks or manage failures before they cascade. Analysis processes will also consider low-probability, high-consequence tail risks and help companies effectively prioritize mitigations. The analysis framework will aid companies in not only addressing the technical factors that contribute to risk but also the environment, organizational management, and human factors that can play a role in system failures. Releasing this non-industry-specific framework for complex systems analysis can help to generate interest in the initiative’s subsequent symposium.

Hold a symposium on mitigating complex systems failure

Following the release of the general complex systems analysis framework, ASME will hold an externally funded symposium with industry-specific tracks focused on the state-of-the-art risk mitigation methods addressing each industry’s specific operational needs. Results across multiple industries will be gathered and published as a compendium to support the development of tailored analysis frameworks and tools.
Develop a mid-level framework and assess the value of industry-specific tools

ASME will develop a proprietary mid-level framework for complex systems analysis that builds on the general framework to address specific industries and plants. ASME can use a successful existing model, such as the Risk Analysis and Management for Critical Asset Protection (RAMCAP) model, as an example approach. ASME will then determine whether or not it is valuable to expand its framework to one or possibly multiple industry-specific tools that focus on promoting a culture of safety within an organization and engaging individuals with knowledge of potential problems before a failure.

RESOURCES AND POTENTIAL PARTNERS

Developing risk analysis tools will require approximately $1.5–$2 million, with the largest share of funding being spent on developing an industry framework. The U.S. Department of Transportation, U.S. Department of Homeland Security, U.S. Department of Energy, and U.S. Department of Defense are all potential government partners in this effort. Potential partners also include foundations such as the Alfred P. Sloan Foundation and George Soros, financier and founder of the Open Society Institute.

TIMELINE AND DELIVERABLES

The timing and key deliverables outlined in Figure 6 will help guide ASME’s Standards and Certification Council in developing risk analysis tools.
KEY DELIVERABLES:
- Compendium of standard risk analysis tools
- General framework for technical complex systems analysis
- Business case for diagnostic/prognostic tools
- Mid-level framework for specific industries/plants
vii. Looking Ahead

The release of a clear and direct position statement will provide a jumping-off point for the Initiative to Address Complex Systems Failure and stake a role for ASME as a leader in addressing this complicated issue head-on. As the designated ASME committees, members, and volunteers launch the four components of the initiative in 2011 in tandem and maintain their momentum over the next three years, they will also remain aligned and in communication as the work done in some components begins to inform other work in the initiative.

Ultimately, ASME aims to make concrete progress that increases engineers’ ability to predict, manage, and mitigate the consequences of failures in complex systems across multiple sectors. The experience and technical expertise of ASME’s members will ensure that the tools, techniques, and methodologies that are a part of this initiative are based in the most relevant and state-of-the-art information and presented in a way that encourages widespread use. By adopting and learning from these materials, the engineers of today and tomorrow will take an important step in cultivating a culture that considers risk at every step, making the complex systems we rely on safer for everyone.
Appendix a. March Meeting Raw Results

At the March 2011 meeting, the task force generated action plans for each component of the initiative that were captured by the facilitation team. While these results have been clarified and summarized in the main body of this document, the tables below contain the raw ideas that were used to inform the identified path forward.

COMMUNICATIONS AND ADVOCACY: ACTION PLAN

- Develop and release internal ASME strategic management position statement (weeks)
- Develop the program initiative plan of what ASME can do to advance field (one month)
- Develop deeper ASME position statement at society level (6-12 months)
- Shop around program initiative plan and get feedback to determine whether or not to form a coalition
- Concurrently meet with President’s Science Advisor to advocate for engineering fellow focused on complex systems to reside within OSTP or other place in White House (propose to Government Relations at June Board meeting and possibly foundations and go from there)
- Determine need for public outreach
| RESOURCES | $75K (funding fellow) |
|———|———|
| | $100K (communications and outreach, obtaining funding for other tasks) |

| DELIVERABLES |
|———|
| ➤ Position statement as a way to set tone and message for all three initiatives (societal response planning and management?) |
| ➤ Advocate that complex systems will fail and that systems should have diagnostic and prognostic systems included as part of the design of the systems |
| ➤ Guiding regulatory bodies on useful responses to systems failures; how to improve regulations to achieve increased resiliency in a technically accurate way |
| ➤ Can’t be too abstract |
| ➤ Program initiative plan of what ASME can do to advance field |
| ➤ Deeper ASME position statement at society level |
| ➤ Potential multi-society position paper about systems |
| ➤ Assess and evaluate need for and then develop and release appropriate public outreach materials (e.g., stakeholders, decision makers, media) |

| INITIATIVE LEAD |
|———|
| ➤ Strategic Management |

| PARTNERS |
|———|
| ➤ OSTP |
| ➤ Other engineering societies and trade associations (if developing multi-society position paper) |
| ➤ Potential communications partner if proceeding with public outreach |
VALUE PROPOSITION

To OSTP
➤ Gain a free fellow/someone to coordinate this timely issue
➤ Raise awareness of initiative to other agencies
➤ Helps Obama Administration with complex systems failures
➤ Increasing public concern about complex systems failure which underpin our economy and quality of life

To ASME
➤ Brand recognition as ASME being a leader

EDUCATIONAL MATERIALS PACKAGE: ACTION PLAN

Phase 1:
➤ Project team established and functioning; project proposal vetted and accepted by ASME
➤ Development of initial set of materials (i.e., organizing and packaging existing content)
➤ Determine how this content fits within existing engineering curricula
➤ Hold workshop with educators to gain their input and buy-in
➤ Educator(s) agree to and integrate material into their course for a pilot test
➤ Conduct pilot test(s) to assess student learning effectiveness

Phase 2:
➤ Develop expanded materials
➤ Generate awareness and use
  • Develop communications plan to ensure broad use of the package and metrics
**Resources**

- Phase 1: $150K per year for 3 years minimum (includes NSF/Sloan grant)

**Deliverables**

- Develop initial educational package of existing materials that is geared toward mechanical engineering department heads and practicing engineers
- Expand package offering and audience
  - Use existing course to develop sample course for others to use
  - Videos and case studies that show gradation of risk and focus on cascade of small decisions
- Develop communications plan to ensure broad use of the package and metrics

**Initiative Lead**

- Center for Education

**Partners**

- NSF (bring in early in process to gain their input)
- Sloan
- Gates Foundation (and other organizations invested in societal improvement)
- George Soros
Center for Education leadership
➤ Fits into existing Vision 2030 initiative

ASME
➤ Opening new frontiers for the discipline
➤ Benefits Vision 2030 initiative

NSF
➤ Charged with improving education in science, technology, and math—fits well with their objectives

Sloan
➤ Use technology to improve society—fits well with their objectives

ENTERPRISE RISK MANAGEMENT FRAMEWORK: ACTION PLAN

Planning (6 months)
➤ Find funding
➤ Identify volunteers to write RFP
➤ Solicit bids
➤ Select winner and contract negotiations

Execution (target: 1–2 years)
➤ Funded with external contractors

Consensus Building
➤ Find volunteers
➤ Form committee
RESOURCES

- $200K for draft documentation
- Volunteer time, staff time

DELIVERABLES

- Annotated bibliography of ERM resources that includes GE ERM process
  - Includes summary of important, relevant information from each book
  - User friendly, searchable information
  - Use PTB-2 as a model for this
  - Provide a brief, concise description of what it is, commentary on where it is most appropriately used and its limitations, typical type of inputs needed to use it, suggestions on interpreting outputs, suggestions on where to find related information (don’t limit to one page)
  - Typical user: graduate mechanical engineer with one area of expertise asked to look at risk tools; can use this source to determine what he/she needs to look at to have an understanding of the topic

- Summary graphic of common themes and how ERM state of the art applies to complex systems (“value-added offering”)
  - Flow chart that describes how to conduct ERM process
  - Include decision points
  - Provide links to references (“hypertext document”)
  - Include suggestions for most important information to review

- Set of examples for how ERM techniques have been applied successfully or unsuccessfully
  - Shorter the better

- Voluntary consensus-based process document that provides broadly based guidance
  - Include definition of complex systems
  - Move beyond just project risk to the management of operations and the design of the system
  - Must consider human factors, legal framework, and business dimensions
  - Risk is dynamic and changes over time
initiative lead

➤ Board on New Development (entry point)

partners

➤ N/A (ASME can and should do this on its own)
➤ May have volunteer members from other organizations

value proposition

To stakeholders we serve

➤ Easy-to-use, quick-start guide to enable companies to think about ERM
➤ Provides an independent, defensible basis for characterizing enterprise risk
➤ Mitigates effects of events that impact the relationship of the company in a way that would significantly damage the reputation of the company and its financial viability

RISK ANALYSIS TOOLS: ACTION PLAN

timeline

➤ Hire contractor to develop compendium of standard risk analysis tools (~2 years)
➤ Hire contractor to develop business cases
➤ Develop generic industry framework for technical complex systems risk assessment methods—this should serve to generate interest for the symposium (2–3 years)
➤ Hold and use input from a separate stakeholder workshop
➤ Hold symposium with industry-specific tracks and publish results (after generic framework is established)
➤ Determine whether going to more detailed-level tool (industry-specific) development is needed/would be beneficial
Initiative to Address Complex Systems Failure: Prevention and Mitigation of Consequences

**RESOURCES**

- **$1.5-2M**
  - Largest share of funding should be spent on developing industry framework

**DELIVERABLES**

- Compendium of standard risk analysis tools (software, hardware, sensors)
  - A place to put existing tools for ASME members
  - Should include diagnostic and prognostic tools in all complex systems (e.g., health monitoring system for gearbox in helicopters; transformers that monitor oil composition and assess health risk; sensor network built into I-35W bridge); using standard risk analysis to determine what data is most essential
  - Can measure small changes over time to know when you're headed toward failure

- Establish value of purchasing these tools to customers—have to influence the top levels of the company (decision is not up to plant manager)

- Provide a framework for technical complex systems analysis on a general basis
  - General analytical tool and set of processes that each industry can tailor to their environment (e.g., ISO standard)
  - Non-proprietary (need private sector input, but do not need proprietary information to accomplish this)
  - Extend thinking beyond plant, operation, etc.—this is a value to all industries, including nuclear
  - Includes environment and organizational management (see graphic from December meeting)
  - Monitor and predict, manage and mitigate
  - Have to include tail risks (low probability, high consequence)
  - Have to include human factors

- Hold a conference/symposium on mitigating the failure of complex systems that has general presentations and industry-specific tracks (petroleum, nuclear, etc.)
  - Theme of talks: State of the art of risk mitigation
  - Gather information from the symposium and publish it as a compendium
  - Externally funded

- Develop mid-level framework for specific industries/plants and assess value of developing detailed tools
  - Use RAMCAP program development model
  - Proprietary
Initiative Lead
- Standards and Certification Council

Partners
- DOT, DHS, DOE, DoD, Foundation (e.g., Sloan), George Soros

Value Proposition
- Offers value to industries not as familiar with risk assessment
- Expands scope of risk analysis beyond the building to include organizational and environmental impacts (even nuclear sector can benefit)
- Non-technical stakeholders can see that there is a process for dealing with complex systems analysis and risk
- ASME owner can broaden scope and provides opportunity for organic growth
Appendix b. March Meeting Agenda

DAY 1: MONDAY, MARCH 28, 2011

12:00 – 1:00  Lunch

12:30 – 1:00  Welcome Remarks - H. Armen
              Project Status Review - G. Feigel

1:00 – 2:15  Develop Implementation Plan for Area #1 - Ross Brindle
            Catalog best practices and enhance methodologies to develop a complex systems risk analysis model

2:15 – 3:30  Develop Implementation Plan for Area #2 - Ross Brindle
            ASME package of educational materials and products

3:30 – 3:45  Break

3:45 – 5:00  Develop Implementation Plan for Area #3 - Ross Brindle
            Program to help public policy makers and private organizations understand, assess, and manage enterprise risk

6:00  Dinner – Nora’s Restaurant
DAY 2: TUESDAY, MARCH 29, 2011

7:30  Continental Breakfast

8:00 – 10:00  Discuss Hand-Off from Strategic Issues - Ross Brindle
   ➤ Review Implementation Plans from Day #1
   ➤ Review Breakthrough Innovation Process for CSF
   ➤ Where are the best “home(s)” for CSF within ASME?
   ➤ Transition Team Membership

10:00 – 10:30  Break

10:30 – 12:00  Discuss Hand-Off from Strategic Issues (continued)

12:00 – 12:30  Lunch

12:30 – 2:00  Closing Session - Ross Brindle
   ➤ Report to Board of Governors
   ➤ Next Steps

2:00  Adjourn
Appendix c. List of Participants

TASK FORCE

S. Massoud Amin, D.Sc., Director, Technological Leadership Institute (TLI), Honeywell/H.W. Sweatt Chair in Technological Leadership, College of Science and Engineering, University of Minnesota

Harry Armen, Sc.D., Chair, Strategic Issues Committee, ASME

Eric Kaufman, Safety & Reliability Manager, GE Energy Infrastructure – Engineering

John Elter, Ph.D., Member, Strategic Issues Committee, ASME; Executive Director, Center for Sustainable Ecosystem Nanotechnologies, University of Albany

Richard E. “Gene” Feigel, Ph.D., Past President, ASME; Vice President, Engineering, The Hartford Steam Boiler Inspection & Insurance Company

Gary Halada, Ph.D., Associate Professor, Department of Materials Science & Engineering, Stony Brook University

Regis Matzie, Ph.D., Member, ASME ITI, LLC Management Committee; RAMatzie Nuclear Technology Consulting

J. Robert Sims, Jr., Vice Chair, Post Construction Committee and Member, Standards Committee on Pressure Vessels, ASME; Senior Fellow, Becht Engineering Co., Inc.
DECEMBER 2010 MEETING PARTICIPANTS

Harry Armen, Sc.D.
Ken Balkey
Andy Bicos
Maurice Darbyshire
Howard Dittmer
Eric Ducharme, Ph.D
John Elter, Ph.D.
Richard E. “Gene” Feigel, Ph.D.
Tommy Gardner
John Goossen
David Jaggi
Eric Kaufman
Jim Harlan
Stacey Swisher Harnetty
Tom Libertiny
Peter Lodal
Tom Loughlin
Regis Matzie, Ph.D.
Vic Mullin
Vickie Rockwell
Keith Roe
Roger Royer
Joe Schroeder
Robert T. Simmons, P.E., President, ASME
J. Robert Sims, Jr.
Scott Stallard
Steven Unikewicz
Charla Wise

OCTOBER 2010 MEETING PARTICIPANTS

S. Massoud Amin, D.Sc
Harry Armen, Sc.D.
Ken Balkey
Eric Kaufman
John Elter, Ph.D.
Richard E. “Gene” Feigel, Ph.D.
Marc Goldsmith
Phillip Grossweiler
Gary Halada, Ph.D.
Regis Matzie, Ph.D.
Charles Perrow, Ph.D.
Chris Przirembel, Ph.D.
Asok Ray, Ph.D.
Robert T. Simmons, P.E., President, ASME
J. Robert Sims, Jr.
Steven Unikewicz

ASME STAFF

Thomas G. Loughlin, Executive Director
Michael Cowan, Director, Public Information
Phil Hamilton, Associate Executive Director, Strategy & Outreach
John Koehr, Managing Director, Technical & Personnel Certification
June Ling, Associate Executive Director, Standards & Certification
Reese Meisinger, Managing Director, Strategic Initiatives & External Affairs
Allian Pratt, Director, Strategic Issues
Patti Jo Snyder, Manager, Strategic Initiatives & Innovation
Mel Torre, Director, Communications

CONSULTING SUPPORT

Ross Brindle, Nexight Group
Jack Eisenhauer, Nexight Group
Fred Hansen, Energetics Incorporated
Lindsay Kishter, Nexight Group
Sarah Lichtner, Nexight Group
Lindsay Pack, Nexight Group
Initiative to Address Complex Systems Failure: Prevention and Mitigation of Consequences
Appendix d.
Previous Meeting Reports

The following section contains the report that was produced after the October 2010 meeting and the report that was produced after the December 2010 meeting. While the results of these meetings have been included in the development of the Initiative to Address Complex Systems Failure: Prevention and Mitigation of Consequences, the reports provide additional detail to illustrate the thinking that went into the formation of the initiative.
Initiative to Address the Prevention of Complex Systems Failure:

Report of the Workshop on
October 4–5, 2010

ACKNOWLEDGEMENTS

The ASME Initiative to Address the Prevention of Complex System Failure was prepared by Ross Brindle and Lindsay Pack of Nexight Group under the guidance of Reese Meisinger, Managing Director, Strategic Initiatives & External Affairs and Allian Pratt, Director, Strategic Issues. On behalf of ASME, we would like to express our appreciation to the workshop participants; the Strategic Issues Committee and its chair, Harry Armen; the Innovation Committee and its chair, Chris Pzirembel; and the ASME staff, including Patti Jo Snyder, Manager, Strategic Initiatives & Innovation, for their input and recommendations.
Contents

i. Background 40

ii. Summary of Presentations 41
   The Next Catastrophe: Reducing our Vulnerabilities to Natural, Industrial and Terrorist Disasters 41
   Teaching by Disaster: The Ethical, Legal, and Societal Implications of Engineering Disaster 42
   Complex Systems Failure: Sustaining Order and Normalcy in Human-Engineered Systems 43
   Identifying Complex System Risks and Actively Learning from External High-Severity Events 44
   The Role of Standards and Certification, Probabilistic Risk Assessment, and Regional Public/Private Partnerships 45
   Discussion Results 46

iii. Potential Areas for ASME Action 47
   High Priority: A new code, standard, or technical tool 48
   High Priority: Educate students and current engineers to better understand complex systems and failure analysis 49
   Moderate Priority: Address organizational issues of individual private companies or public agencies by enabling companies and agencies to better understand consequences of decisions (designs, processes, policies) and ethical considerations 50
   Moderate Priority: Increase public and political awareness about complex systems 51
   Lower Priority: Address human factors 52

iv. Next Steps 53

v. Agenda 54
The recent tragic events in the Gulf of Mexico have heightened the public awareness of the broad-based consequences of a large-scale, complex, dynamic human-engineered system failure. These consequences include social, economic, and environmental effects. Engineers need to consider the operation of these systems, together with the appropriate level of fault-tolerance in the initial design; development and operation of these systems working under projected and unexpected circumstances; and the ethical responsibility associated with process management and maintenance.

In response, ASME convened a task force of experts to explore experiences across industries and consider topics such as lessons learned, best practices, R&D needs, and ethical responsibilities. This meeting, which occurred at ASME Headquarters in New York on October 4-5, 2010, was the first of a series of meetings planned for 2010. The overall goal of the initiative is to identify future initiatives that ASME can undertake in 2011 and beyond to contribute to the understanding and more effective mitigation of the consequences of complex system failure.

This report summarizes the high-level conclusions of the meeting. The meeting agenda is provided in Section v of this report.
ii. Summary of Presentations

Presentations given on the first day of the meeting aimed to both inform participants about current efforts to mitigate complex systems failures from a mechanical engineering perspective and to encourage thought about what actions ASME can potentially take to address these issues going forward. At the end of the presentation session, participants discussed ASME’s role and made determinations that served as the framework for the second day of the meeting.

THE NEXT CATASTROPHE: REDUCING OUR VULNERABILITIES TO NATURAL, INDUSTRIAL AND TERRORIST DISASTERS

Charles Perrow, Ph.D., Yale University

This presentation centered on the major themes of Dr. Perrow’s book, *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial and Terrorist Disasters*. His book asserts that while the United States cannot escape disasters (e.g., terrorist attacks, natural disasters), it can and should focus on protecting the targets of potential disasters by enhancing their resistance and ability to handle catastrophe. For example, chlorine gas is transported in 90-ton tank cars, a concentration that could be disastrous if an attack or crash occurred. Rather than focusing on defense against these outside forces, efforts should concentrate on developing methods to transport hazardous materials in smaller quantities and in areas with less potential impact. This more modular approach to planning can be applied to many systems, thus reducing the consequences of system failure. Dr. Perrow also focused on the critical role of the organizational system in reducing risk and responding to catastrophe. He criticized U.S. organizational systems for their high failure
rate in effective planning and response, and identified them as a necessary consideration when addressing the mitigation of complex system failures.

**Key Takeaways**

➤ Absolute defense is impossible; need to focus on managing risk.

➤ A distributed or modular approach can, in some cases, reduce concentrations of energy and, therefore, the consequences of systems failure.

➤ When configuring risk management and responses to catastrophe, there is a need to address and minimize three different types of failure: built failure, societal failure, and organizational failure.

### TEACHING BY DISASTER: THE ETHICAL, LEGAL, AND SOCIETAL IMPLICATIONS OF ENGINEERING DISASTER

**Gary Halada, Ph.D., Stony Brook University**

Dr. Halada’s presentation focused on the role of engineering education in enhancing the ability of future engineers to limit complex systems failures and respond to failure in a way that limits the possibility of future failures. He noted that the primary causes of engineering disasters are human factors (both “ethical” failure and accidents), design flaws, materials failures, extreme conditions or environments, and, most importantly, combinations of these. Dr. Halada believes that education is critical to preventing these occurrences in the future, particularly human factors. He provided his personal experience teaching his “Learning from Disaster” course as an effective way to teach students from a variety of backgrounds regarding the ethical, legal, and societal impact of engineering. In the culminating activity of the course, Dr. Halada challenges his students to choose a systems failure that has already occurred (such as the Toyota recall) and “prevent” it from happening. Through exercises such as this, students learn causes of failure, risk, and uncertainty; system design and how to design for reliability; and ethical problem solving—skills that will enable them to approach risk mitigation and failure response in an innovative and effective way, helping to reduce the negative impact of human factors.

**Key Takeaways**

➤ Human factors play a major role in the cause and effective mitigation of critical systems failures.

➤ Lifelong learning is a key way to prevent human failures; it encourages thoughtful insight, and the concept of designing for failure becomes second-nature and more innovative.

➤ Engineering-based industries are facing a wave of retirement of the technical people who built complex systems, making education of the next generation of engineers critical.
It is the responsibility of engineering professionals to better educate engineers. We need to better integrate engineering failure models with financial consequences models.

Professional societies like ASME can help develop and replicate courses like “Learning from Disaster” to ensure that they reach engineering students and engineers currently working in the industry and academia.

COMPLEX SYSTEMS FAILURE: SUSTAINING ORDER AND NORMALCY IN HUMAN-ENGINEEREED SYSTEMS

Asok Ray, Ph.D., Penn State University

This presentation covered the U.S. Department of Defense’s (DoD) strategy to ensure that its complex systems are not compromised by failure by making its systems autonomous. The “science of autonomy” involves predicting a fault via the emergence of the precursor data or anomaly detection and then acting before the fault evolves into a failure of the component or system. Dr. Ray noted that to sustain order and normalcy in human-engineered complex systems, four areas must be covered: 1) anomaly detection and fault mitigation, 2) fault/damage mitigation decision and control (replacing human decisions with automated decisions), 3) network-centric objective force, and 4) computer system and software reliability. In order to address these areas, failure information must be generated to facilitate early detection and quantification of anomalous behavior. Impending failures must be circumvented and failure consequences mitigated via the timely decisions and control of mission operators. Dr. Ray and his team are conducting research to determine what these early anomaly signals are and what the potential consequences might be. The end goal of the DoD program is to develop real-time, autonomous detection and failure prognosis for sustaining order and normalcy in human-engineered complex systems.

Key Takeaways

- System autonomy involves building precursor data, anomaly detection, and mitigating actions into a system to prevent a fault from evolving into an unacceptable failure.
- The system is largely autonomous, but it would have some centralized control.
- Attention should be paid to communicating this critical, complex information to the operator in a clear and consistent way, enabling them to better process information and respond as an event is unfolding.
IDENTIFYING COMPLEX SYSTEM RISKS AND ACTIVELY LEARNING FROM EXTERNAL HIGH-SEVERITY EVENTS

Eric Kaufman, GE Energy Infrastructure – Engineering

This presentation focused on GE’s incorporation of risk assessments into its energy infrastructure development processes. Mr. Kaufman noted that there is a constant struggle in a business environment when a project demonstrates a major potential return on investment, but also requires taking on risk. There is a tendency to point to past history of successful operation as justification to take on incremental risk. There are also sensitivities about sharing risk assessments with the public and conducting quantitative risk assessments—these can create “enterprise-level” risk, which can potentially damage the company’s brand and/or share price. At GE, the risk group is independent from the product design groups. The group provides engineers with a communications tool that quantifies risk and helps them understand what they need to do to move from an unidentified or unacceptable level of risk to an acceptable level of risk. The group also conducts reviews of every product that include quantitative risk modeling (the accident scenario review). In addition, the group measures the risk growth of an existing fleet over time and examines external events, such as the Kleen Energy power plant explosion that occurred in Connecticut in February 2010, to apply the lessons learned to its own products and processes. At GE, the cross-business product safety team, common workflow process and record system, single safety risk quantification process, audits on process execution, standardized metrics and trending, and continuous improvement feedback loop all work together to enable proper risk assessments. By conducting these assessments, there is a better understanding during the design phase of whether or not redundancies need to be built into the system.

Key Takeaways

➤ Business goals often conflict with risk management.

➤ GE has a risk management group that cuts across all product development groups, providing a consistent and streamlined way to ensure that its products meet acceptable levels of risk.

➤ When working to mitigate risk, there seems to be a disconnect between what is considered fundamental engineering and safety knowledge in a real-world business setting and what is being taught as fundamentals in engineering schools.

➤ Engineering clinics and faculty members with industry ties could help bring fundamental lessons from an industry perspective to the classroom.
THE ROLE OF STANDARDS AND CERTIFICATION, PROBABILISTIC RISK ASSESSMENT, AND REGIONAL PUBLIC/PRIVATE PARTNERSHIPS

Kenneth R. Balkey, P.E., Westinghouse Electric Company, LLC

Mr. Balkey’s presentation provided an overview of the roles that ASME has played and continues to play in mitigating the consequences of complex systems failure in industry. One major ASME contribution was the development of the standard for probabilistic risk assessment (PRA). The PRA is a tool used heavily in the nuclear industry that prioritizes certain activities and events in terms of potential impact on risk and also allows plant designers and operating plant engineers to change the risk profile of the design. The first time the PRA was formally used, there were 65 plants conducting PRAs in 65 ways, which led to confusion and inconsistency in its approach to the risk assessment, its subsequent results, and its application in assessing actual risk. As a result, the U.S. Nuclear Regulatory Commission (NRC) asked ASME to develop a PRA standard. ASME developed the standard and currently provides industry training programs, both of which have helped increase model robustness. Mr. Balkey noted that ASME could continue to help the effort to increase the robustness and usefulness of the current PRA modeling techniques by partnering with other organizations to conduct peer reviews on plant modeling. He also noted that ASME may choose to play a potentially significant role in public-private partnership building that can assist in the mitigation of the consequences of disasters quickly on a regional level. In Pittsburgh, Mr. Balkey helped form a regional business coalition for homeland security to help get businesses operating after an incident to create necessary economic activity. While ASME did not participate in this effort, Mr. Balkey indicated that ASME could use lessons learned from the Pittsburgh example and from its own previous attempt in 2005 to get regions to share best practices to facilitate the establishment of public-private partnerships that can respond to a crisis faster than federal efforts.

Key Takeaways

- ASME has played and continues to play a role in mitigating the consequences of complex systems failures.
- One successful contribution involved the development of the standard for PRAs and PRA training to fill the void in undergraduate curriculum.
- ASME can and should contribute in many other ways, including peer reviews on nuclear plant modeling and facilitating regional public-private partnership building for disaster response.
DISCUSSION RESULTS

At the end of the presentation session, the group discussed what they had heard and the implications for the role of ASME in mitigating the consequences of complex systems failure. The high-level conclusions from this discussion include:

➤ When considering complex systems it is useful to think in terms of three classes of systems: Built, Societal, and Organizational

• All three classes of systems are important; it is beneficial to consider more than one class (where appropriate) to accurately reflect the vulnerabilities and embedded risks associated with a complex system.

➤ More distributed or modular systems can reduce concentrations of energy and, therefore, the consequences of systems failure.

➤ The appropriate level of autonomy assigned to the components of the distributed system depends on the specific application for which they are used.

➤ Human factors are always at play in risk management.

• Psychological issues (e.g., risk tolerance build-up) are important contributing factors.

• Using sensors to gather and process the most appropriate data into useful knowledge that humans can act upon before failures occur is a fundamental requirement and a significant challenge associated with reducing the vulnerabilities of complex systems and mitigating the consequences of their failure.

➤ There is great need for significant educational efforts to train current and future engineers about complex systems and their potential to fail.

• A wave of retirements by experienced engineers who built many of today’s complex systems creates a compelling need to capture and transfer that knowledge to new engineers.

• Current coverage of risk analysis and systems failure in undergraduate engineering curricula is weak.

➤ The best risk management processes engage multiple, diverse experts to review risks and risk evaluation methodologies.
### iii. Potential Areas for ASME Action

The Project Team identified five potential areas for ASME action and prioritized these areas according to two criteria: (1) the magnitude of potential impact, and (2) the fit with ASME capabilities and resources:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High Priority</strong></td>
<td>➤ A new code, standard, or technical tool:</td>
</tr>
<tr>
<td></td>
<td>● Global methodology for risk analysis in complex systems</td>
</tr>
<tr>
<td></td>
<td>● New tool on a component basis</td>
</tr>
<tr>
<td></td>
<td>➤ Educate students and current engineers to better understand complex systems</td>
</tr>
<tr>
<td><strong>Moderate Priority</strong></td>
<td>➤ Help address individual companies’ (private) or agencies’ (public)</td>
</tr>
<tr>
<td></td>
<td>organizational issues by enabling companies and agencies to better understand ethical implications and to better understand consequences of decisions (designs, processes, policies)</td>
</tr>
<tr>
<td></td>
<td>➤ Increase public/political awareness about complex systems</td>
</tr>
<tr>
<td><strong>Lower Priority</strong></td>
<td>➤ Address human factors (i.e., include the human in the system; address human psychological and organizational issues)</td>
</tr>
</tbody>
</table>
The sections that follow offer more details regarding the areas of potential ASME action and specific initiatives that ASME may consider undertaking to address the topic of complex systems failures.

**HIGH PRIORITY: A NEW CODE, STANDARD, OR TECHNICAL TOOL**

One area of ASME’s expertise and strength is the development of codes, standards, and technical tools to manage risk, beginning with the first boiler code. There are two levels at which ASME could address the creation of a new technical tool:

**A new code, standard, or tool for assessing risk in specific components of complex systems**

This approach builds upon one of ASME’s traditional strengths. An effective tool would place greater emphasis on failure precursor detection, uncovering hidden failure modes, assessing and assigning appropriate probabilities of failure, and start to understanding the dynamics of a larger system. Specific approaches could include:

- Developing a standard or policy that creates incentives for including diagnostic and prognostic equipment into complex systems, and a corresponding enforcement process
- Convening a conference on diagnostic and prognostic tools for complex systems
- Starting an educational process on diagnostic and prognostic tools for complex systems

**A global methodology for conducting risk analysis of complex systems**

Creating such a methodology may be a complex, difficult undertaking. The proposed methodology would begin as a tool or guideline and potentially evolve into a standard over time. The methodology would offer more detail than ISO risk management standards but not as much detail as nuclear power plant standards. To be effective, the methodology must incorporate human factors, as these factors are almost always a major contributor to complex system failures. The methodology would likely begin with a determination of the risk of failure for each individual component in a system, assign probabilities of failure, and then combine these component-level risks into a systems-level assessment in a manner that considers economic, personnel, and environmental influences.
HIGH PRIORITY: EDUCATE STUDENTS AND CURRENT ENGINEERS TO BETTER UNDERSTAND COMPLEX SYSTEMS AND FAILURE ANALYSIS

Many of the engineers who designed and built today's most complex systems are entering the latter stages of their careers and retiring. Educating today's and tomorrow's early-career engineers about complex systems and risk assessment in such systems is critical to avoid the potential knowledge gap that might otherwise arise. ASME could address this educational need in many ways; potential approaches are identified below:

Develop an interactive, web-based tool for students K-12 that tells stories about disasters and failures and gets people thinking about systems complexity and failure

Such a tool can introduce the concept of systems, complexity, and failure to young minds, hopefully capturing interest and steering people to educational programs and eventual careers assessing and managing risks in complex systems.

Develop an undergraduate course that could pique interest in pursuing complex systems at the graduate level

Such a course may be an interdisciplinary course (akin to Dr. Halada's course at Stony Brook University described on Day 1), a freshman seminar for first-year engineering majors, or a capstone project for senior engineering majors. Each approach has advantages and disadvantages, but they share the same objective: further expose undergraduates who are likely to encounter complex systems to risk management, complexity, and failure. One potential barrier to making a major impact is the small number of professors who might be interested in teaching such a course or integrating it into highly demanding ME programs that do not have much room for additional requirements.

Ensure that undergraduate mechanical engineering curricula integrate discussion of failure modes throughout

Rather than creating a dedicated course, ASME can provide modules that would allow professors to introduce risk, complexity, and failure issues throughout the engineering curricula, perhaps as one or two lectures in a semester-long course. Partnering with other professional societies (e.g., IEEE) may extend this concept beyond mechanical engineering departments and into other engineering disciplines which often must work together in complex systems.

Create case studies to provide to faculty members to enable students to better understand complex systems

Whether in a dedicated course or as a recurring theme throughout the curriculum, interesting case studies that offer real-world examples can resonate with students and expose them to the rich set of issues
that typify complex systems failures (e.g., ethics). Such case studies could also be useful as a continuing education product aimed at working professionals, potentially tying into professional engineering continuing education requirements.

**MODERATE PRIORITY: ADDRESS ORGANIZATIONAL ISSUES OF INDIVIDUAL PRIVATE COMPANIES OR PUBLIC AGENCIES BY ENABLING COMPANIES AND AGENCIES TO BETTER UNDERSTAND CONSEQUENCES OF DECISIONS (DESIGNS, PROCESSES, POLICIES) AND ETHICAL CONSIDERATIONS**

Organizational issues are critical factors in determining the capacity of a company or agency to assess and manage risk and mitigate the consequences of a complex system failure. ASME can help to address these organizational issues by creating resources that improve understanding of relevant issues, including the ethical aspects of decision making regarding complex system failures. Specific actions ASME may pursue include the following items:

- **Develop a short course for business and government leaders addressing systems complexity and organizational implications**
  
  Such a course can address the definition of a complex system, the factors that combine to make a system complex, and the concepts of “manmade ecosystems” as they relate to organizations. A key aspect of such a course would be the ethical implications of decision making to reduce the probability and potential consequences of failure, and instances where such decisions may conflict with traditional organizational drivers.

- **Develop a tool for collecting risk factor data and displaying it clearly in a day-to-day management tool**
  
  Such a “dashboard,” if developed properly, could simplify risk management and facilitate the incorporation of risk into the day-to-day practices of organizational leaders.

- **Develop a standard for a third-party, independent design audit**
  
  Such a standard would ensure some party outside of the organization could evaluate systems designs to assess complexity, risk, and management techniques built into the system design. Doing so would reduce the likelihood of organizations making decisions that benefit it in the near term at the expense of increased risk or failure consequences in the longer-term, uncertain future.
Develop educational materials that impart lessons about “safety culture” learned in nuclear, aviation, and aerospace industries to leaders of organizations in other industries

A course for company or government executives that introduces the concept and best practices for creating and implementing a “safety culture” could have important impacts in industries that would benefit. By partnering with other societies in target industries, ASME can extend its reach and increase the relevance of such courses to the targeted sector.

MODERATE PRIORITY: INCREASE PUBLIC AND POLITICAL AWARENESS ABOUT COMPLEX SYSTEMS

Even the most sophisticated engineering tools for managing complex systems cannot completely eliminate the risk of failure. In addition to technical tools and educational efforts targeting engineers and organizational leaders as described above, ASME can undertake efforts to educate politicians and the general public about complex systems and failures. Specific initiatives ASME could undertake are further described below:

Serve as a catalyst for public-private partnerships to address complex systems failure risk

Because 80-90 percent of assets are privately owned, it is impossible for the government to address complex systems failures without partnering with the private sector. However, the motivations of individual companies may not span an entire complex system, or may not properly account for the public harm that a failure could create. ASME can host workshops and other partnership-building activities that create regional or local public-private partnerships that can be used to increase resilience of systems under normal conditions and improve responses to failures in the event that they do occur.

Develop communications products about complex systems failure in a manner that is easily understood by non-technical audiences

By definition, communicating about complex systems and failures can be challenging. Yet many policy makers and members of the public will struggle to understand complex technical jargon, demanding a different approach. ASME can develop brief (30- to 120-second) communications pieces that convey ASME messages about complex systems, risks, and options for making improvements, perhaps in partnership with organizations such as the Center for Strategic and International Studies, the National Academy of Engineering, or the Santa Fe Institute to extend their impact.
Assess and provide information about the critical systems impacts of proposed policies

ASME can engage its government relations capabilities to provide an unbiased, engineering-based view of how proposed policies might affect critical systems issues. Examples of issues that have under-covered systems impacts include plug-in electric vehicles, the integration of renewable energy sources into the electric power grid, and water management issues. By providing an unbiased, informed viewpoint on such issues, ASME can help to ensure that enacted policies do not unintentionally increase the probability or consequences of systems-related failures.

LOWER PRIORITY: ADDRESS HUMAN FACTORS

No complex system can be engineered to be completely isolated from human interactions. These human interactions are frequently the root cause of systems failures. Accordingly, addressing human factors is a critical aspect of any complex systems failure program. However, because such issues are further afield of ASME’s core competencies, this area is viewed as lower in priority than the others identified in this document. Potential ASME initiatives to address human factors include:

Partner with psychological associations to better understand and inform engineers about psychological aspects of risk and system failure

The concept of “risk creep” is a real psychological phenomena, whereby individuals become increasingly comfortable with risky situations because they have dealt with them in the past without failures. Partnering with psychological experts could shed light on how such phenomena occur and techniques for managing them. Specifically, organizing a conference and publishing proceedings on such topics may be a logical starting point for a larger effort focused on the intersection between complex engineered systems and psychological phenomena.

Develop a topic paper that makes the statement that design, maintenance, and operation of complex systems must factor in human element

Simply by formally recognizing the critical aspect of human elements via a white paper, ASME can raise awareness of such human factors among its membership and the related community. Ultimately, doing so would increase the likelihood that risk analysis methodologies and standards would incorporate human factor components as an essential part of a comprehensive approach.
iv. Next Steps

The results of this workshop will be used to focus the ASME Industrial Advisory Board (IAB) meeting on December 1–2 in Washington, D.C. The IAB will focus on planning out specific ways for ASME to achieve the priority activities identified at the October meeting; the results of both meetings will be compiled into a strategic approach for the ASME Strategic Issues Committee to employ in the initiative to mitigate the consequences of complex systems failure. Ultimately, ASME aspires to implement specific projects that increase engineers’ ability to predict, manage, and mitigate the consequences of failures in complex systems.
v. Agenda

MONDAY, OCTOBER 4, 2010

8:00  Continental Breakfast Served

8:30 – 9:00  Welcome, Introductions, and Overview of Meeting Objectives
            Harry Armen, Sc.D., Chair, Strategic Issues Committee

9:00 – 10:00  Presentation and Discussion
               Charles Perrow, Ph.D., Professor Emeritus of Sociology, Yale University;
               author of “The Next Catastrophe: Reducing Our Vulnerabilities to Natural,
               Industrial and Terrorist Disasters”

10:00 – 11:00  Presentation and Discussion
                Gary Halada, Ph.D., Associate Professor, Department of Materials Science &
                Engineering, Stony Brook University

11:00 – 11:15  Break

11:15 – 12:15  Presentation and Discussion
                Asok Ray, Ph.D., Distinguished Professor of Mechanical Engineering, Penn
                State University; Penn State Joint Project with the U.S. Army on Complex
                Systems Failure
12:15 – 1:15  **Lunch**

1:15 – 2:15  **Presentation and Discussion**  
**Eric Kaufman**, Safety & Reliability Manager, GE Energy Infrastructure – Engineering

2:15 – 2:30  **Break**

2:30 – 3:30  **Presentation and Discussion**  
**Kenneth R. Balkey, P.E.**, Consulting Engineer, Nuclear Services, Westinghouse Electric Company, LLC

3:30 – 4:00  **Wrap Up Discussion and Closing Comments**  
Review common themes  
Identify key lessons learned

4:00  **Adjourn Day One**

5:30  **Dinner (location TBD)**

---

**TUESDAY, OCTOBER 5, 2010 (PROJECT TEAM ONLY)**

7:30  **Continental Breakfast Served**

8:00 – 8:30  **Review Key Learnings from Day 1**  
Facilitated Discussion: *What were the key insights we learned on Day 1 about critical systems failures and mitigation strategies?*

8:30 – 9:30  **Identify and Prioritize Major Gaps**  
Facilitated discussion: *What are the most significant gaps in our ability to mitigate the consequences of critical systems failures?*  
Prioritize according to two criteria: 1) potential impact if filled, and 2) ability of ASME to fill the gap.

9:30 – 11:30  **Develop Recommendations for Potential ASME Action**  
Facilitated discussion: *What potential ASME initiatives can we recommend for 2011 and beyond to fill gaps and make a contribution to this field?*  
Prioritize to develop small number (1-3) of recommendations for ASME action.

11:30 – 12:00  **Adjourn**
ACKNOWLEDGEMENTS

The ASME Initiative to Address the Prevention of Complex System Failure: Results of the Industry Advisory Board Meeting was prepared by Lindsay Kishter, Sarah Lichtner, and Lindsay Pack of Nexight Group under the guidance of Reese Meisinger, Managing Director, Strategic Initiatives & External Affairs and Allian Pratt, Director, Strategic Issues. On behalf of ASME, we would like to express our appreciation to the workshop participants; the Strategic Issues Committee and its chair, Harry Armen; the Industry Advisory Board and its chair, Charla Wise; and the ASME staff, including Patti Jo Snyder, Manager, Strategic Initiatives & Innovation, for their input and recommendations.
CONTENTS

i. **Background** 58

ii. **Summary of Presentations** 59
   - Keynote Address 59
   - ASME Initiative to Address the Prevention of Complex Systems Failure: Report of the Workshop on October 4–5, 2010 60
   - The Role of Standards and Certification, Probabilistic Risk Assessment, and Organizational Levels of Defense 61
   - Identifying Complex System Risks and Actively Learning from External High-Severity Events 63
   - Managing Operations Integrity in Oil and Gas Operations 64

iii. **Top Priority ASME Initiatives** 65
   - Catalog Best Practices and Enhance Methodologies to Develop a Complex Systems Risk Assessment Model 66
   - Develop an ASME Package of Educational Materials and Products 68
   - Develop Program to Help Companies Assess and Manage Enterprise Risk 71

iv. **Next Steps** 73

v. **Raw Meeting Results** 74

vi. **Agenda** 79
i. Background

The recent tragic events in the Gulf of Mexico have heightened the public awareness of the broad-based consequences of a large-scale, complex, dynamic human-engineered system failure. These consequences include social, economic, and environmental effects. Experience, knowledge, and tools across industries are needed to aid engineers in designing fault-tolerant systems, assessing and managing risks in system operation, and considering the ethical responsibility associated with process management and maintenance.

In response, ASME convened its Industrial Advisory Board (IAB) and a task force of experts over the course of two meetings to identify future initiatives that ASME can undertake in 2011 and beyond to contribute to the understanding and more effective mitigation of complex system failure.

The first meeting, held at ASME Headquarters in New York on October 4–5, 2010, brought together an expert task force to explore experiences in complex systems management across industries. Participants identified potential areas for ASME action, including standards and tools, educational efforts, addressing organizational and ethical issues, and increasing public awareness of complex systems. High-priority areas identified from that meeting were used as a springboard for strategic planning efforts at the subsequent meeting of the ASME IAB.

This report summarizes the high-level results of that second meeting, held at the Renaissance Mayflower Hotel in Washington, D.C. on December 1–2, 2010. The advisory board and invited guests examined the high priority areas of action where ASME efforts could make a significant impact that were identified at the first meeting. The group ultimately developed a set of three initiatives and corresponding action plans for ASME efforts in the next year and beyond. This report summarizes the high-level conclusions of the meeting.
ii. Summary of Presentations

Presentations that opened the Industrial Advisory Board meeting aimed to both inform participants about current efforts to mitigate complex systems failures from a mechanical engineering perspective and to encourage thought about what actions ASME can potentially take to address these issues going forward.

KEYNOTE ADDRESS

The Honorable Richard Thornburgh, Former Governor of Pennsylvania

Mr. Thornburgh addressed the Industrial Advisory Board at the meeting’s opening reception, where he imparted lessons from his experience as the governor of Pennsylvania during the Three Mile Island nuclear accident and its impact on the state and the nuclear industry in the following years. Mr. Thornburgh had been governor for 72 days when the accident occurred, leaving the new administration to address an unprecedented event in the nuclear industry with untested and sometimes faulty emergency response plans. In the days following the accident, Mr. Thornburgh and his staff encountered experts whose information often could not be fully trusted, inaccurate news reports from media who had similar difficulty in obtaining correct information, conflicting evacuation plans in the surrounding counties, poorly analyzed radiation readings that resulted in a faulty U.S. Nuclear Regulatory Commission (NRC) evacuation advisory, and jammed or dysfunctional communication lines. He ultimately had to work across party lines, in concert with NRC management in Washington, D.C., and in cooperation with the media to pursue the facts needed to ensure the safest resolution for the area’s 250,000 residents. While the accident halted nuclear plant construction in the United States, Mr. Thornburgh noted that a positive result was an increased emphasis on safety
across the board at U.S. plants. With recent renewed interest in expanding nuclear power, success will require industry organizations like ASME to contribute to improving the design and management of complex systems, he said.

Key Takeaways

➤ In an emergency, managers must sometimes rely on a trusted “ad hocracy” rather than an untested bureaucracy when organizing an effective response to unforeseen events.

➤ Managers must be ready to restrain those who are tempted to act for the sake of action, without regard for the safety or necessity of those actions.

➤ While managers must maintain a visible and reassuring presence, round-the-clock work without rest can be counterproductive.

➤ Off-site management often results in misinformation and miscommunication; managers need a trusted person on-site during emergency response.

➤ Well-documented and widely published lessons from past events are very useful in emergency management.

➤ ASME is well positioned to make a positive contribution to improving the design and management of complex systems.

ASME INITIATIVE TO ADDRESS THE PREVENTION OF COMPLEX SYSTEMS FAILURE: REPORT OF THE WORKSHOP ON OCTOBER 4–5, 2010

Harry Armen, Sc.D., Chair of the ASME Strategic Issues Committee

At the beginning of the meeting on December 2, Dr. Armen presented the high-level results of the first meeting of the ASME Initiative to Address the Prevention of Complex Systems Failure, in which a task force of experts identified potential areas of ASME action and rated them by priority. Dr. Armen reaffirmed that addressing this issue is in “the DNA” of ASME, with its demonstrated history of transforming research and knowledge into practical applications that aid in preventing failures in multiple industries and applications. The results Dr. Armen presented provided the basis for a strategic planning session later in the day, in which the Industrial Advisory Board built upon the first three of the five priority areas identified in the first meeting:

Priority Areas for ASME Action

➤ Develop a new code, standard, or tool for assessing risk in complex systems.

➤ Educate students and current engineers to better understand complex systems and failure analysis.
Address organization issues of individual private companies or public agencies by enabling companies and agencies to better understand consequences of decisions and ethical considerations.

Increase public and political awareness about complex systems.

Address human factors.

THE ROLE OF STANDARDS AND CERTIFICATION, PROBABILISTIC RISK ASSESSMENT, AND ORGANIZATIONAL LEVELS OF DEFENSE

Kenneth R. Balkey, P.E., Westinghouse Electric Company, LLC

Mr. Balkey’s presentation provided an overview of the roles that ASME has played and continues to play in mitigating the consequences of complex systems failure in industry. One major ASME contribution was the development of the standard for probabilistic risk assessment (PRA). The PRA is a tool used heavily in the nuclear industry that prioritizes certain activities and events in terms of potential impact on risk and also allows plant designers and operating plant engineers to change the risk profile of the design. The first time the PRA was formally used, there were 65 plants conducting PRAs in 65 ways, which led to confusion and inconsistency in its approach to the risk assessment, its subsequent results, and its application in assessing actual risk. As a result, the NRC asked ASME to develop a PRA standard. ASME developed the standard and currently provides industry training programs, both of which have helped increase model robustness. Capacity factor and safety both have risen, and many organizations now use the PRA to make day-to-day operational and maintenance decisions. Mr. Balkey noted that ASME could continue to help the effort to increase the robustness and usefulness of the current PRA modeling techniques by partnering with other organizations to conduct peer reviews on plant modeling. Organizational lines of defense provide another critical protection, Mr. Balkey noted, supporting hardware defense-in-depth through four organizational levels: (1) workers and workgroups—the first to notice issues; (2) management and supervision; (3) independent assessments, and (4) external assessments. These organizational defenses can be critical in identifying issues and preventing failures, but can also override hardware defenses or maintenance schedules that are designed to prevent problems. As a result, organizational defenses are a necessary consideration in and component of an organization’s risk assessment, Mr. Balkey said.

Key Takeaways

- ASME has played and continues to play a role in mitigating the consequences of complex systems failures.

- One successful contribution was the development of the standard for PRAs and PRA training to fill the void in undergraduate curriculum.

- ASME can and should contribute in many other ways, including peer reviews on nuclear plant modeling and facilitating regional public-private partnership building for disaster response.
Organizational levels of defense play a vital role in preventing complex system failure and can significantly enhance response mitigation and recovery from serious events.

COMPLEX SYSTEMS DESIGN, ENGINEERING DISASTER, AND ENGINEERING EDUCATION: PRACTICES AND NEEDS

Gary Halada, Ph.D., Stony Brook University

Dr. Halada's presentation focused on the role of engineering education in enhancing the ability of future engineers to limit complex systems failures and respond to failure in a way that limits the possibility of future failures. Teaching complex systems design often focuses on case studies of past events, he noted, and professional organizations like ASME can play a role in providing this material for educators. Incorporating failure prevention into engineering education includes a focus on structured approaches, such as design for reliability, redundancy, fail-safe design, absolute worst case design, and probabilistic risk assessment (PRA). Teaching PRA for complex systems, though difficult and often left out in undergraduate education, is critical for students to understand the inherent difficulties in risk analysis for complex systems from dynamic or unclear boundary conditions, long time scales, uncertainties from incidental interactions, and especially, the role of human factors. He provided his personal experience teaching his “Learning from Disaster” course as an effective way to teach students from a variety of backgrounds the ethical, economic, societal, and environmental impact of engineering. In the culminating activity of the course, Dr. Halada challenges his students to choose a past systems failure and “prevent” it from happening. Through exercises such as this, students learn causes of failure, risk, and uncertainty; focus on system design and how to design for reliability; and examine what is needed to avoid similar catastrophes without the psychological bias of hindsight or overconfidence—skills that will enable them to approach risk mitigation and failure response in an innovative and effective way.

Key Takeaways

- Lifelong learning is a key way to prevent human failures; it encourages thoughtful insight, and the concept of designing for failure becomes second-nature and more innovative.
- Engineering-based industries are facing a wave of retirement of the technical people who built complex systems, making education of the next generation of engineers critical.
- Human factors play a major role in the cause and effective mitigation of critical systems failures.
- It is the responsibility of engineering professionals to better educate engineers by incorporating PRA and other models into engineering courses with a focus on the inherent uncertainties and human dimension of complex systems.
- Professional societies like ASME can help enhance the anti-disaster education of current and future engineers by making educational materials—such as case studies, standards, and PRA methods—available to educators for integration into course curricula.
IDENTIFYING COMPLEX SYSTEM RISKS AND ACTIVELY LEARNING FROM EXTERNAL HIGH-SEVERITY EVENTS

Eric Kaufman, GE Energy Infrastructure – Engineering

This presentation focused on GE’s incorporation of risk assessments into its energy infrastructure development processes. Mr. Kaufman noted that there is a constant struggle in a business environment when a project demonstrates a major potential return on investment, but also requires taking on risk. There is a tendency to point to past history of successful operation as justification in a safety analysis instead of conducting scenario planning. Design engineers must meet technical requirements while also protecting the company brand, workers, and people who interact with the company product; this responsibility involves mitigating risks of varying levels that could result in complex system failure. While enterprise risk is high severity and high probability, with the potential to damage a company brand and product success, tail risks are high severity but low probability. The recent Deepwater Horizon incident demonstrates the importance of identifying and taking action to mitigate lower probability risks. At GE, the risk group is independent from the product design groups. The group provides engineers with a communications tool that quantifies risk and helps them respond quickly in the face of a threat or disaster to transition from an unidentified or unacceptable level of risk to an acceptable level of risk. The group also conducts reviews of every product that include quantitative risk modeling (the accident scenario review). In addition, the group measures the risk growth of an existing fleet over time and examines external events, such as the Kleen Energy power plant explosion that occurred in Connecticut in February 2010, to apply the lessons learned to its own products and processes. At GE, the cross-business product safety team, common workflow process and record system, single safety risk quantification process, audits on process execution, standardized metrics and trending, and continuous improvement feedback loop all work together to enable proper risk assessments. By conducting these assessments, there is a better understanding during the design phase of whether or not redundancies need to be built into the system.

Key Takeaways

➤ Business goals often conflict with risk management. A standardized risk assessment process can help create a company safety culture by identifying both enterprise and tail risks.

➤ Risk assessment extends beyond meeting codes and standards and includes the responsibility of protecting the company brand, workers, and people who come in contact with company products.

➤ GE has a risk management group that cuts across all product development groups, providing a consistent and streamlined way to ensure that its products meet acceptable levels of risk.

➤ Human error must be integrated into the design process to optimize human performance over the course of the product lifecycle.
MANAGING OPERATIONS INTEGRITY IN OIL AND GAS OPERATIONS

J. Wayne Purdom, ExxonMobil Refining and Supply

Mr. Purdom outlined ExxonMobil’s approach to avoiding complex system failures. ExxonMobil employs complex and large-scale systems (e.g., a refinery delivering 20 million gallons per day) that must be able to operate continuously for many years with minimal disruption. Mr. Purdom indicated that new requirements for various products involve construction in hazardous areas, which introduces an additional factor to consider while maintaining operations. To avoid system failures, ExxonMobil expanded on a longstanding process industry approach that aims to prevent loss of containment by selecting the right equipment, includes operating procedures and practices, and involves both offline and online maintenance to restore the strength of equipment. The ExxonMobil Operations Integrity Management System includes 11 elements (management leadership and accountability, risk assessment and mitigation, facilities design and construction, information and documentation, personnel and training, operations and maintenance, management of change, third party services, incident reporting and analysis, emergency preparedness and response, and operations assessment and improvement) that work together to form a robust system by identifying tasks, resources, roles and responsibilities, emergency response practices and procedures, and verification and measurement mechanisms. Mr. Purdom noted that every ExxonMobil system has a site owner and administrator, integrates internal stewardship to the site leadership team, and periodically undergoes an external audit (every three years) when third-party safety professionals assess systems against the corporate standard. Active management of each critical component of the Operations Integrity Management System facilitates an individual and organizational commitment to reliable and safe operations and enables improvements in system performance.

Key Takeaways

➤ Successful performance requires a systematic emphasis that includes both facilities and people.

➤ Effective risk assessment and mitigation is an ongoing process that enables ongoing awareness of critical system issues.

➤ The ExxonMobil Operations Integrity Management System breaks risk management into 11 elements that identify tasks, resources, roles and responsibilities, emergency response practices and procedures, and verification and measurement mechanisms of activities affecting critical system design, construction, and operation.

➤ Active management of each critical component of the Operations Integrity Management System facilitates reliable and safe operations and enables continuous improvements in system performance.
iii. Top Priority ASME Initiatives

The meeting participants were divided into three groups focused on ASME priority needs related to complex system failure, shown in the table below. Each group developed an initiative to address its priority area according to three criteria: the initiative (1) represents an area of ASME strength, (2) has the potential to have a significant impact on mitigating complex system failures, and (3) can realize progress in one year (see Section v for the raw results of this meeting).

<table>
<thead>
<tr>
<th>Priority Need</th>
<th>ASME Initiative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop Standard or Tool on Global Methodology for Risk Analysis in Complex Systems</td>
<td>Catalog best practices and enhance methodologies to develop a complex systems risk analysis model</td>
</tr>
<tr>
<td>Educate Students to Better Understand Complex Systems</td>
<td>Develop an ASME package of educational materials and products</td>
</tr>
<tr>
<td>Enable Companies to Better Understand Consequences of Decisions and Ethical Implications</td>
<td>Develop a program to help companies assess and manage enterprise risk</td>
</tr>
</tbody>
</table>
CATALOG BEST PRACTICES AND ENHANCE METHODOLOGIES TO DEVELOP A COMPLEX SYSTEMS RISK ASSESSMENT MODEL

A comprehensive methodology for assessing risk in complex systems would provide organizations across multiple industries the capabilities needed to consider the dynamic interactions and economic, personnel, and environmental influences at both a component and systems level. Industries with decades of experience in managing complex systems (e.g., nuclear, aerospace) offer a wealth of tools, practices, and case studies, from which ASME can identify core elements of effective risk assessment methodologies that individual industries or companies can use to develop tailored approaches. These practices can also form the basis of a technical complex systems risk analysis model, as well as a comprehensive risk assessment methodology that integrates both the technical and organizational factors that present unique challenges to complex systems risk assessment.

Description of the Initiative

One of ASME’s primary areas of strength and expertise is the developments of codes, standards, and technical tools to manage risk. Creating a global methodology for complex systems risk analysis will be both challenging and time consuming; however, ASME can make near-term progress on this end goal that will deliver value to industry in performing risk assessments.

The three-step approach is illustrated in the figure at right and outlined under Implementation Plan below. By building a compendium of best tools and practices, ASME can identify those that consider both technical and organizational factors (Part 1). In the near term, the tools and processes examined can form the basis of a complex systems risk assessment model that focuses on technical issues, but recognizes that subsequent integration of organizational issues must follow (Part 2). In Part 3, ASME will use the organizational best practices cataloged in Part 1 to expand the model into one or several sector-specific methodologies that accommodate both organizational and technical considerations.

Expected Impact

The initiative will better enable organizations to perform risk assessments in the near term and further improve that capability as more work is done. The methodologies developed have the potential to
evolve into a standard over time. This approach will provide the foundation for ASME’s policy and educational initiatives in this arena, and enable a flow down of requirements to suppliers.

**Implementation Plan**

This program will require the commitment of a broad group of stakeholders across multiple industries and areas of expertise, and appropriate scoping, strategic planning, and activity prioritization. To implement this program, ASME should initiate the following steps:

**Part 1: Catalog tools and processes to assess complex systems risk and develop a compendium of best practices**

*Time to complete: 2–3 years*

With its respect in the industry and role to educate engineers, ASME is well-positioned to develop and publish a compendium of technical, safety, environmental, and other best practices for complex systems management and risk analysis. Detailed practices and lessons from several experienced industries can provide a valuable learning tool to organizations, which can tailor these practices to their own industry and use them to better perform risk assessments and prepare for low-probability, high-consequence events. In the longer term, these can form the basis of this initiative’s complex system risk assessment methodologies.

**Immediate Next Steps for ASME Staff**

- Create a joint task force of volunteers and staff to develop the compendium of best practices.
- Determine the best mechanism for identifying task force members that enables broad participation from across industries and organizational roles to assist the group in pursuing all aspects of risk.
- Identify other organizations to partner with on this effort, including the American Society of Safety Engineers, the Institute of Nuclear Power Operations, the American Petroleum Institute, etc.

**Part 2: Develop a global model for conducting complex systems risk analysis by enhancing an existing model**

ASME can use a successful existing model, such as the Risk Analysis and Management for Critical Asset Protection (RAMCAP) model, as a starting point to develop a more safety-specific complex systems risk assessment model that multiple industries can use. The model can be a springboard for other ASME initiatives to enhance complex systems risk assessment, including training courses and policy initiatives.
Part 3: Integrate technical and organizational factors into one or more risk analysis methodologies (possibly sector-specific) based on best practices

Drawing on the best practices identified in Part 1, ASME will expand its model to one or possibly multiple sector-specific risk assessment methodologies that focus on promoting a culture of safety within an organization and engaging individuals with knowledge of potential problems before a failure. To be effective, a comprehensive methodology must incorporate human and organizational factors, as these factors are almost always a major contributor to complex systems failure. Collecting data across multiple industries to support the use of the developed methodologies will be valuable going forward.

DEVELOP AN ASME PACKAGE OF EDUCATIONAL MATERIALS AND PRODUCTS

While the failure of a complex system often arises from multiple smaller or cascading failures, human factors almost always play a major role. Human error can be the direct cause of or exacerbate an unraveling situation; making simple mistakes, following a standard operating procedure that worsens a situation, or being trained in one specialty but having to respond to a failure that cuts across specialties can all contribute to this issue. The specialized education and training that engineers typically receive, in combination with the retirement of the engineers who designed and built today’s most complex systems, have created a gap in knowledge that is critical to the detection, avoidance, and mitigation of complex systems failures.

Educating today’s and tomorrow’s early-career engineers about complex systems and risk assessment is necessary to decrease failures in the long term. A large number of case studies, modules, and instructional content regarding these issues currently exists throughout various industries and academia, but these are often not in a form that is readily usable in different applications and are not broadly shared. Combining existing and newly developed materials into a comprehensive, unified package will give educators and trainers a “one-stop shop” to pick and choose the tools they need to communicate the intricacies and implications of complex systems. The materials in this package will not only help to ensure that the individuals involved with complex systems know how to react in the correct way during a failure situation, but also that the engineers of today and tomorrow are constantly thinking about new and innovative ways to mitigate failure at all stages of system development and operation.

Description of the Initiative

As a recognized authority in mechanical engineering standards and best practices, ASME will use its strong education and outreach capabilities to develop and encourage the use of the materials and products that are part of the package. ASME staff and volunteers will reach out to the extensive ASME membership to gather existing complex systems and risk analysis materials and then develop new materials as needed. The package of materials and products is not limited to but could include any of the following components.
An accompanying communications plan for distributing the package of materials and products will also be developed to ensure wide use by a number of audiences, as will metrics to measure the effectiveness of the materials.

**Expected Impact**

The overall success of this initiative will be determined by its ability to have the following effects:

- Impact on individual learning and behavior: Achievement of learning objectives
- Impact on curricula: Adoption of materials into university curricula and continuing education
- Impact on industry: Long-term decrease in complex systems failure

**Implementation Plan**

The successful implementation of this program will require strategic planning, activity prioritization, and stakeholder engagement, as well as the identification and solicitation of resources from funding sources. ASME will use a phased approach for developing and distributing the package of materials and products:

**Develop initial educational package**

A project team of ASME staff and volunteers will begin by packaging existing content and gearing it toward specific target audiences (e.g., mechanical engineering department heads and practicing engineers). To accomplish this step, the team may consider contracting out the development of the package of materials to an ASME limited liability company.

**Expand package offering and audience**

After conducting pilot tests of this package, the team will then work to develop new content and expand the audience base to students at varying levels of education, engineering professionals with different amounts and types of experience, and potentially even to individuals outside of the engineering field (e.g., business majors).
Develop a communications plan to ensure broad use of the package and metrics to measure its effectiveness

The team will focus on developing a communications plan as part of this initiative by potentially conducting a workshop with educators to obtain their input and buy-in, working with the ASME Center for Education, and bringing in other societies (i.e., IEEE) to help encourage use of the materials. The team will also develop metrics based on the expected impacts to assess the effectiveness of the materials and adjust the package to better meet the needs of intended audiences as the initiative grows.

Proposed Timeline

Over the next year, the project team can likely make enough progress on the development and distribution of the educational materials and products package to have a pilot in place by Q3 2011. Meeting participants opted for a more aggressive timeline to spur action and emphasize how important they believe this initiative to be. The project team should attempt to achieve the following milestones in the timeframes indicated:

- Q1 2011: Project team established and functioning
- Q1 2011: Project proposal vetted and accepted within ASME
- Q2 2011: Development of initial set of materials (i.e., organizing and packaging existing content)
- Q2 2011: Hold stakeholder workshop to get input and buy-in
- Q3 2011: Educator(s) agree to and integrate material into their course for a pilot test
- Q4 2011: Pilot test(s) conducted

Immediate Next Steps

To stay as close as possible to the suggested timeline, ASME staff and volunteers will need to work together to achieve the milestones slated for Q1 2011 in the timeline above. Immediate next steps for the team to undertake include the following:

- Establish staff lead and volunteer champions to ensure that the initiative maintains momentum and is effectively managed.
- Establish project team to carry out the work of the project.
- Develop and vet a project proposal for the initiative.
- Begin gathering the initial set of materials and products for the package.
DEVELOP PROGRAM TO HELP COMPANIES ASSESS AND MANAGE ENTERPRISE RISK

Company organizational structures and internal decision-making processes are integral to how firms manage risk across the enterprise. They affect the capacity of a company or agency to assess, manage, and mitigate the risks of a complex system failure. Business culture and practices, including how business is conducted with customers, suppliers, and across the tiers of a company, can impact the performance and safety of a complex system, and potentially result in a tarnished company reputation, litigation, reduced funding, and other consequences that could jeopardize the future of a company.

Description of Initiative

ASME can enable companies to better understand the consequences and ethical implications of decisions by developing a program that is designed to help companies take a comprehensive, integrated approach to assessing and managing enterprise risk. Such an effort requires a comprehensive program that should incorporate autonomous and independent assessments in management processes that approach risk assessment from a business lifecycle perspective (i.e., considers risks associated with system design, development, operation, environmental impact, and company reputation). Possible program activities could include company guides and tools to understand and implement enterprise risk management, case studies, best practices, and assessments.

Expected Impact

This program will ultimately enable companies to build a corporate culture of safety and security that is synchronized across managers and all employees.

Implementation Plan

The successful implementation of this program will require strategic planning, activity prioritization, and stakeholder engagement. To implement this program, ASME must initiate the following steps:

Develop program roadmap

ASME should develop a roadmap to outline the specific program elements that will be needed to achieve the desired outcomes of this enterprise risk program. Such a program plan will identify specific needs, outline program activities, and define an appropriate timeline for activities that can be implemented by companies of different sizes from a variety of industries.

Prioritize program products and services

ASME must prioritize the possible program products and services to develop the most effective program for helping companies to assess and manage enterprise risk. Such activities may include a guide to help companies achieve enterprise risk management objectives that identifies key risk factors and determines
ways to evaluate them; case studies and best practices of organizational design to manage complex systems risk; and standards for conducting enterprise risk assessments.

**Leverage funding from government sources**

ASME can leverage its resources by partnering with government agencies and other key stakeholders to develop core program content that would provide mutual benefit to ASME member companies and the agencies. It will enable ASME to extend its reach and increase the relevance of this program to specific sectors through partnerships with government agencies (e.g., U.S. Department of Energy, Department of Defense, Homeland Security, and the Environmental Protection Agency), other societies in target industries, and other stakeholders interested in managing complex systems risk.
iv. Next Steps

The results of this workshop will be used to develop a strategic approach for 2011 and beyond that ASME and its partners can pursue to prevent and mitigate complex systems failure. The ASME Strategic Issues Committee will use the plan to guide initiatives it undertakes in this arena. Ultimately, ASME aspires to implement specific projects that increase engineers’ ability to predict, manage, and mitigate the consequences of failures in complex systems.
v. Raw Meeting Results

Each group at the December 2 meeting generated ideas pertaining to their respective topic that were captured by the facilitation team. While these results have been clarified and summarized in Section iii of this document, the charts below contain the raw ideas that were used to inform the identified path forward.
CATALOG BEST PRACTICES AND ENHANCE METHODOLOGIES
TO DEVELOP A COMPLEX SYSTEMS RISK ANALYSIS MODEL

Part 1: Catalog tools and processes to assess complex systems risk and develop compendium of best practices

➤ Start with existing safety standards across industries and identify the “best in class” that can apply to all industries
  • Build a compendium of best technical practices for complex systems
  • ASME’s role is to educate on practices; companies can tailor those practices to their industry or organization
  • Detailed practices and lessons from other industries can provide a valuable learning tool
  • These will help organizations imagine low-probability, high-consequence events

➤ Catalog tools and processes used to assess complex systems risk to identify the best practices ASME can recommend
  • Include safety, environmental, etc. practices

➤ May need to consider multiple methodologies—one-size-fits-all approach likely will not work

Part 2: Develop a global model for conducting complex systems risk analysis by enhancing an existing model

➤ The Risk Analysis and Management for Critical Asset Protection (RAMCAP) model is a good example

➤ Use RAMCAP or other existing model as the starting point and build a more safety-specific (not terrorism-specific) model
Part 3: Integrate technical and organizational factors into one or more risk analysis methodologies (possibly sector-specific) based on best practices

- Root cause of failure is most often a people issue—most difficult problem and most generic across industries
- Somebody always knows that a problem is imminent—need a methodology that finds and engages that person
- Start with a methodology and then integrate it into a standard
- First look to nuclear and mining industry best practices and case studies and expand to other sectors
- Identify best practices that promote a culture of security and safety
- Collect data now in a way that can be categorized to see how it applies to other industries
- Accumulate data after developing methodology to prove it
- The initial focus can be technical issues, but need an acknowledgement that organizational issues will need to be addressed
DEVELOP AN ASME PACKAGE OF EDUCATIONAL MATERIALS AND PRODUCTS

**Components of the Package**
- Case studies
- Standards
- Case studies with standards
- Lesson plans
- Directions on how to use the package based on the audience
- Course modules on failure analysis, details of the system, and risk analysis
- Exercises
- Continuing education module
- Video
- Develop an ASME short course on complex systems and risk analysis
- Develop and use assessment metrics to measure use of materials

**How to Develop the Package**
- ASME LLC company could be in charge of development (contract it out)
- Identify and solicit resources from funding sources
- Use a phased approach

**How to Encourage Use of the Package**
- Conduct a workshop with educators to get their input and buy-in
- Work with the Center for Education
- Bring in other societies (i.e., IEEE) to help publicize use of materials
- Develop a communications plan around these materials
### DEVELOP A PROGRAM TO HELP COMPANIES ASSESS AND MANAGE ENTERPRISE RISK

#### Key Concepts
- Enterprise risk includes risks that could jeopardize the future of a company
- Autonomous and independent assessments
- Organizational structures and human performance
- Full enterprise risk—environmental, reputation-based, operational, etc. (as opposed to just system design and development)

#### Key Objectives for Organizations
- Understand complex systems
- Incorporate autonomous and independent assessments in management processes
- Business lifecycle assessment process (e.g., design, development, and operations)
- Implement process throughout the supply chain

#### Possible Program Products and Services
- Guide to help companies achieve enterprise risk management objectives
- Identify key factors
- Determine how to evaluate factors
- Case studies / best practices of organizational design to manage complex systems risk
- Develop a standard and conduct assessments

#### Program Implementation
- Develop roadmap for the program
- Prioritize program products and services
- Funding idea: Tap government sources to help develop content (e.g., Department of Energy, Department of Defense, Homeland Security, Environmental Protection Agency, etc.)
vi. Agenda

WEDNESDAY, DECEMBER 1, 2010

5:30  Opening Reception at Sam & Harry’s Restaurant

6:30  Opening Remarks
Charla Wise, Chair, ASME Industry Advisory Board

7:15  Keynote Address
The Honorable Richard Thornburgh, Former Governor of Pennsylvania

THURSDAY, DECEMBER 2, 2010

7:30  Continental Breakfast Served

8:30 – 10:15  Plenary Session: Complex Systems Failure
Harry Armen, Sc.D., Chair, Strategic Issues Committee
Ken Balkey, PE, Consulting Engineer, Nuclear Services, Westinghouse Electric
Company, LLC
Gary Halada, Ph.D., Associate Professor, Department of Materials Science &
Engineering, Stony Brook University
Eric Kaufman, Safety & Reliability Manager, GE Energy Infrastructure –
Engineering
Wayne Purdom, Operations Advisor, ExxonMobil Refining and Supply
10:15 – 10:30  **Break**

10:30 – 12:00  **Facilitated Breakout Sessions: Key Recommendations from October Workshop**
   1. Develop Standard or Tool on Global Methodology for Risk Analysis in Complex Systems
   2. Educate students to Better Understand Complex Systems
   3. Enable Companies to Better Understand Ethical Implications and Consequences of Decisions

12:00 – 1:00  **Lunch**

1:00 – 2:30  **Recommendation Session**
   Presentations and facilitated discussion

2:30  **Adjourn**