Weaknesses and Failures
of Risk Assessment

Dr. William L. Oberkampf

Consulting Engineer
Austin, Texas
wloconsulting@gmail.com

Motivation

- **How well has quantitative risk assessment performed in high-consequence:**
  - **System failures?**
  - **Modeling and simulation analyses?**

- **What improvements are needed in:**
  - **Quantitative risk assessment?**
  - **Characterization of uncertainty?**
  - **Risk-informed decision making?**

Outline of the Presentation

- **Review the structure of quantitative risk assessment (QRA)**

- **What can be learned from recent:**

  - **High-consequence system failures**

  - **High-consequence modeling and simulation (M&S) analyses**

  - **Criticisms of QRA**

- **Lessons learned**

- **Closing remarks**

Structure of Quantitative Risk Assessment

The goal of QRA is to quantify the answer to three questions (Kaplan and Garrick, 1981):

1) What can go wrong?

2) How likely is it to go wrong?

3) What are the consequences of going wrong?

How Do We Answer These Questions?

1. **What can go wrong?**
   - Identify initiating events (abnormal and hostile environments)
   - Construct plausible event and fault trees (scenarios)

2. **How likely is each plausible scenario?**
   - Use experimental and operational data to characterize probabilities
   - Use expert-opinion to characterize probabilities
   - Assume independence/dependence between events/subsystems
   - Use M&S to predict outcomes of each scenario
   - Compute probabilities of each scenario

3. **What are the consequences of each scenario?**
   - Merge probabilities and adverse impact to obtain a consequence for each scenario

   or

   - Deal directly with computed probabilities of each scenario

What Can Be Learned From High-Consequence System Failures?

- **Three Mile Island Event (1979)**

- **Loss of Space Shuttle Challenger (1986)**

- **Chernobyl Disaster (1986)**

- **Loss of Space Shuttle Columbia (2003)**

- **Fukushima Disaster (2011)**

What Can Go Wrong?

- **Identify initiating events:**
  - **(Chernobyl) Incorrect recognition of plant operator actions during a reactor-test scenario**

- **Construct plausible event and fault trees for each scenario:**
  - **(TMI) Incorrect recognition of plant operator actions during a minor abnormal event**
  - **(Fukushima) Incorrect recognition of the impact of a large tsunami**

How Likely Is Each Plausible Scenario?

- **Use experimental and operational data to characterize probabilities:**
  - (Challenger) Operational data on O-ring leakage was overruled by management

- **Use expert-opinion to characterize probabilities:**
  - (Fukushima) Gross underestimate of the probability of a large tsunami

- **Assume independence/dependence between events/subsystems:**
  - (Fukushima) Assumed independence of cooling-water-pump failure

- **Use M&S to predict outcomes:**
  - (Columbia) Erroneous use of M&S to predict foam impact damage

- **Compute probabilities of each scenario:**
  - (TMI) Gross underestimate of the probability of severe core damage
  - (Fukushima) Gross underestimate of the probability of severe core damage

What Are The Consequences
of Each Scenario?

- **Merge probabilities and the negative impact to obtain the consequence of each scenario:**
  - **(TMI) Gross underestimate of the impact of the failure**
  - **(Columbia) NASA management unwilling to take prudent action while Columbia was in orbit**
  - **(Fukushima) Japanese Nuclear and Industrial Safety Agency did not act on warnings of the risk of loss of electrical power by the U. S. Nuclear Regulatory Commission in 1990.**
  - **(Fukushima) Gross underestimate of the impact of the failure**

Constructive Criticisms From Pilkey and Pilkey-Jarvis (2007)

- **Prediction of complex natural processes is essentially impossible**

- **Model calibration is fundamentally different than model prediction**

- **Risk assessment can be misused (or ignored) to fit the agenda of groups that have a vested interest in the activity**

- **Recommendations for risk assessment:**
  - **Assessment should be transparent and open to review**
  - **Parameters should be based on experimental and field observations**
  - **Should be reproducible by an independent party**

Lesson Learned 1

- **Lack of an external, independent, review of a QRA can destroy its credibility**

  "The fundamental question should not be whether old studies (1 in 100,00 loss of crew) were inaccurate. What is important is what NASA does with them." (Apostolakis, 2004)

"The [NASA] safety organization sits right beside the person making the decisions, but behind the safety organization, there's nothing back there. There's no people, money, engineering expertise, analysis." (Admiral Gehman, 2003)

- **Conclusion:**

Lack of independent review of a QRA and lack of use of a QRA is a purposeful decision of the controlling authority.

Lesson Learned 2

- **Expert-opinion-based probabilities and assumed independence of events/subsystems have been grossly in error**

- **Helton et al (2011) stated:**

"When confronted with a probability or a calculation involving probability, the first two questions to ask are ''What is the sample space?'' and ''What subset of the sample space is under consideration?''. If you do not know the answers to these two questions, then you do not know enough to meaningfully assess the probability or calculated result under consideration. … Basically, having a probability without knowing the associated sample space and the subset of that sample space for which the probability is defined is analogous to knowing the answer to a question without knowing what the question is."
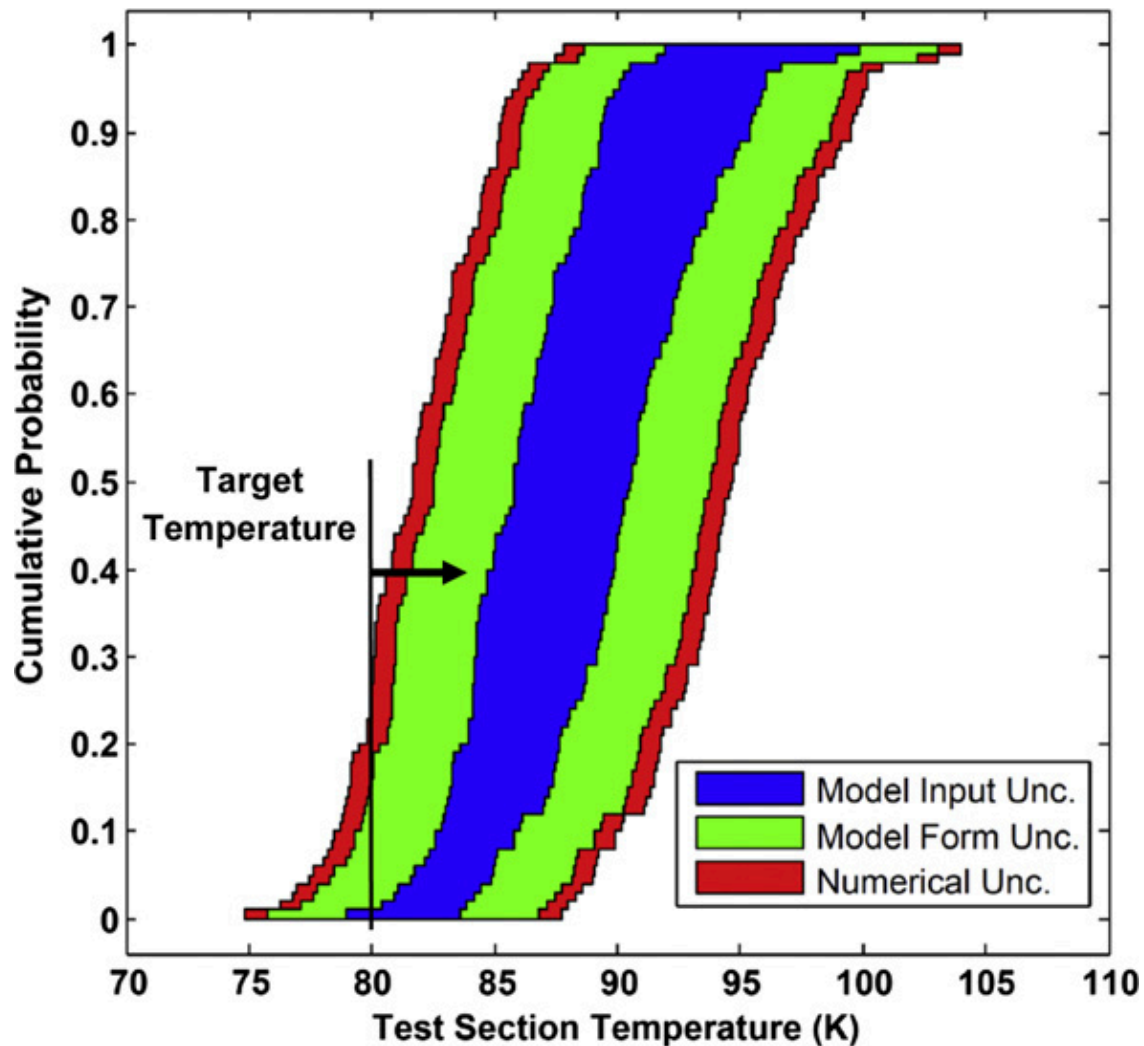
Conclusion:

Lack of understanding of the assumptions and details of the analysis are lost in communication.
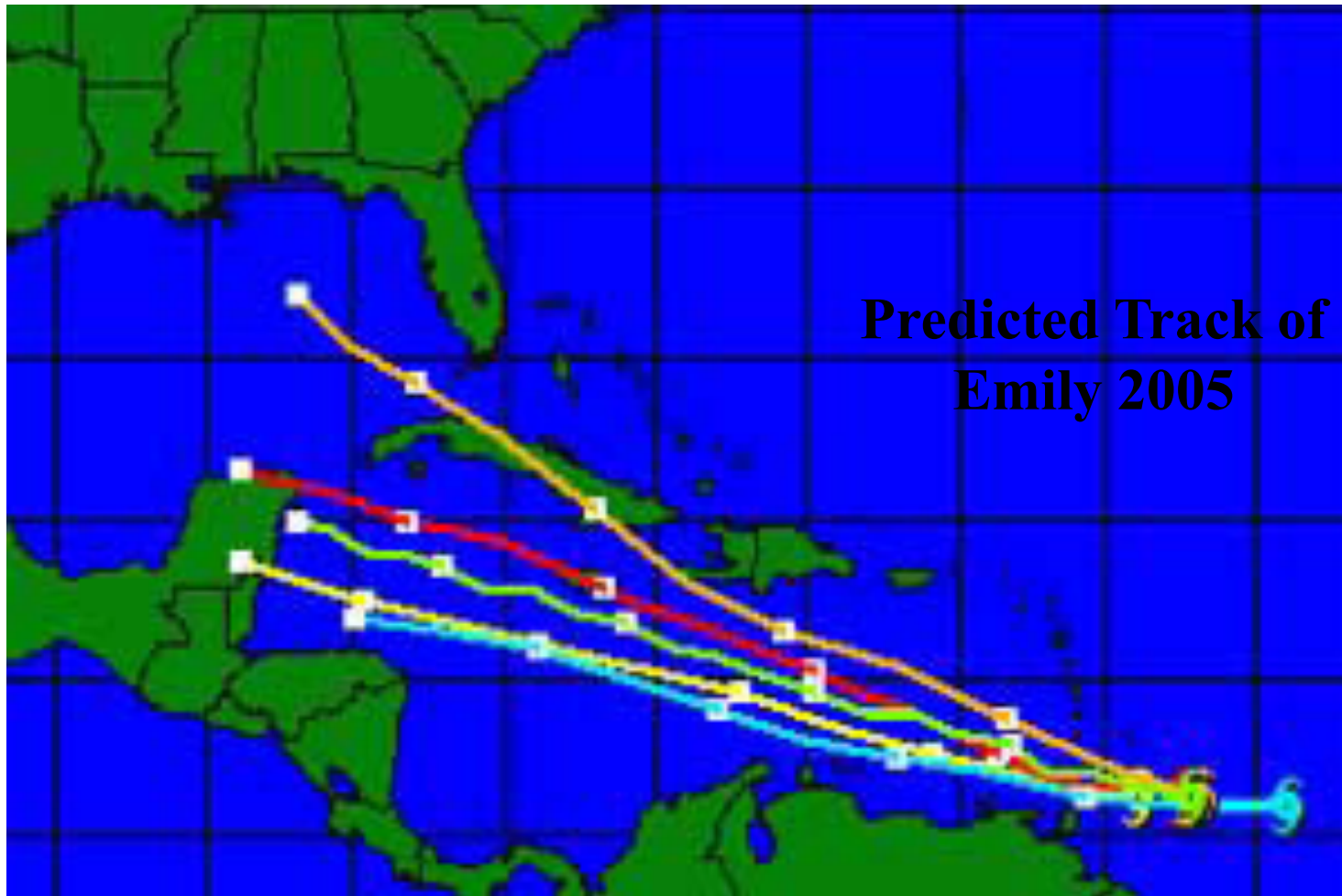
Lesson Learned 3

- **Using model calibration can greatly underestimate model form and model-parameter uncertainty**

- **Lipton (2005) stated:**

  "Accommodation [calibration] is like drawing the bulls-eye afterwards, where as in prediction the target is there in advance."

- **Conclusion:**

  Lack of knowledge due to model form and parameter uncertainty is underrepresented to the decision maker.

Example Of How Uncertainty
Can Be More Clearly Communicated

From Roy and
Oberkampf (2011)

Another Example

Predicted Track of Emily 2005

From Green (2007)

Concluding Remarks

- **Risk assessment community must improve the clarity of communicating uncertainty by using imprecise probability distributions.**

- **Increased uncertainty bounds commonly lead to results that are unwelcomed by decision makers and vested interests.**

- **When high risks or system failure are predicted, prediction carries much less influence than observed failures.**

- **Attorneys, politicians, and special interest groups have little interest in the "truth", transparency, or independent-peer-reviewed risk assessment.**

- **For high-consequence systems there must be significant independence between the system operator and the regulating authority.**

References

- Apostolakis, G. E. (2004). "How Useful is Quantitative Risk Assessment?" *Risk Analysis. 24(3), 515-520.*

- Gehman, H. W. (2003), *Aviation Week & Space Technology*, May 23.

- Green, L. L. (2007), "Uncertainty Analysis of Historical Hurricane Data," American Institute of Aeronautics and Astronautics, Paper 2007-1101.

- Helton, J. C., J. D. Johnson and C. J. Sallaberry (2011). "Quantification of Margins and Uncertainties: Example Analyses from Reactor Safety and Radioactive Waste Disposal Involving the Separation of Aleatory and Epistemic Uncertainty." *Reliability Engineering and System Safety. 96(9), 1014-1033.*

- Kaplan, S. and B. J. Garrick (1981). "On the Quantitative Definition of Risk." *Risk Analysis. 1(1), 11-27.*

- Lipton, P. (2005). "Testing Hypotheses: Prediction and Prejudice." *Science. 307, 219-221.*

- Roy, C. J. and W. L. Oberkampf (2011). "A Comprehensive Framework for Verification, Validation, and Uncertainty Quantification in Scientific Computing." *Computer Methods in Applied Mechanics and Engineering. 200(25-28), 2131-2144.*