

A Window of Opportunity for INCOSE: The Zeroth Order Risk Management Standard

A Position Paper for the International Symposium Panel:
Myriad Multiplying Risk Management Standards
“Converging Toward Best Practice” or “A Maze of Docs to Trap Us?”
Would an INCOSE Systems Approach Help or Hurt?

Mark A. Powell
Stevens Institute of Technology
Attwater Consulting
mpowell@stevens.edu; attwater@aol.com
208-521-2941

Copyright © 2006 by Mark A. Powell. Published and used by INCOSE with permission.

Abstract. Risk and risk management are difficult to perform well, despite the fact that we use risk and manage risk in our every day lives. Systems engineers almost always perform risk management in projects, and are faced with a number of risk management standards that often conflict, and rarely are complete. It seems that each industry attempts to republish its own version of a risk management standard, with a jargon unique to that industry. INCOSE has a window of opportunity now to advance the practice of systems engineering, specifically the practice of risk management. INCOSE can provide the systems engineer with guidance on these different standards, how to use them, how they conflict, what are their deficiencies, and how to address these deficiencies. INCOSE can further provide a “zeroth” order standard on risk and risk management, to help the systems engineer required to comply with some other standard. This “zeroth” order standard should also provide “how to” guidance for properly performing a quantified risk assessment, the heart of risk management.

Introduction

It is an extreme irony that systems engineers face the problem of having so many risk management standards from which to choose. All of us, systems engineers and others, live with risk and manage risk successfully in every day of our lives, personal as well as professional. Every decision ever made by the human mind has also been based on some assessment of the risk each alternative poses to achievement of some desired outcome. So, why should there be more than one risk and risk management standard? The answer is that despite all this, we as humans do not understand risk and how we use risk very well, even though we use it and manage it quite successfully in everyday life.

An analog to this conundrum is that of a major league batter. Most engineers learn in their first two years of undergraduate school how to write the six-degree of freedom equations of motion for a pitched baseball. Engineers can solve these differential equations, and predict exactly the path of a pitched baseball. A major league batter solves these differential equations as well, but

not like the engineer. The major league batter integrates these equations deep within his subconscious mind. Good batters make contact with a large majority of pitches at which they swing. Really good batters not only make contact frequently, but also contact well enough to make it to first base or beyond about a third of the time at bat. We, like the major league batter, use risk effectively every day to make decisions, integrating complex mathematical and statistical equations in our subconscious. But unlike the engineer, for most real world problems, we cannot write down clean easily solvable equations for the risk.

Risk itself has actually been quite hard to define. Just about every standard on risk starts with a definition of this and other related terms. Some define risk in a purely adverse context. Others define it in a context that can be adverse or advantageous. Some include in the definition of risk a link to some root cause event, which helps kick off the risk analysis activity but complicates things in reality. Rarely does the INCOSE Risk Management Working Group (RMWG) meet without some discussion of the definition of risk, or at least discussion of competing definitions. And the INCOSE RMWG members are all grizzled veterans of the risk management practice.

The practice of risk management does not enjoy a history of stellar successes. Bahill (Bahill and Henderson, 2005) and numerous other sources have identified many well-known failures of systems engineering. If one were to look a bit closer at these failures, even though most have other attributions for cause, it is relatively easy to see that there was also some failure in identifying, analyzing, and assessing risk. Not only that, but the practice of risk management does not enjoy clear clean metrics (Roberts and Kitterman, 2005), much like systems engineering itself. When risk management is successful, there are not very many problems to identify as being avoided by good risk management. Identifying a risk, some consequence adverse to a project, that never materializes, regardless of mitigation or not, usually is viewed as a waste of resources. However, failure to identify a risk that does materialize and become a problem is viewed as a failure of risk management, and by association, failure of the systems engineers. It seems risk management can only be a risky proposition for the systems engineer.

Inherent in risk and risk management is the issue of uncertainty. The measure of uncertainty is probability, and hence the measure of risk is probability. Risk assessment is the process of statistically inferring the measure of risk (i.e., the probability of a risk being realized) from all available data and information. Statistical inference for risk produces a quantified probability that the risk exceeds or is below some level. This is a probability of a probability (the risk). Merely mentioning this concept to most systems engineers produces a glassy eyed stare. This is very problematic, and may be one of the primary sources of risk management angst. It is also most likely one of the reasons so much effort is expended in defining terms in standards. Risk is a difficult concept to grasp.

For the real world problems faced by systems engineers, with limited data of various types that need to be somehow fused, statistical inferences to quantify the risk are often seemingly impossible to perform, even for a trained professional statistician. Few systems engineers are trained as professional statisticians, not that it helps much. So systems engineers, and other practitioners of risk management, are mostly forced rely on qualitative risk assessments for their risk items. Qualitative or semi-qualitative risk assessments are best guesses, nothing more, and only as good as the guessers. It is not much of a stretch to trace the famous failures of systems engineering to qualitative practices. Ex post facto quantitative risk assessments always reveal these mistakes. The shuttle Challenger accident is a good example of this.

And to top it all off, risk management is a big business now. There are numerous software tools that can be used in the practice, most quite pricey. Virtually all of these tools fall into two

categories, risk analysis tools and risk bookkeeping tools (tracking and control). Hardly any of these tools offer any real risk assessment capabilities. Some offer a few classical statistical tests, but these traditional methods are well known to impart conservatism and do not work well for risk assessments. There are also quite a few professional conferences each year that focus specifically on risk and risk management, mostly hosted by professional societies for which risk management is just an adjunct activity. INCOSE in fact sponsored the Project Risk Symposium 2006 in Houston earlier this year, in conjunction with the Project Management Institute (PMI). Both PMI and INCOSE have documents that address risk management, essentially providing standards to the systems engineer.

The Problem with Multiple and Conflicting Risk Management Standards for the Systems Engineer

Multiple and conflicting risk management standards are a big problem for the systems engineer. In projects that practice risk management, if there is a systems engineering organization, risk management almost universally falls to them. Gary Lyles, chief engineer of NASA's Exploration Systems Mission Directorate, declared last year at the NASA Exploration Systems Risk Summit that risk and risk management belongs to systems engineering as part of its discipline. This is not an uncommon sentiment.

In projects organized without a clear systems engineering function, risk management is almost always practiced out of project management. In these cases, systems engineering is also practiced as a project management function, so as far as risk management is concerned, this is really no different from projects with a clearly defined systems engineering organization. The persons responsible for risk management are almost always responsible for systems engineering, whether they have a systems engineering title or not. A systems engineer always gets stuck with the risk management job. This is right and proper.

Systems engineers by tradition are heavily dependent on standards. This is most likely due to the heavily standards laden DoD environment where many systems engineers learned their craft. Systems engineering is now found in many non-DoD arenas, some of which rely on standards, some do not. Even for those that do not, it would not be surprising if systems engineers were the champions of developing standards for them. As is usually the case, systems engineers prefer working to a standard with which they are familiar. Many adopt DoD standards to their new field, or rewrite them to use the vernacular of the particular industry. NASA, which could very well use most DoD standards directly, always insists on rewriting them. This happens with risk management standards as well.

Conflicting standards were rarely if ever a problem in the DoD environment. This is apparently not the case for other arenas where standards are being borrowed or rewritten, especially for risk and risk management. In some cases, the customer levies requirements to use more than one standard that addresses risk management. For a systems engineer, this makes things very difficult in the practice of risk management. Little things like definitions of a risk, and the risk management activities, easily differ from standard to standard, and can render the practice less than optimally effective.

Often, a standard is written such that none of the available risk tools work well with it. Sometimes a standard is written to enable easy use of some particular tool. The NASA Procedural Requirement (NPR) 8705.5 on Probabilistic Risk Assessment appears to be written

such that adherence is easy if using one particular tool from the Idaho National Laboratory. One failing of modern systems engineering is reliance on tools to the exclusion of really understanding what the tool is doing. This greatly complicates the risk management picture for the systems engineer, especially if the tool cannot help with the all important risk assessment process.

Why there are so many different risk management standards. As suggested earlier, risk management is difficult to understand, even though we all use it effectively every day. Quantitative risk management is especially difficult to both understand and execute. The primary problem is fundamentally that we have to use probability and statistics in risk. Probability and statistics is generally very mathematically intense. And for risk, the probability and statistics that is needed goes beyond that usually taught to engineers. Each industry, and each group involved with risk, wants risk and risk management to be easy to use. So far, every risk management standard I have read cannot be described as excessively clear on exactly how it should be practiced. It seems that all standards these days are becoming more generalized, with fewer specifics, than the standards were from a generation ago. None of these standards provide a “how to” manual for the practice. To be able to effectively use most risk management standards these days, a systems engineer needs to be sufficiently seasoned in the practice to have been an author of the standard.

Every industry has some risks (or at least potential consequences) that are inherently unique. Each industry has its own jargon, and a unique jargon for risk. And every standard written is an attempt to simplify risk and risk management to make it easier to use for those in the industry. My observation is that just about every risk management standard fails at this. I also have observed that these standards do not appear to be converging to any sort of common practice of risk management.

Risk management is just plain difficult. The concepts are difficult and the definitions are hard to explain. Risk identification and risk analysis are processes that require that engineers look for faults in their work, an anathema to the way most of us were trained. Risk assessment is a complex and mathematically intense statistical inferential process that must fuse very unlike data types. The standard statistical tests (z, t, chi-square, F, goodness of fit tests, etc.) that we learned as engineers, and available in most computer tools, do not work well for risk and risk management. The math and statistics in risk assessment themselves are usually at the graduate level for most real world problems, and few systems engineers maintain their math skills at that required level. Each risk management standard is written as an attempt to solve these problems, to make risk and risk management easy to use. The idea is that if it is easy to use, people will use it. I also have observed that these standards do not appear to be converging to any sort of common practice of risk management, easy or not.

All risk management standards are inadequate. Over the past thirty plus years, I have only sampled about a dozen risk standards. I have found what I believe are serious problems in all of them. To start, rather than clarify the meanings of the various terms, most definitions have been so generalized that they cause more confusion, especially for a systems engineer who has not focused on risk management for most of their career. NASA’s NPR 8705.5 companion guide (Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners) for example describes a rigorous mathematical risk assessment process. Later in the examples, the

authors apparently use the famous S. Harris cartoon step three (“Then a miracle occurred.”) by only showing what is to be done after the statistical assessment, assuming that everything worked out well. The risk assessment process they describe is the hard part that needs good examples. This guide also begins to mix terminology that was previously defined, often calling a statistical assessment just an update.

This is not an uncommon situation for most risk management standards, and can really confuse the systems engineer who is going to rely on the standard. It almost seems that the authors of the standards have as much difficulty understanding risk and risk management as those systems engineers who need that understanding.

So far, I have seen no risk standard that properly addresses how to perform the important step of risk assessment. The new 2006 Risk Management Guide for DOD Acquisition, recently reviewed by the INCOSE RMWG, completely ignored the statistical processing of data to assess the risk. This standard claimed that risk assessment was the combination of risk identification and risk analysis, completely ignoring any sort of statistical inference of risk from data. The RMWG addressed this omission in comments by referencing the standard that provides the closest intimation of how to perform risk assessment. This standard is the US Government’s Office of Management and Budget’s Proposed Risk Assessment Bulletin, which was also reviewed by the INCOSE RMWG. This document is the top standard that applies to the practice of risk management by all US government agencies, including the US DoD, and compliance by law is required of all US government agency risk management standards. Yet, this standard merely requires that all presentations of risk should display the entire uncertainty distribution for the risk vice point estimates. This suggests how to perform risk assessment, leaving the methodology to the assessor. Most authors of standards in general think this is a good idea. As a practicing systems engineer, I want to know how to do it.

It is not apparent that any entity is attempting to identify the conflicts, gaps, and redundancies in all the existing risk management standards. It is not apparent that such an effort would be welcome by the owners and authors of these standards either. The literature is not rich with reports extolling success in using any particular risk management standard. And risk management standards seem to be multiplying; at least the numbers grew while the RMWG was preparing this panel.

Recommendations to address the problem of multiple and conflicting risk management standards. It seems that the primary victims of the myriad of risk management standards are mostly systems engineers. Systems engineers perform risk management, and risk management standards have largely failed to satisfy their requirements for good guidelines on how to best perform risk management.

The practice of risk assessment is poorly understood in general, and no standard explains with good clarity to the systems engineer how to perform a good quantitative risk assessment. There has always been a very good reason for this, until recently.

The reason: risk and risk management practices were developed initially in the middle of the last century, mostly in the great graduate business schools. The practice has not really advanced much since the 1970’s. The process for performing a risk assessment was always a Bayesian statistical estimation process. Bayesian statistics always produces the full distribution of a risk. Without specifically addressing it, the OMB Risk Assessment Bulletin required the use of Bayesian statistics in performing a risk assessment by requiring display of the full distribution of

the risk. However, OMB did not explain how to obtain the required full distribution of risk to display. The NASA NPR 8705.5 procedures guide did explain the mathematics behind a Bayesian statistical inference, but only provided some nice textbook type examples solvable analytically. Real world risk assessment problems faced by systems engineers have been rarely solvable analytically and as easily as textbook examples. In fact, up until about 10 to 12 years ago, virtually all real world risk assessment problems could not be solved using Bayesian statistics. Bayesian statistics almost always produces analytically intractable and non-integrable risk assessments for real world risk problems. These assessments are not amenable to solution using numerical methods, even using ordinary Monte Carlo methods. However, in the early 1990's, in Europe in biomedical fields, statisticians developed new numerical methods with which it is very easy to solve real world risk assessments using Bayesian statistics. The vast majority of the literature using these methods has been published in European and South American medical and biostatistics journals. These methods are now being applied to real world risk problems faced by systems engineers (Powell and Sheppard 2002, and Powell 2004), but are not in widespread use in the practice of risk management. Systems engineers need to understand both Bayesian statistics and these new numerical methods to properly perform risk assessments. There are a number of textbooks now that cover both topics (Berger 1980, Gamerman 1997, Gilks et al 1996, Jeffreys 1961, Schmidt 1969, and Sivia 1996), and they address work mostly by European and South American biostatisticians. Systems engineers and biostatisticians do not really enjoy a common vernacular and approach to solving problems. Systems engineers who need to perform risk assessment really need training with examples in systems engineering to augment these texts. Only Stevens Institute of Technology offers training in these new methods in their systems engineering graduate programs.

I have two recommendations to address these problems. These recommendations provide a means for INCOSE to serve systems engineers who perform risk management. There is a window of opportunity to solve this problem of the myriad of risk management standards.

Recommendation 1: The INCOSE RMWG should review all existing risk management standards and provide a matrix of commonalities, conflicts, and gaps. This product will provide a guide to systems engineers to the existing risk management standards, and how to use them. Systems engineers using this product will not be forced to perform an analysis of standards to identify the conflicts and gaps to plan an effective risk management program as they must today. The INCOSE RMWG will have performed the lion's share of that onerous task. The matrix should further identify potential sources for filling the gaps, with recommendations for addressing conflicts between standards. This product should be reviewed annually as standards evolve and new standards are identified.

Recommendation 2: The INCOSE RMWG should produce a "zeroth" order risk standard for use by systems engineers in conjunction with other required standards. This standard should clarify commonalities amongst all standards' definitions, and relate each standard's definitions to the general concepts of risk and risk management. It should establish clear procedures for performing risk assessments using Bayesian statistics and the new numerical methods mentioned earlier, with real world systems engineering examples. This "zeroth" order risk standard should be a "how to" manual for systems engineers to perform risk management. It should not be intended to take precedence over any other risk management standard, but provide guidance and insight that will make the practice of risk management using other risk management standards much more effective.

Summary and Conclusions

Risk and the practice of risk management are complex and difficult. They are difficult on a conceptual level. Many agencies and industries, recognizing an imperative need to practice good risk management to assure project success, have developed and established risk management standards. However, nothing seems standard across all these standards.

Systems engineers, whether or not a systems engineering organization exists in a project, perform risk management. They are faced with a myriad of risk management standards that are all wanting. Systems engineers need some means to understand each standard, and how best to use it. Systems engineers need good guidance on how to properly perform risk assessments.

INCOSE can significantly advance the practice of risk management by systems engineers, and provide service to systems engineers, by directing the RMWG to develop two products. One is a guide to existing risk management standards, identifying the commonalities, conflicts, and gaps, providing clarity and resources for addressing the gaps. The second is a “zeroth” order risk standard for use by systems engineers in conjunction with other required risk management standards. This “zeroth” order risk standard will provide detailed guidance on how to perform risk assessments using Bayesian statistics and the new numerical methods that enable solutions.

These recommendations offer the potential for convergence, definitely in the practice of risk management by systems engineers, and possibly amongst the myriad of risk management standards that exist today.

References

- Bahill, A. Terry, Henderson, Steven J., *Requirements Development, Verification, and Validation Exhibited in Famous Failures*. Systems Engineering, 8(1): 1-13, 2005.
- Berger, James O., *Statistical Decision Theory and Bayesian Analysis, Second Edition*. Springer-Verlag, New York, 1980.
- Gamerman, Dani, *Markov Chain Monte Carlo*. Chapman & Hall, London, 1997.
- Gilks, W. R., Richardson, S., and Spiegelhalter, D. J., *Markov Chain Monte Carlo in Practice*. Chapman & Hall, Boca Raton, Florida, 1996
- Jeffreys, Harold, *Theory of Probability*. Oxford University Press, Oxford, 1961.
- Powell, M. A., Sheppard, E. B., *Applications of Conditional Inferential Methods for Operational Cost Savings for US Coast Guard C130 Aircraft Maintenance*. Proceedings from the 12th Annual International Symposium, International Council on Systems Engineering, Las Vegas, 2002.
- Powell, M. A., *Optimal and Adaptable Reliability Test Planning using Conditional Methods*. Proceedings from the 14th Annual International Symposium, International Council on Systems Engineering, Toulouse, France, 2004.
- Roberts, Barney B., Kitterman, Richard, *Measuring the Performance of the Risk Management Process*. Proceedings from the 15th Annual International Symposium, International Council on Systems Engineering, Rochester, New York, 2005.

Schmitt, Samuel A., *Measuring Uncertainty, An Elementary Introduction to Bayesian Statistics*. Addison-Wesley Publishing Company, Inc., Phillipines, 1969.

Sivia, D. S., *Data Analysis, A Bayesian Tutorial*. Oxford University Press, Oxford, 1996.

BIOGRAPHY

Mark A. Powell. Mr. Powell is currently a member of the systems engineering faculty at Stevens Institute of Technology. After a career of over 30 years in systems engineering and project management, he maintains an active consulting practice for engineering and management, and has had customers worldwide. Mr. Powell recently provided systems engineering consultation supporting government oversight on the \$22B Future Combat System for the Army and the Defense Advanced Research Projects Agency. Most recently, he has performed quantitative risk assessments for numerous projects at the NASA Johnson Space Center. Mr. Powell serves INCOSE as chair of the Risk Management Working Group, and participates in the Education and Research Technical Committee and Technical Visions Workshops. He also is a member of the INCOSE Speakers Bureau, and provides entertaining and informative programs for chapter meetings on a variety of system engineering topics.