Risk in S&T: A Fresh Look
A Systems Engineering Approach

AFRL/RX Systems Engineering Team
Bob Rapson, Bob Enghauser, Bill Kesling, AFRL/RX
Tom Archer, Carol Ventresca, Bryan DeHoff, SynGenics
Gerry Hasen, Universal Technology Corporation

14th NDIA Systems Engineering Conference
San Diego
October 2011
Abstract

In S&T, the word *risk* carries connotations of uncertainty, fear, and the likelihood of wasted time and effort. The conservative S&T manager may conclude that no “risky” project is worth doing. This paper argues for accomplishing more effective S&T through more accurate recognition and thorough addressing of risk at both the technical and strategic levels.

Risk is easily trivialized when it is described as a schedule slippage or cost overrun. These are simply causes for far more dramatic disasters in S&T. There is an implicit assumption that greater risk leads to greater rewards. While it is an appealing premise that may apply in lotteries and casinos for recreation, it has no place in S&T. Instead, it is a problematic assumption that helps to rationalize casual risk management practices.

The briefing challenges the often-stated axiom that S&T is inherently *the business of risk*. Professional S&T management is the business of eliminating risk, both within S&T and for the S&T mission.

The true *risks*, or more accurately, failure modes, in S&T are often unrecognized or ignored. In fact, risk is generally well managed when explicitly recognized. In some cases, the S&T objective is to characterize risk. Risk has three components: a definition, a probability of occurrence, and an undesirable consequence. In S&T, the definitions are often misstated, the probabilities are rarely known, and the consequences are regularly trivialized. So what is usually described as risk is more accurately *uncertainty*. Using the elements of risk, recognizing that they need to be applied with mathematical precision in an environment of uncertainty, leads to developing more effective S&T.

This briefing captures the current state of risk recognition and management in a typical S&T environment: it proposes an approach that is more focused on the end user and that attains the rigor and precision necessary to manage elements of risk to enhance the outcomes of S&T efforts.
Outline

- Overview
- Risk in S&T
- Elements of Risk and Consequences
- Assessing and Managing Risk in S&T, the Systems Engineering Approach
- Discussion
Risk in Science & Technology (S&T) Is Problematic

- *Risk* is about the unknowns and un-knowables.

- S&T is about the future; everything we *know* about *risk* is in the past.

- S&T can be inherently low risk, or the S&T professional can embrace risk with user focus.

- Risk in S&T exists at the technical level and the executive (strategic) level.
  - The typical focus is on programmatic elements at the technical level
Greatest Risk in S&T Today:
that the work has minimal value

- Unwanted
- Unresponsive
- Prohibitively expensive
- Not conceived in a systems context
- Too late, overcome by events or commercial product
S&T Risk Exposure Areas

➢ Executive level
  – Failure to properly fund the “right” S&T
  – Failure to resource it in a timely manner

➢ Technical level
  – Selecting the best technical approach(es),
    ....with all that “best” means
  – Program planning
  – Program execution
Something is **risky** if there is an expectation or belief that there is more than a remote possibility the outcome will be bad.

- “Texting while driving greatly increases the *risk* of being injured or killed in a motor vehicle crash.”
- “The annual *risk* of being killed in a plane crash for the average American is about 1 in 11 million.”
- Flying on a commercial flight in good weather is not considered risky; driving while intoxicated is.

We have a useful common-sense notion of risk
Risk in a Professional Context

- “…gaps in the utility’s gas system records, upkeep, and emergency response plan created an ‘unacceptable risk’ of a disaster…”

Unclear

- Guaranteed a “100% probability of failure within 24 months of installation”

Clear

- “Buffett’s bet on BofA [Bank of America] may be among his riskiest.”

Inaccurate

Risk in a professional context needs clarity and mutual understanding
Risk in S&T

“Mistaken assumptions about airflow over the U.S. DARPA’s Lockheed Martin HTV-2 hypersonic glider are believed to have resulted in the early termination of its first flight on April 22, 2010….Investigators discovered a stronger-than-expected coupling between vehicle yaw and roll….Extensive post-mishap hypersonic wind tunnel testing improved designers’ understanding of the phenomenon, but failed to remove all question marks about when the transition would occur.”

Beyond the safety aspects, the HTV-2 was not risky; it was a planned experiment with minimum negative consequences and the results, though not desired, were not unexpected.

The notional thought about risk in S&T tends to focus on the objective science and the technology.

Example – Typical S&T Risk Chart

Risk Mitigation Plans:
• Cost Performance Listed as Yellow due to Program changes, including new PM. Expenditure rates are being reviewed and will be accelerated.


DLP: Approved for public release; distribution is unlimited.
**Risk and Uncertainty**

*Risk*, as commonly used in the S&T community, is more accurately *uncertainty*.

Risk is the appropriate term when two conditions are met:

1. The probability of an event occurring can be accurately estimated or is known, usually based upon a large data set concerning similar events in the past with a known distribution of outcomes and the assumption is made that the future mirrors the past.

2. A large number of similar events are part of the future candidate universe and the risk concern is with the events in aggregate, not with a particular event.

**With a few exceptions, neither condition is met in S&T**

Therefore, the risk tools so widely used in fields like insurance, banking, investment and even life cycle maintenance must be applied carefully, modified or abandoned in favor of more effective approaches.
Consequences Not Semantics
The Elements of Risk

*Risk*, to a purist in a professional context, has three elements:

- A description of the risk or risk event
- A known or expected probability of occurrence; rarely, if ever known in S&T
- A significant consequence

*Uncertainty* is the state of not knowing whether something is true or false, whether it will or will not happen. In S&T the absence of a probability distribution for the occurrence of an event creates uncertainty rather than risk, at least to a purist. Still, the convention is to call the situation *risk*.

Casual S&T convention is to use *risk* and *uncertainty* interchangeably, the issue is consequences, not semantics.
Risk that the Risk Model Is Wrong

Here's what killed your 401(k)  David X. Li’s Gaussian copula function as first published in 2000. Investors exploited it as a quick—and fatally flawed—way to assess risk. A shorter version appears on this month’s cover of Wired.

Probability
Specifically, this is a joint default probability—the likelihood that any two members of the pool (A and B) will both default. It's what investors are looking for, and the rest of the formula provides the answer.

Survival times
The amount of time between now and when A and B can be expected to default. Li took the idea from a concept in actuarial science that charts what happens to someone's life expectancy when their spouse dies.

Equality
A dangerously precise concept, since it leaves no room for error. Clean equations help both quants and their managers forget that the real world contains a surprising amount of uncertainty, fuzziness, and precariousness.

Copula
This couples (hence the Latinate term copula) the individual probabilities associated with A and B to come up with a single number. Errors here massively increase the risk of the whole equation blowing up.

Distribution functions
The probabilities of how long A and B are likely to survive. Since these are not certainties, they can be dangerous: Small miscalculations may leave you facing much more risk than the formula indicates.

Gamma
The all-powerful correlation parameter, which reduces correlation to a single constant—something that should be highly improbable, if not impossible. This is the magic number that made Li’s copula function irresistible.

Proposed Working Definition of Risk in S&T

**Risk** (in an S&T effort) – An event that can result in a significant negative consequence outside the S&T effort or organization.

It is the prospect of significant external consequences that creates internal risk; and the corollary is that failure may create internal consequences.
Significant is a qualitative term, in this context. It is more clearly defined in the risk assessment and mitigation phase.

The possibility of negative consequences outside the organization changes the focus from traditional technical and programmatic elements.

The S&T world is dynamic. Priorities change, sometimes quickly and dramatically.
Summarizing Risk Elements and Consequences

- **Risk in S&T** is an event in an S&T effort that can result in a significant negative consequence outside the S&T effort or organization.

- Risk is not an inherent measure of significance or importance. S&T efforts may be potentially “disruptive” or “game changing” but not risky until the consequences of failure are understood and valued.

- In S&T, the probabilities that a risk event will occur are unknown; so risk approaches and tools have to be adapted.
Assessing and Managing Risks Under Uncertainty

➢ Straightforward in concept:
  – Identify and define the risks and consequences *to the degree possible*
  – Assess the risks, focusing on consequences
  – Monitor the situation; iterate as appropriate
  – Manage the risk; mitigate if appropriate

➢ Difficult in execution
  – S&T environment evolves, internally and externally
  – Consequences can be difficult to identify, more difficult to anticipate
  – People will not agree
Example: Stakeholder Risk-Consequence Matrix

Modified Failure Modes and Effects Analysis (FMEA) Tool

This tool graphically displays the degree of risk associated with a user designated consequence of failure, C, and probability of failure, P. The tool will also show specific regions of risk severity by color coding a matrix that depicts the functional relation between C and P. The severity region boundaries are user selectable based on the “Risk Avoidance / Risk Tolerance” philosophy associated with a particular program. The user can also provide his/her own C values to allow different degrees of display granularity than what the default 1 to 5 values provide. A light yellow cell in any of the three tables below will accept a user input. Defaults are provided except for C and P. Definitions of several C categories are also given.

### Consequence Matrix

<table>
<thead>
<tr>
<th>Probability of Failure</th>
<th>Very High</th>
<th>High</th>
<th>Moderate</th>
<th>Low</th>
<th>Very Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability of Failure Pi</td>
<td>Very High</td>
<td>High</td>
<td>Moderate</td>
<td>Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>Very High</td>
<td>System inoperable, usually destroyed. Project fails and must be cancelled.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>System inoperable but moderate to severe damage, but not destroyed. Project may continue but with significant cost overruns, schedule slip, and/or compromised results.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td>System operable but may be unsafe, with damage and major performance degradation. Project has significant cost overruns and/or schedule slip, and compromised results.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>System operable and safe with somewhat degraded performance. Project facing cost overruns, schedule slip, and/or somewhat compromised results.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Very Low</td>
<td>System operable with minor inconvenience(s). Project proceeds with slight overruns or schedule slip, and/or minor compromises to results that do not impact transition.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Probability of Failure

- **Very High**: S&T Program: P ≤ 0.000009 (%); System: P < 0.000009 (%); Production: P < 0.000009
- **High**: S&T Program: P: 0.000009 - 0.0001 (%); System: P < 0.00099 (%); Production: P < 0.00099
- **Moderate**: S&T Program: P: 0.0001 - 0.001 (%); System: P: 0.001 - 0.009 (%); Production: P: 0.009 - 0.099
- **Low**: S&T Program: P: 0.009 - 0.09 (%) ; System: P: 0.09 - 0.9 (%); Production: P: 0.9 - 9%
- **Very Low**: S&T Program: P: 0.9 - 90%; System: P: 0.9 - 90%; Production: P: 0.9 - 90%

### Note

1. The probability of failure guidelines are examples only. They are typical of the way people tend to think about risk in different environments.
2. On the other hand, when nearing transition, technical risk may need to be low. Production risks are based on typical industry quality standards.

### Possible Consequences of Failure in Other Categories

<table>
<thead>
<tr>
<th>Personal Safety</th>
<th>Personal Property</th>
<th>Health</th>
<th>Legal</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Injury resulting in lost work time greater than 30 days</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td>Injury resulting in lost work time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>Minor injury with no lost work time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Very Low</td>
<td>No injury</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Financial Consequence

<table>
<thead>
<tr>
<th>Financial Consequence</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Requires request environmental clean-up after event [Example - $2M to $5M]</td>
</tr>
<tr>
<td>Moderate</td>
<td>Requires moderate clean-up effort to prevent toxic effects on environment, regulate, etc. [Example - Less than $50K]</td>
</tr>
<tr>
<td>Low</td>
<td>No environmental damage fees exist in a relatively short time</td>
</tr>
</tbody>
</table>

### Example: Stakeholder Risk-Consequence Matrix

- ‘Consequences’ are to outside stakeholders, not to the program or project elements.

---

AFRL FMEA Tool (unpublished)
William L. Nolte, AFRL/XPQ

Approved for public release; distribution is unlimited.
Step 1: Define Objective

Step 2: Determine Requirements
- Define Requirements
- Define Tech Challenges
- Define S&T Exit Criteria (KPP sets)
- Validate with customer

Step 3: ID Success Components (Alternatives)
- ID what must happen to successfully meet requirements

Step 4: Probabilistic Risk Assessment
- Estimate from history, or calculate the probability distribution using standard techniques

Step 5: Risk Mitigation Plan
- Define the risk areas to be mitigated
- Prepare for intended action course

Do:
- Define Problem at the appropriate level, may be project or may be system level

Document:
- Problem Definition
- Prioritized Requirement Set
  - Performance
  - Affordability
  - Producibility
  - Reliability
  - Supportability
- S&T Exit Criteria
- Alternative Definitions
- Risk probability distributions and methods of developing
- Results of assessment
- Risk mitigation plan
1. Define the desirement(s) *(What do you want?)*
2. Identify alternative(s), the technologies with potential to satisfy the desirements
3. Score the alternative(s): the best estimate of how well an alternative will meet the desirement
4. Estimate a probability distribution
5. Perform a sensitivity analysis
6. Focus on highly leveraged *(most sensitive)* issues
7. Generate a probabilistic risk profile
   - Monitor and change as more information is available
No “requirements” in the acquisition sense; desirements that may evolve in pre-acquisition.

Desirements are the starting point for identifying risks:

- What is the S&T output intended to accomplish?
- Why is it better than the alternatives, including nothing?
- When will it be available; when needed?
- How will it do that and in what context (part of a system)? Is anything else needed?
- Who will make it happen and who will want it?
- How much to develop and how much will it cost as delivered?

Every S&T risk is associated with an S&T desirement. If there is no desirement, there is no risk. Risk requires an external consequence. S&T risk has a desirement and a consequence for failing to achieve that desirement.
Desirement - Example

Desirement:
Nominal Power (kW)

Customer: 1. Island Winery
Desirement Number: P01
Priority: High
Desirement Type: Perf
How Measured: kW
Objective: 5500
Lower d-Limit: 3000
Upper d-Limit: More
Objective Type: More

Curve Style: S-type
Dsmt Value where d=0: 3000
Dsmt Value where d=1: 5500
Set Point (Rqmt Value): 4400
Set Point (desirability value): 0.8

Desirability Test Point: 4250
Desirability: 0.6705

Desirement Description: Continuous power which the system is capable of providing in kW.
Objective Rationale:
Rationale for d-Limit:
Assumption, How Tested or Other Clarification:
Comments:
Worksheet - Example

Worksheet:
- System: 1 New SETFST Project
- Dsmt Type: Cost
- Customer: 1. Island Winery
- Technology: MicroTurbine w/ Conventional Generator

<table>
<thead>
<tr>
<th>Desirement</th>
<th>Priority</th>
<th>How Measured</th>
<th>Objective</th>
<th>Lower</th>
<th>Upper</th>
<th>Est m</th>
<th>Est s</th>
<th>Risk (PF)</th>
<th>Weight</th>
<th>d</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1 Acquisition or First Cost</td>
<td>Med</td>
<td>$</td>
<td>1000000</td>
<td>1000000</td>
<td></td>
<td>600000</td>
<td>1</td>
<td>0.0000</td>
<td>1</td>
<td>1.00</td>
<td>similar to current diesel</td>
</tr>
<tr>
<td>C2 Installation Cost</td>
<td>Med</td>
<td>Scale: 1 to 5, 5 is highest 2=current</td>
<td>1</td>
<td>3</td>
<td>2.5</td>
<td>1.0</td>
<td>0.3085</td>
<td>1</td>
<td>0.058</td>
<td></td>
<td>heavier than conventional with additional efficiency</td>
</tr>
<tr>
<td>C3 Operating Cost at Point of Use</td>
<td>Med</td>
<td>$/kW-hr</td>
<td>5</td>
<td>15</td>
<td>6.0</td>
<td>1.0</td>
<td>0.0000</td>
<td>1</td>
<td>0.967</td>
<td></td>
<td>2X as efficient overall</td>
</tr>
</tbody>
</table>

Aggregate:
- 0.3085

P01 Nominal Power
- High kW
  - 5500
  - 3000
  - 5,500.0
  - 1.0
  - 0.0000
  - 5
  - 1.000

P02 Surge Capacity: Spike
- High % of Nominal
  - 200
  - 110
  - 120.0
  - 1.0
  - 0.0000
  - 1
  - 0.111

P03 Surge Capacity: Continuous
- High % of Nominal
  - 110
  - 100
  - 110.0
  - 1.0
  - 0.0000
  - 1
  - 1.000

P04 Reliability
- High MTBF
  - 10000
  - 2000
  - 6,000.0
  - 1.0
  - 0.0000
  - 3
  - 0.270

P07 Footprint
- High Sq ft
  - 6000
  - 150000
  - 50,000.0
  - 1.0
  - 0.0000
  - 2
  - 0.451

P09 Set-up Time
- Med Hours
  - 24
  - 72
  - 60.0
  - 1.0
  - 0.0000
  - 4
  - 0.250

Aggregate:
- 0.0000

Approved for public release; distribution is unlimited.
Risk identification and evaluation is part of the analysis of alternatives in the S&T Streamlined Systems Engineering approach:

- Expert judgment from in-house resources
- Expert judgment from professional risk assessors
- Simple stratification or ranking
- Scoring, including weighted scoring; multiple methods
- Multi-attribute assessments that deal simultaneously with multiple factors
- Probabilistic modeling and simulation, gaming simulation
  - Modeling and simulation are powerful, but can be expensive; costs are coming down and the environment is more comprehensive
  - Models can be wrong or misunderstood.
  - What happens to one individual or event has a small probability of reflecting the actual highest probability (often the mean) expected outcome and, in fact, no actual “highest probability” event may ever occur.
Risk Chart from SEADS Toolkit
Composite Score Sheet Example

Non-dimensional composite number characterizes the alternative’s expectation of meeting all requirements. The higher the better.

Non-dimensional composite number characterizes the alternative’s risk with respect to all alternatives. The lower the better.
Radar Charts

- Tri-Generation - Recovery
- Solar - Thermal Concentrator, Steam Generator
- Solar - Photovoltaics with Bulk Storage
- Conventional Generator with on-site Bio-diesel
- Micro Turbine with Conventional Generator
- Wind Turbine with Bulk Storage
Risk Analysis - Executive Level

- **Desirements** are strategic; therefore the risks are strategic
- Process is the same in principle, more qualitative in execution
- Evaluation relies heavily on judgment of response to strategic desirements

<table>
<thead>
<tr>
<th></th>
<th>Meets one or more strategic objectives</th>
<th>There is a clearly defined, actively engaged customer or sponsor</th>
<th>Customer desirements are explicit and understood</th>
<th>Success is clearly defined, such as an agreed upon ATD and timing</th>
<th>Is a unique AF skill, urgent requirement or AF unique requirement</th>
<th>Represents the best approach among alternatives</th>
<th>Is a critical technology or enabling technology</th>
<th>Composite Score</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WEIGHT</strong></td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td><strong>PRODUCTS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S&amp;T Program 1</td>
<td>5</td>
<td>2</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>289</td>
</tr>
<tr>
<td>S&amp;T Program 2</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>160</td>
</tr>
<tr>
<td>S&amp;T Program 3</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>147</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S&amp;T Program n</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Case Number: 88ABW-2011-5437. Distribution A: Approved for public release; distribution is unlimited.
Risk Issues in S&T
High Risk Is Necessary For High Rewards

➢ The history of technology is a history of evolution, not revolution

➢ Evidence is anecdotal: “the plural of anecdote is not data”

➢ Not accurate in the investment community where the theory originates

➢ Requires specificity for analysis
Risk Issues in S&T
S&T Is Risk Averse

- Evidence? Is this accurate?
- Risk aversion is a function of risk/value perception
- Risk in S&T is inherently associated with objectives
Risk In S&T — Summary

- Risk in S&T exists at two basic levels: the technical level and the executive (strategic) level.
- Risk is both the probability that something bad will occur and that if it does, it will have significant consequences outside the organization.
- In S&T the probabilities are rarely known and the consequences of an undesirable event may be insignificant or difficult to recognize.
- Risk should be embraced in S&T by striving for significance to the outside.
- Successfully dealing with risk in S&T requires constant monitoring and a responsive approach using a structured process with evolving tools.
- The more significance, the more risk inherent in an S&T project, the more likely it will be managed successfully.
Contact Information

Thomas Archer
SynGenics Corporation
5190 Olentangy River Road
Delaware OH 43015
Email: archer@syngenics.com
Direct phone: 614-442-7858