



Evolution of Cost Threat Handling within the Cx Program Office Support Tool

January 15th, 2008
Steve Wilson
Darren Elliot
Kelley Cyr
James Johnson

CONSTELLATION



Outline



- I. Introduction to CxPOST and Constellation Cost/Risk Analysis**
- II. Evolution of Cost Threat Handling in CxPOST**
- III. Fun yet Interesting Topic ~ *Time Permitting***
 - I. Threat placement within the model and its effect on the Total Program S-Curve



CxPOST and Constellation Cost/Risk Analysis



Summary of CxPOST



◆ Constellation (Cx) Program Office Tool

- Master cost model
- Output-based approach
 - Modeled in the ACEIT software suite
 - Integration of risk-adjusted cost estimates (outputs) submitted by each project (e.g. Orion, Ares)
 - *Projects may not have considered all factors that contribute to overall cost uncertainty*
- Costs are bucketed into Cx Phases
 - Initial Operating Capability
 - ISS Operations
 - Human Lunar Return
 - Lunar Operations
- Correlation
 - Among cost elements within a project
 - Among projects and threat parent

Cx Cost Risk Analysis

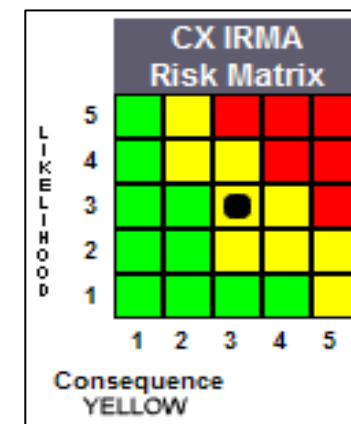
- ◆ **Cost risk analysis typically captures ~**
 - Effort associated with activities
 - Labor rate changes
 - Weight growth
 - SLOC growth

- ◆ **Cost risk analysis typically does NOT capture ~**
 - Major requirement changes
 - Major design changes (e.g., engine change)
 - Major test failures
 - Changes in development/production plans (e.g., adding additional test cycles, additional spares, etc)
 - Funding impacts to planned activities that cause delays

Comprehensive cost risk analysis would attempt to capture many of these items as 'cost threats'.

◆ IRMA

- Integrated Risk Management Application
- Key repository of Cx cost threats
 - ‘Threats’ = Risk items that the current budget provided to each project cannot cover
 - Determined by projects and program
 - Cost threats are potential liens against program reserves
- Threat characteristics
 - Threat likelihood
 - Cost consequence by year if threat is realized





Incorporation of Cost Threats into CxPOST



- ◆ **For the PMR 07 Cx Confidence Level Estimate**
 - Projects varied in risk assessment style
 - Broad approach
 - Considers contingencies within and without the current work scope paradigm
 - At least some threats included
 - Parametric models based on historical program data
 - “Steady-as-she-goes” approach
 - Considers contingencies within the current work scope paradigm
 - Major plan changes not considered
 - Most threats identified in IRMA not included in risk distributions
 - Project s-curves normalized for risk content
 - Cx program risk analysis appended to include threats not captured by project distributions

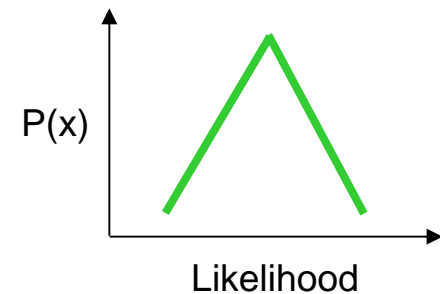
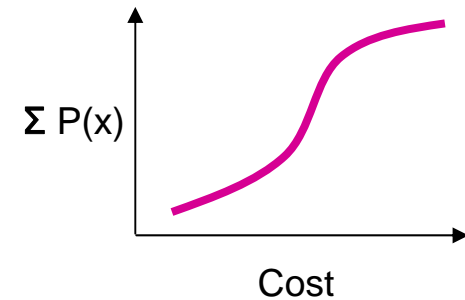
- ◆ **All projects must have same scope of risk content, including both**
 - Technical risk assessments performed by cost estimators
 - Discrete threats identified by project personnel who are not necessarily cost estimators
 - What if the projects risk assessments included discrete threats?
- ◆ **Projects were thus approached to determined which...**
 - Threats were covered by project risk analysis
 - Threats were not addressed by project risk analysis

Evolution of Cost Threat Handling in CxPOST

◆ **Threats not addressed were incorporated into a probabilistic risk model**

◆ **Threat Characteristics**

- Distributions placed on cost threat parameters
 - Cost impacts ~ Convolved distribution
 - High/Low provided by IRMA
 - Likelihood of occurrence ~ Triangular Distribution
 - Level 1 (66% = low, 84% = most likely, 100% = high)
 - Level 2 (33%, 50%, 66%)
 - Level 3 (0%, 17%, 33%)
- Phasing
 - Threats bucketed into the four program phases
 - Initial Operating Capability
 - ISS Operations
 - Human Lunar Return
 - Lunar Operations
 - Cross-phase threats split between the phases based on time period



◆ Method

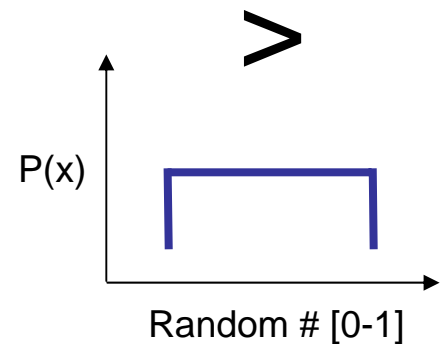
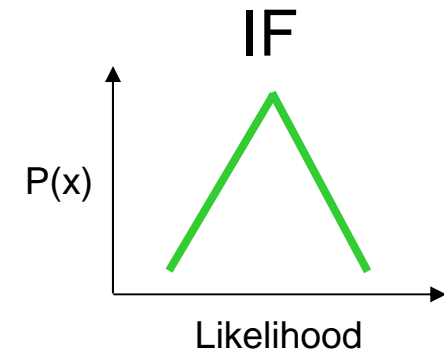
- A random number from 0 to 1 is compared to a sampling from the threats' likelihood distribution.
- If the sampled likelihood $>$ the random number, the cost distribution is sampled...
-else, a zero cost is returned.

◆ Pro

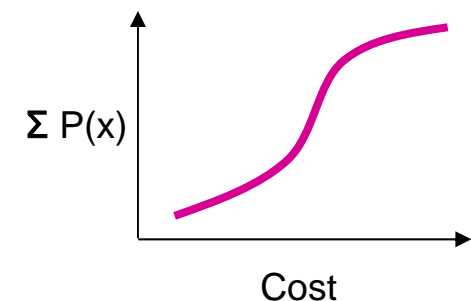
- Full correlation customization between threats'
 - Cost distributions
 - Random # distributions
 - Likelihood distributions

◆ Con

- Long risk run time due to the requisite sampling of three separate distributions.



THEN



1.5th Generation of Threat Handling

◆ Method

- The random # distribution is subtracted from a threat's likelihood distribution.
- The resultant distributions [there are only 3] are converted to custom CDFs and reapplied to the session's threats.
- If the combined distribution > 0 , the cost distribution is sampled...
-else, a zero cost is returned.

◆ Pro

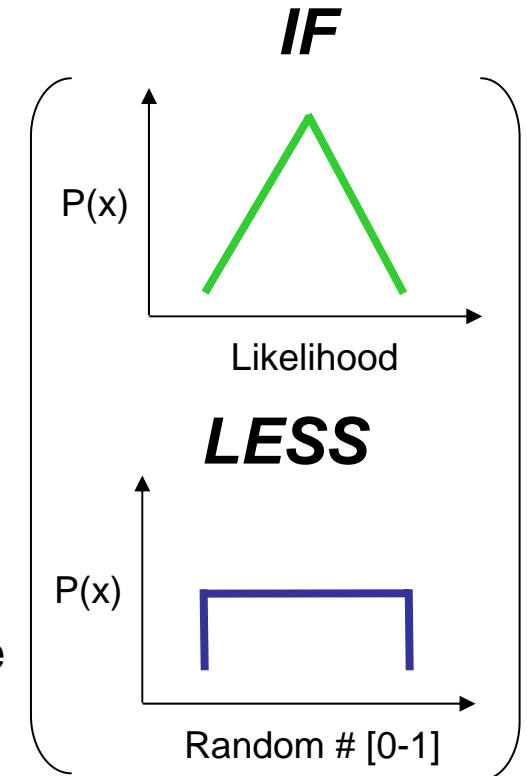
- Faster risk run than first generation method because only two distributions are sampled.

◆ Con

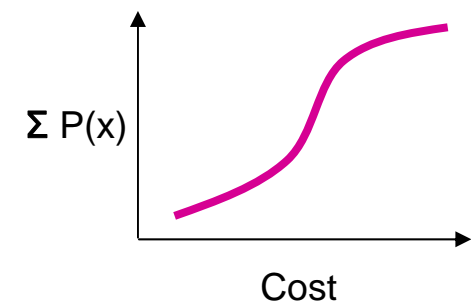
- No correlation customization possible among threats' likelihoods and among random distributions.

◆ ...Con Caveat

- ...but could correlate combined distributions.



> 0 , THEN



◆ Method

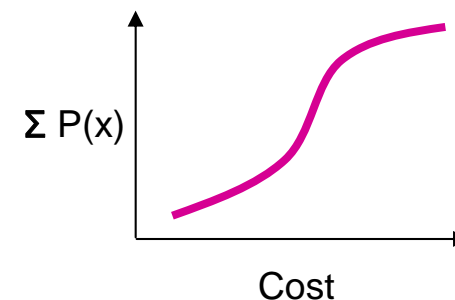
- 7.1's "Probability of Occurrence" column replaces combined distribution, w/ the likelihood distribution remaining as a parameter.

◆ Pros

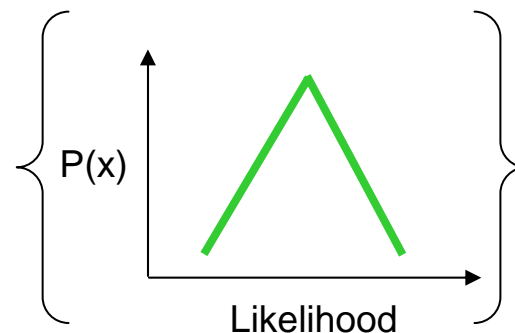
- Requires only one model section ~ easier updates to model.
- Shorter risk run time (induces a 20% run time reduction vs the First Generation method).

◆ Cons

- No correlation possible among internal random # distributions.
- Still samples more than one distribution.



~W/ 'Probability of Occurrence' column parameter:



Alternative to Second Generation

◆ Method

- The random # distribution is subtracted from a threat's likelihood distribution...
- ...and then convolved with the cost distribution.
- The resultant distributions are converted to custom CDFs and then reapplied to the session's threats.

◆ Pros

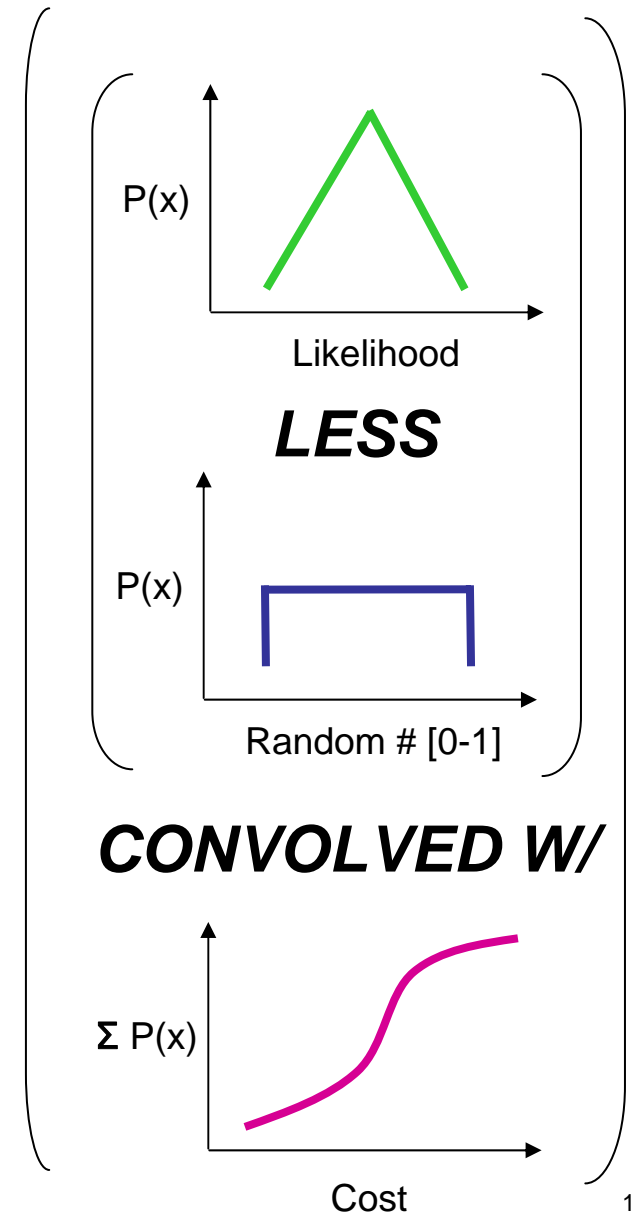
- Requires only one model section.
- Samples only one distribution, thus the shortest risk run time of the options.

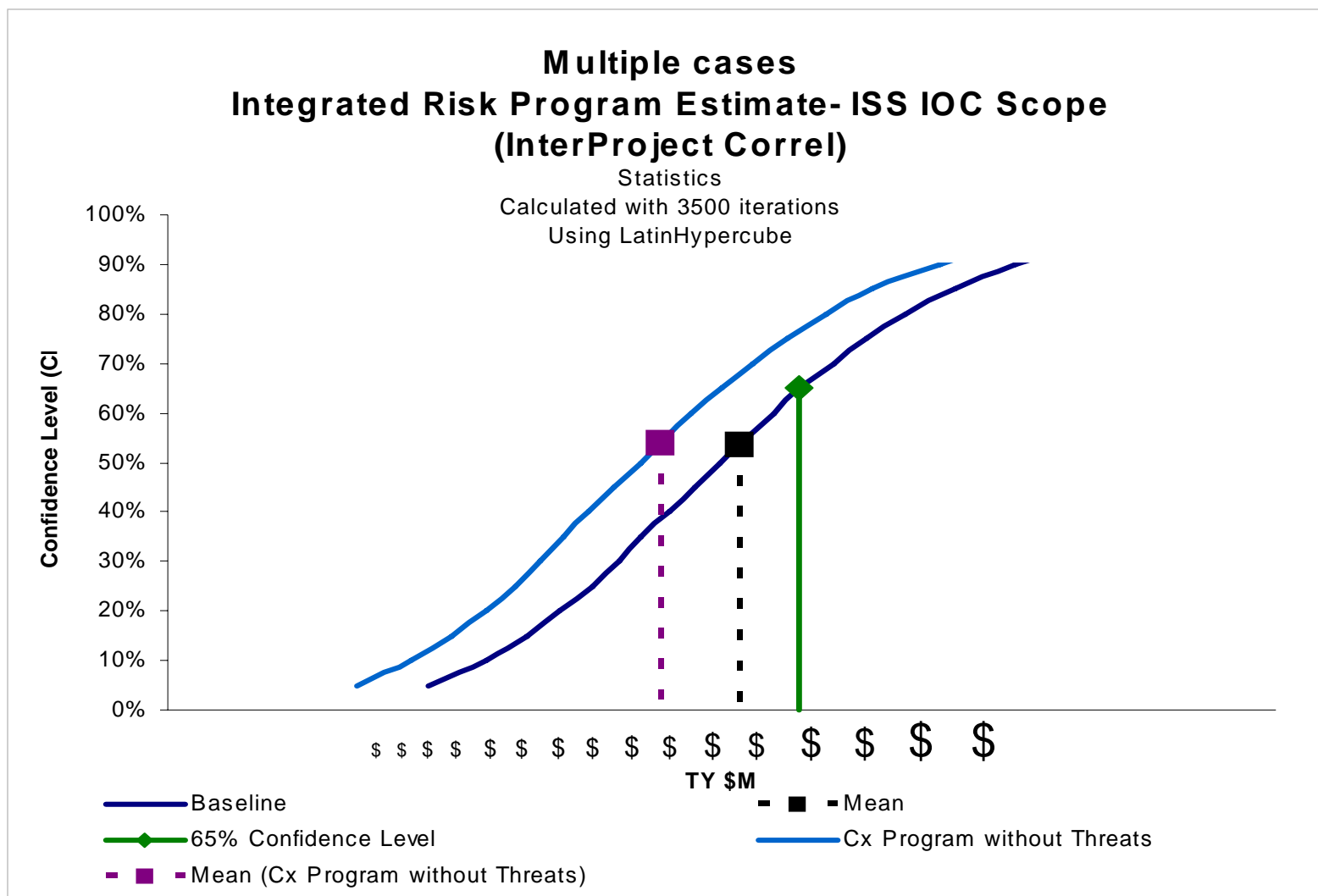
◆ Cons

- Only top level correlation can be specified.
- Must recalculate the threat library at every threat update...

◆ Con Caveats

- ...however, threat updates only occur every 6 weeks.
- Correlation logic still may be defensible even if only applied at top level.

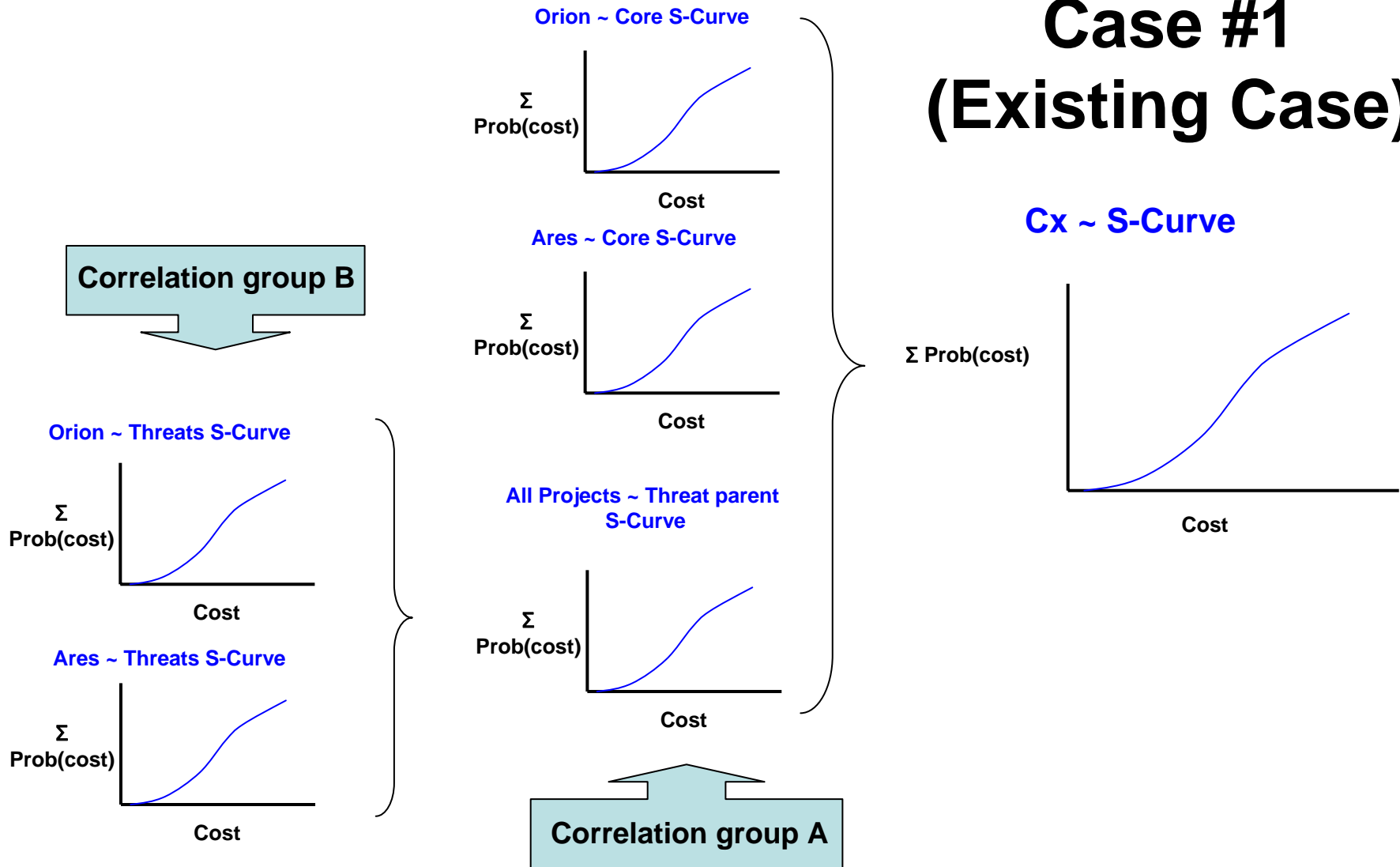




Including threats in risk analysis shifts the program s-curve.

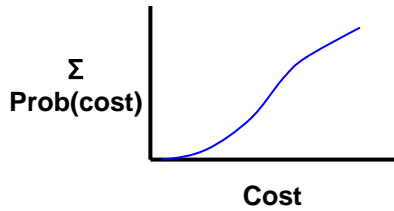
Threat placement and the effects on Total Program S-Curve

Case #1 (Existing Case)

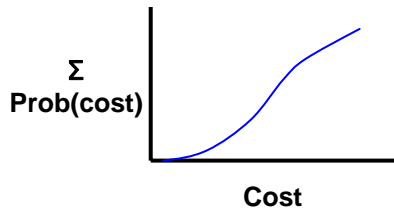


Alternative Threat Placement

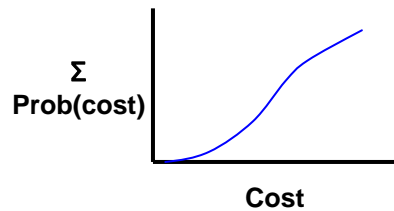
Orion ~ Core S-Curve



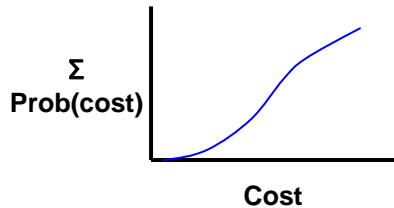
Orion ~ Threats S-Curve



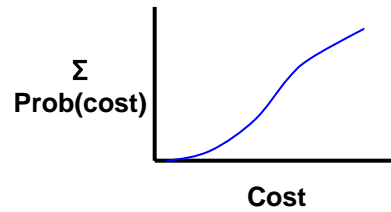
Ares ~ Core S-Curve



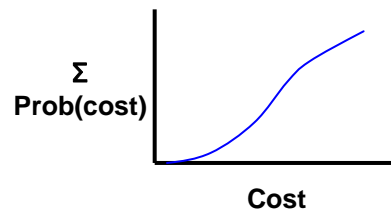
Ares ~ Threats S-Curve



Orion ~ Total S-Curve

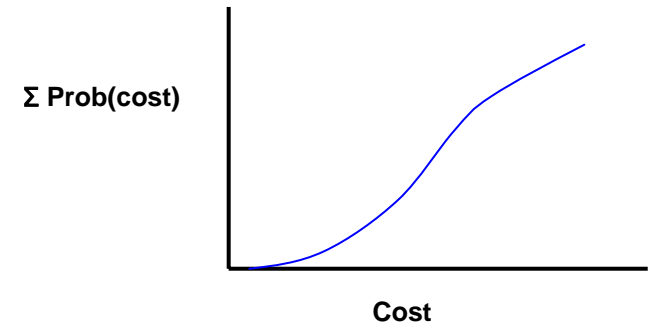


Ares ~ Total S-Curve



Case #2

Cx ~ S-Curve



Do these program CDFs differ?

◆ **No, given that...**

- Correlation among project cores does not vary between cases
- Correlation among threats does not vary between cases
- No additional correlation is assigned at the total project level for Case #2
- There is no strict correlation assigned to the threat parent in Case #1.

◆ **Given these assumptions, it does not matter where threats are placed; however...**

◆ Correlation

- Is it better to structure the model like Case #2 and assign correlation at the total project level?
 - Should total project estimates rather than core project estimates correlate with one another?
 - Case #1's results provide insight to Cx management through threat transparency...
 - ...but Case #2 assigns intuitive correlation among total project costs.
- If there is little or no historical data to specify the magnitudes of correlation...
 - Among threats
 - Among core projects and a threat parent
 - Note: Current model assigns the same correlation factor among these elements
- ...What is the best philosophy for assigning (or not assigning) a value to them?

◆ Risk Distribution deep-dive

- In addition to asking the projects...
 - “What cost threats did you include in your cost risk analysis?”
- ...we will ask:
 - “What technical and schedule threats did you consider when rendering your risk distributions?”



Backup

