SAND2021-13747C

LWRS LIGHT WATER REACTOR SUSTAINABILITY

Risk-Informed Access/Delay Timeline Development

2021 International Topical Meeting on Probabilistic Safety Assessment and Analysis

Douglas M. Osborn, PhD

November 2021

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2021-XXXX-PE

Overview

- Risk informed timeline development is a new direction to aid in development of access delay timelines

- *What does this new approach do?*
  - Gives a broader understanding of delay performance than traditional timeline development methods
  - Includes probability of both attack timeline and probability of attack success

- *What does this new approach give?*
  - Provides methods to include additional data without throwing out any of the previous work
  - Provides statistically defensible methods for combining SME judgement from multiple sources as well as performance test data

Traditional Timeline Development

- Timeline developed from performance data
  - Human performance test results of specific tasks (e.g., running climbing, cutting, etc.)
- Most performance data focuses on the quickest time that a task was completed in during performance testing
- When applicable, SME judgement or data can be used with test data to adjust for challenging environments
- Full timeline built from these minimum task times and reported as the delay timeline
  - Conservative approach to minimize risk
  - Backed by commonly accepted performance test data
  - Method minimizes SME judgement for a given task when feasible

Historical Probability Data for Access/Delay

- For some software tools, probability distributions were desired
- Tools that account for these probabilities range back as far as the late 1970s
- Simplifications were made to ensure computational resources could handle the distribution, as well as to account for limited data
  - Assume fastest performance data was somewhere near the mean
  - Triangle distribution, selected to represent an approximately normal distribution
  - Peak at the reported task time
  - Legs extending +/- 50% of task time in either direction
- Limitations
  - Does not account for non-normal distributions
  - Provided for distribution of task time completions, but did not account for probability of task success
  - Does not address situations where testing was performed by highly capable personnel and was more likely somewhere above average in the distribution

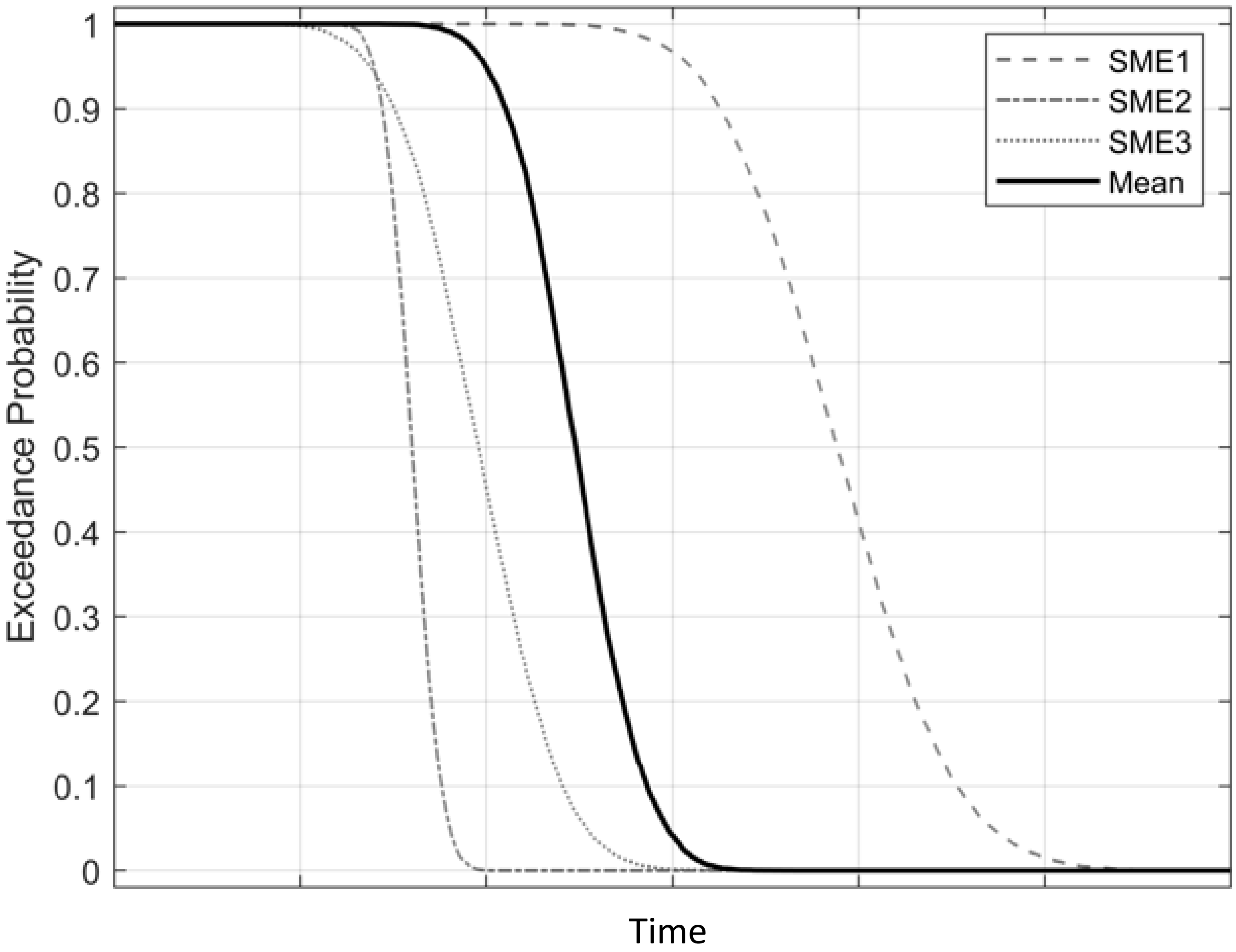
Risk-Informed Timeline Development

- To develop risk informed timelines, begin with an event tree structure to characterize the underlying tasks
- Next utilize SME judgement to populate those tasks
    - Break timeline down into tasks similar to traditional methods
    - Generate a probability distribution for the time of each task
    - Generate a probability distribution for the success rate of each task
        - Complex tasks where a single tool failure will cause the attack to fail will have a lower probability of success than traversing across an open field
- Then use Bayesian analysis to define uncertainty on the branch points in the event tree
- Use Monte Carlo sampling to propagate the uncertainty in each task through the full timeline
- Once model is based on available information, Bayesian updating can be used to incorporate new test data or new SME judgement into the model while maintaining the previous data

Bayesian Updating

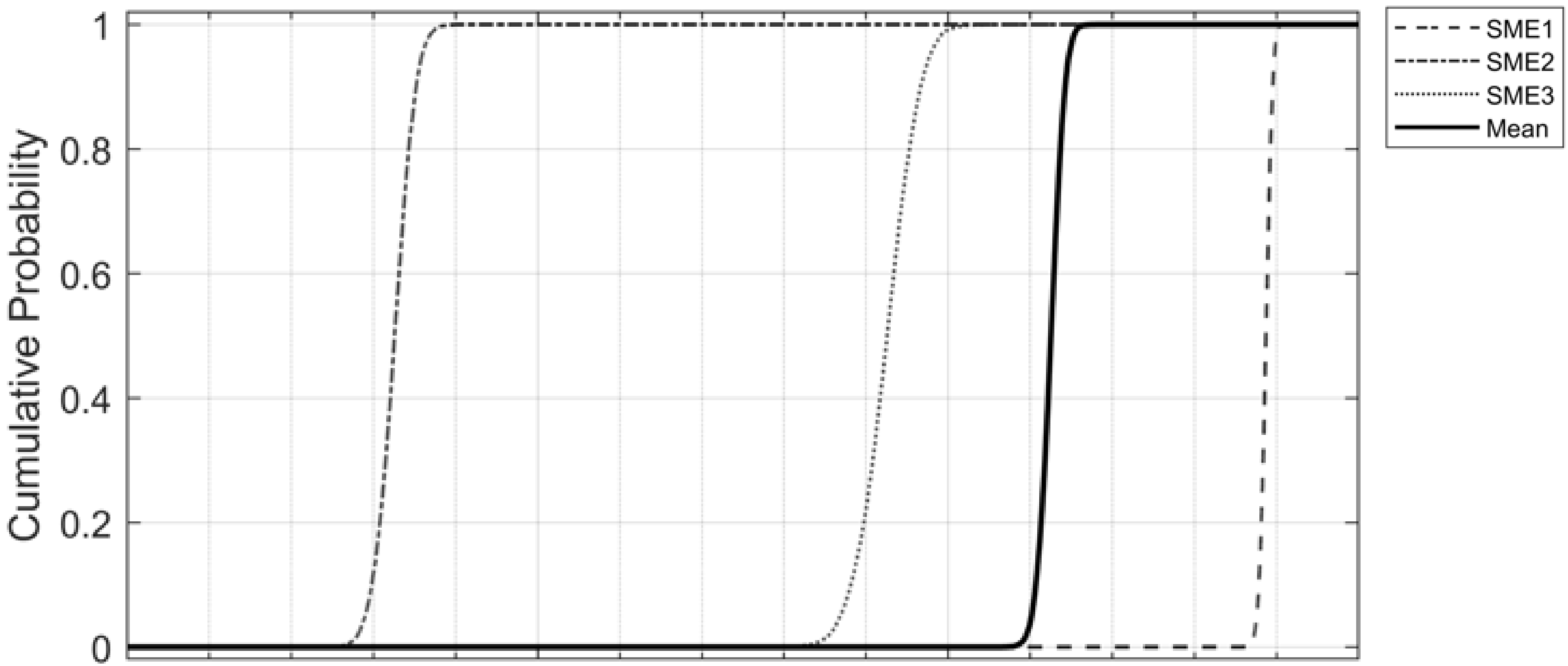
- Bayesian updating is a method to incorporate a prior belief and update it based on additional information that has become available
  - Prior beliefs can be subjective, such as SME judgement, or quantitative, such as previous relevant test data
- Has been widely developed in recent years to support machine learning and artificial intelligence
- While related to machine learning, does not have the same “black box” concerns that other machine learning methods can create
- Bayesian methods can be used with smaller data sets than frequentist methods
  - Due to the costs associated with access/delay tests, this often results in limited data sets

Event Tree Result: Attack Duration



Event Tree Results: Probability of Success

without Bayesian Methods Applied



Probability of Adversary Success

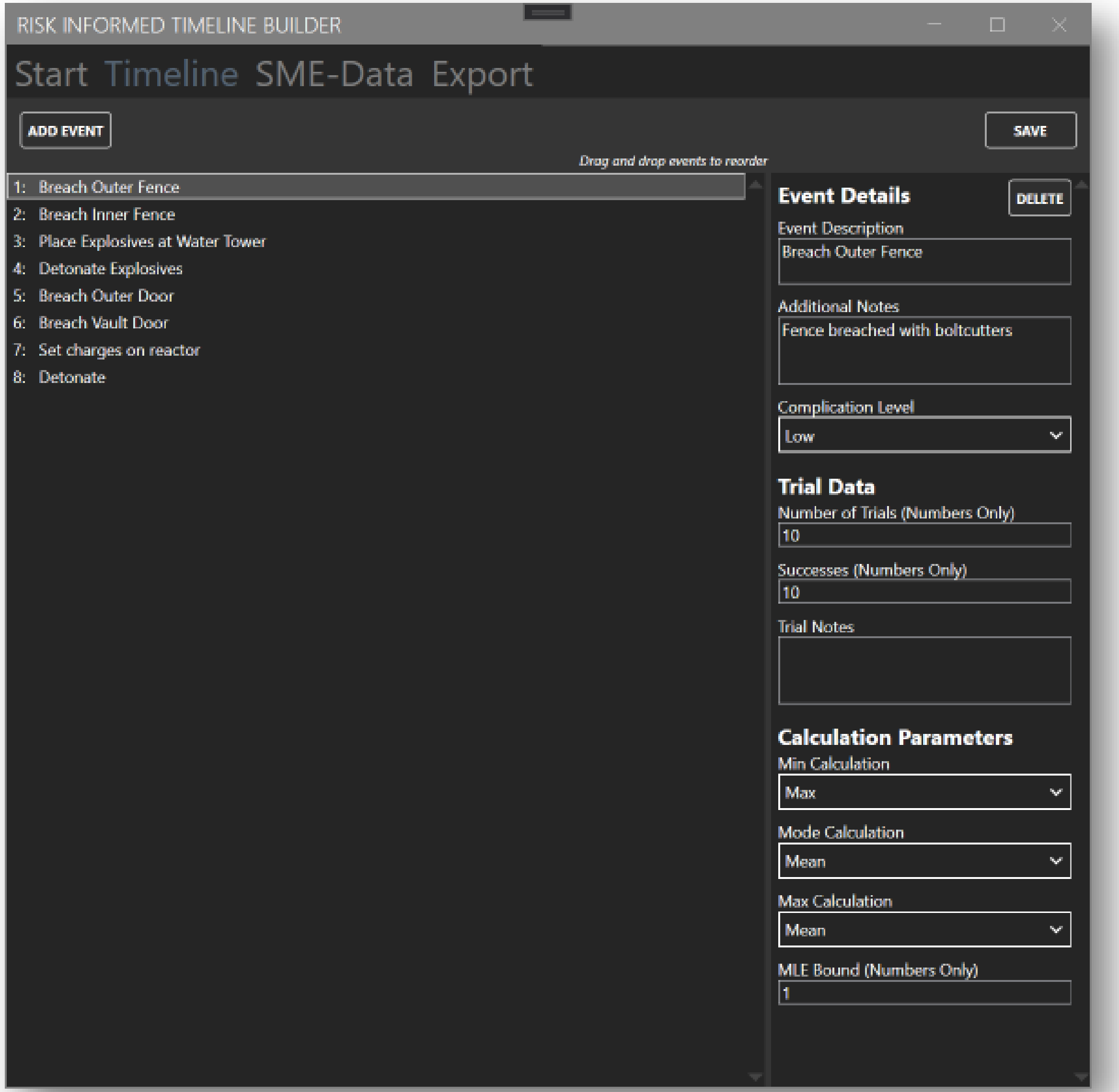
Expected Benefits of Risk-Informed Timelines

- Moving to a risk-informed method allows the focus to move from the attacks that are the fastest, to the attacks that are most likely to succeed
  - Repeat timeline analysis for multiple potential paths
  - Adversaries are going to try to maximize their chance of success, which does not always equate to the shortest timeline
- Provides a broad understanding of which pathways have the most risk associated with them, allowing prioritization of funds for upgrading physical protection systems
  - Focus on the areas where your investment will give the greatest returns on overall system effectiveness
- Provides a method for combining all available data in a statistically sound and consistent way
- Provides more detailed probability distributions for incorporating into modern system evaluation tools
- May allow reconsideration of DBT elements, as with a risk-informed basis it may be feasible to address a wider range of threats, resulting in higher overall system performance

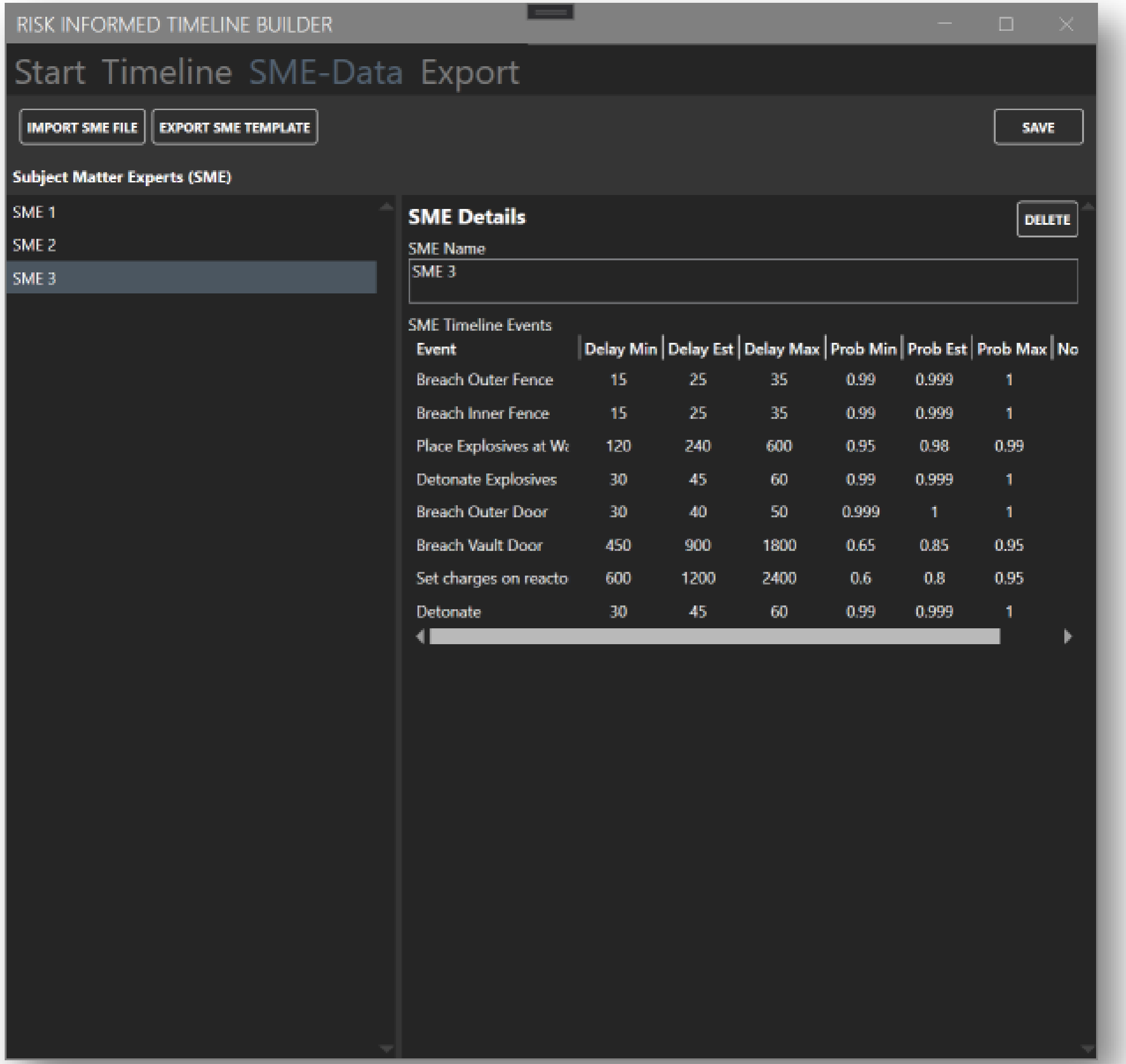
Next Steps to Realize Value

- Before these methods can be adopted, they will require buy-in from all stakeholders
  - Incorporate feedback and discuss the benefits as well as potential drawbacks with stakeholders
    - Utilities, vendors, NRC, and DOE
    - What can and *cannot* be done with these methods and interpretation of results
  - Run demonstration risk-informed timelines to compare the results of these methods with those of timelines developed using existing methods
  - Evaluate the methods to determine how they can be best applied
- Work with stakeholders to determine how these methods can best be implemented
  - Statisticians and PRA SMEs employing these methods with Security SMEs at sites
  - Incorporating these methods into existing system evaluation tools
    - AVERT, Simajin/VANGUARD, SCRIBE3D, DANTE etc.
  - Develop standalone tools for developing risk-informed timelines
- How does this new approach to timelines align with regulators?
  - NUREG/CR-7145
  - NRC Reg Guide 5.81
  - IAEA NSS Guidance
  - DOE Guidance

Risk-Informed Access/Delay Timeline Software



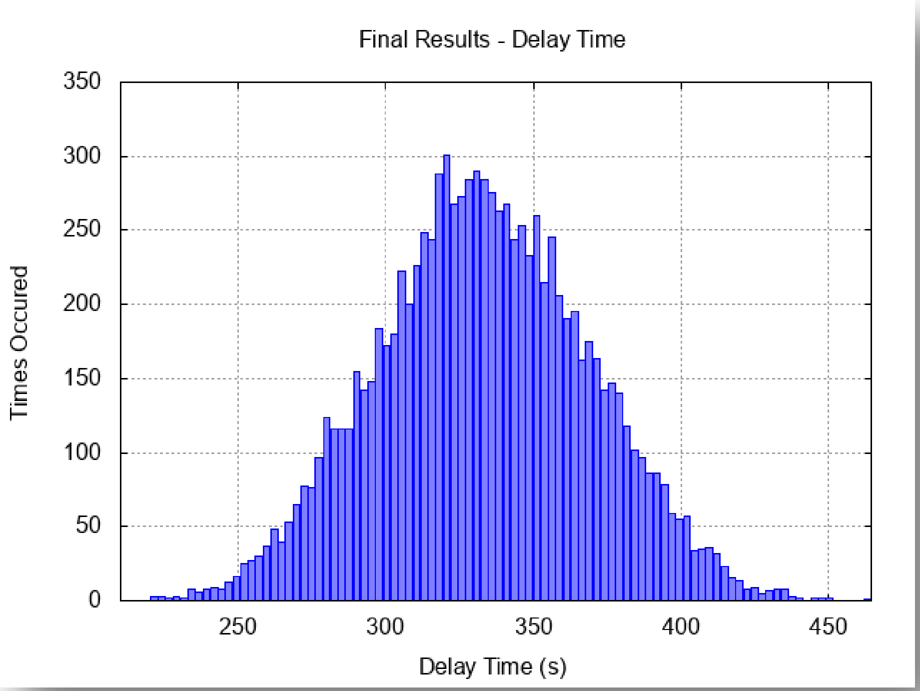
Timeline Builder

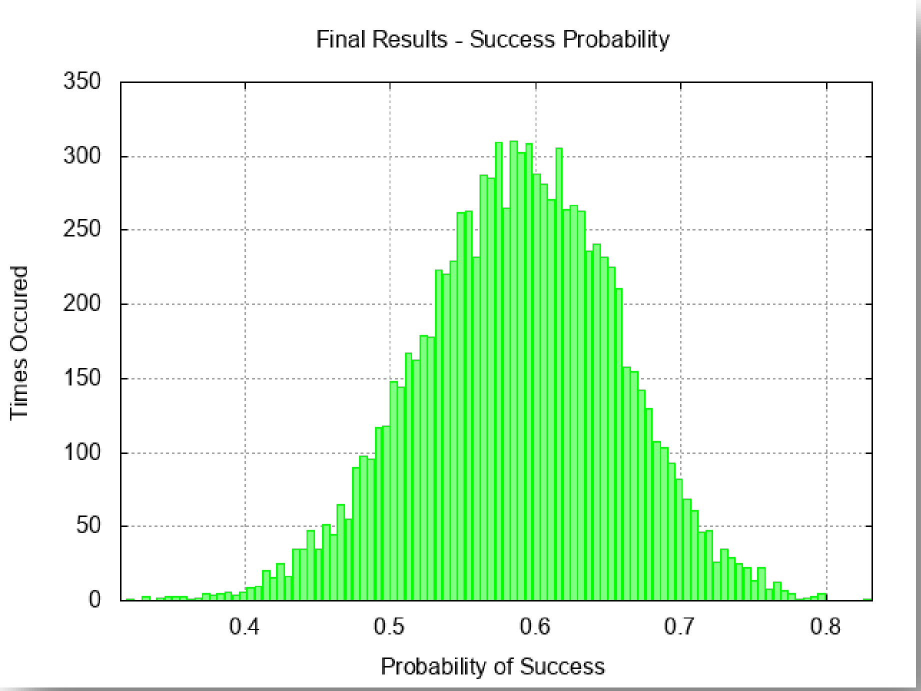


SME Input

Overall Results

	A	B	C
1	Time (s)	Probability	
2	298.585	0.546642	
3	251.671	0.429096	
4	327.336	0.532537	
5	341.203	0.76217	
6	352.259	0.655987	
7	408.011	0.593516	
8	330.626	0.451808	
9	372.394	0.614843	
10	326.721	0.701756	
11	336.48	0.670137	
12	341.26	0.587326	
13	320.311	0.588527	
14	326.912	0.629845	
15	330.104	0.618139	
16	350.633	0.540689	
17	346.788	0.589012	
18	319.815	0.61898	
19	292.944	0.573744	
20	307.191	0.570334	
21	302.816	0.595195	
22	269.57	0.680389	
23	344.824	0.644457	
24	375.926	0.572367	
25	340.257	0.602478	
26	317.822	0.652101	
27	335.177	0.582267	
28	391.545	0.656344	
29	397.929	0.674959	
30	369.67	0.657368	
31	351.494	0.632042	
32	357.28	0.571734	
33	429.95	0.499764	
34	352.96	0.546925	
35	290.187	0.694931	
36	395.997	0.557683	
37	355.105	0.674108	
38	386.576	0.599134	
39	338.836	0.531616	
40	276.129	0.520845	
41	308.327	0.579351	
42	357.401	0.648775	
43	319.298	0.651398	
44	346.115	0.651244	
45	301.762	0.629206	
46	268.387	0.605068	
47	295.121	0.629594	
48	353.936	0.624688	

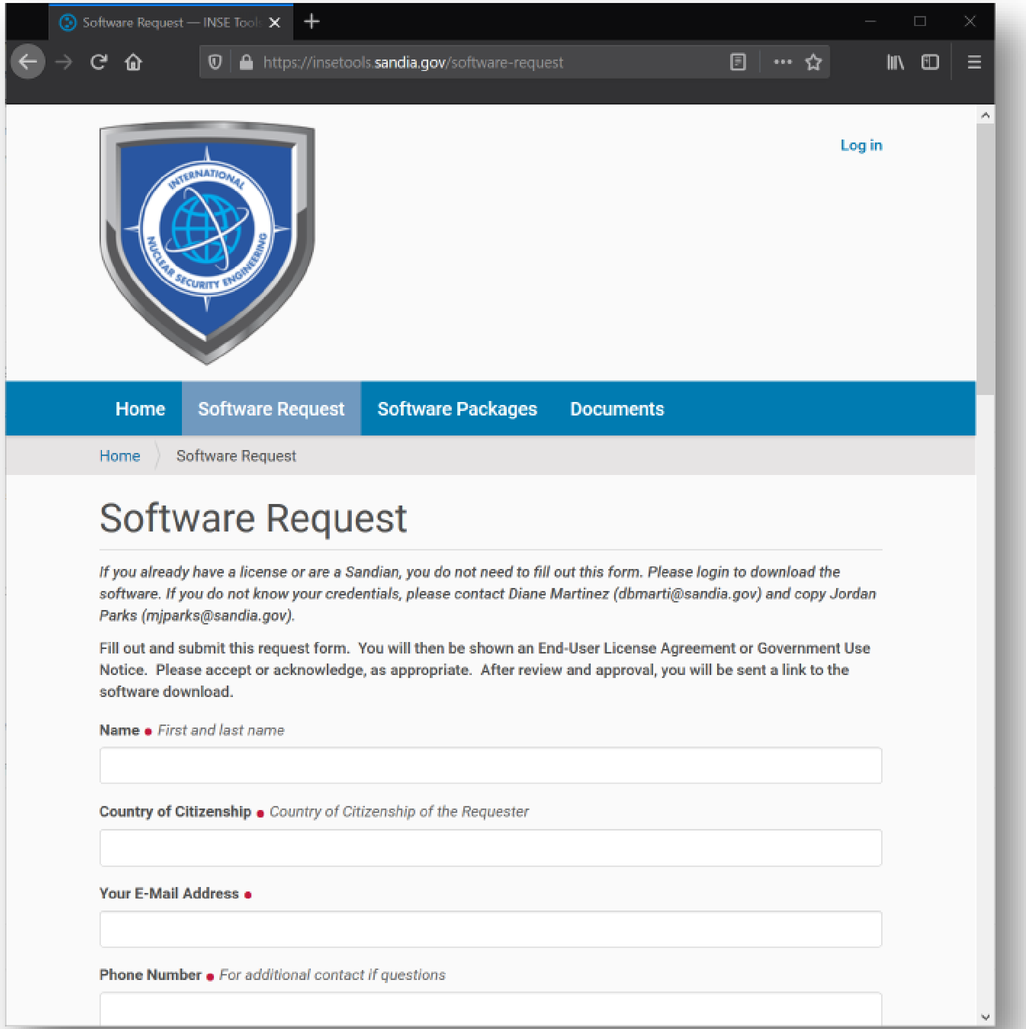




Requesting Software

https://insetools.sandia.gov/software-request

- Fill out form and select “Risk Informed Timelines” in the software section.
- Sandia will then process the request
  - Usually 2-4 weeks
  - After execution of license, a download link will be sent for the software
  - Software will include a comprehensive user guide.



Thanks to Andrew Thompson, Dusty Brooks, and Todd Noel for their efforts in developing this method and software

LWRS

LIGHT WATER
REACTOR
SUSTAINABILITY

Sustaining National Nuclear Assets

http://lwrs.inl.gov