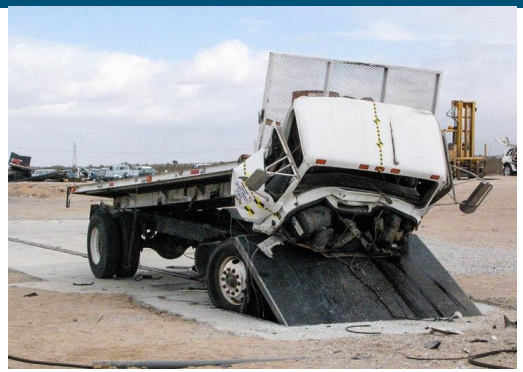
Exceptional service in the national interest

Sandia National Laboratories



Risk Informed Timeline Development

June 29, 2022

SAND2020-6377 PE

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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

Overview

- Risk informed timeline development is a new direction to aid in development of access delay timelines
  - Gives a broader understanding of delay performance than traditional timeline development methods
  - Includes probability of both attack timeline and probability of attack success
  - 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

Sandia National Laboratories

Traditional Timeline Development

- Timeline developed from performance data
- Most performance data focuses on the quickest time that a task was completed in during testing
- When applicable, SME judgement or data can be used to apply complexity factors to the 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

Sandia National Laboratories

Historical Probability Data

- 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
  - Simplified triangular distributions with many assumptions were typically used
- Limitations
  - Does not account for non-normal distributions
  - Provided for distribution of task time completions, but did not account for probability of task success
  - Doesn’t address situations where our 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 based on available information is complete, 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, and due to the costs associate with delay tests we often work with limited data

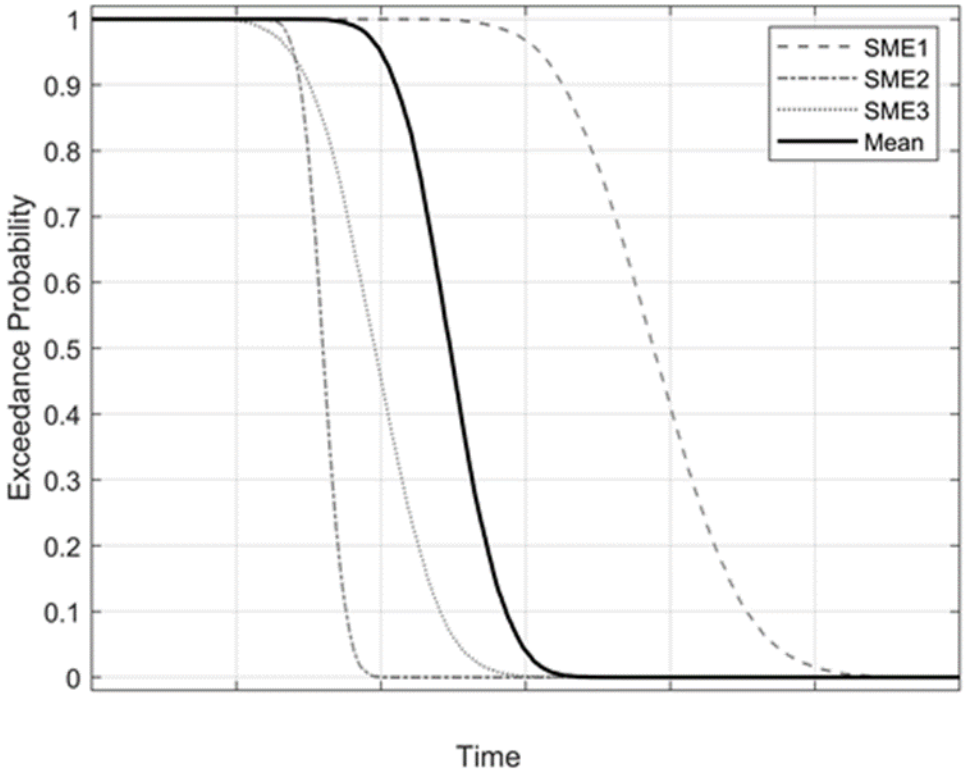
Risk Informed Timeline Example

- An example scenario was analyzed using these methods in order to demonstrate how it could be used
- 2 individual SMEs and one group of SMEs generated timelines for these tasks including estimated probability of success for each task
- Performance testing was completed on several tasks that had high uncertainty
- Data was analyzed using an event tree and Bayesian analysis to combine the SME judgement and the test data in a defensible way

Event Tree Method

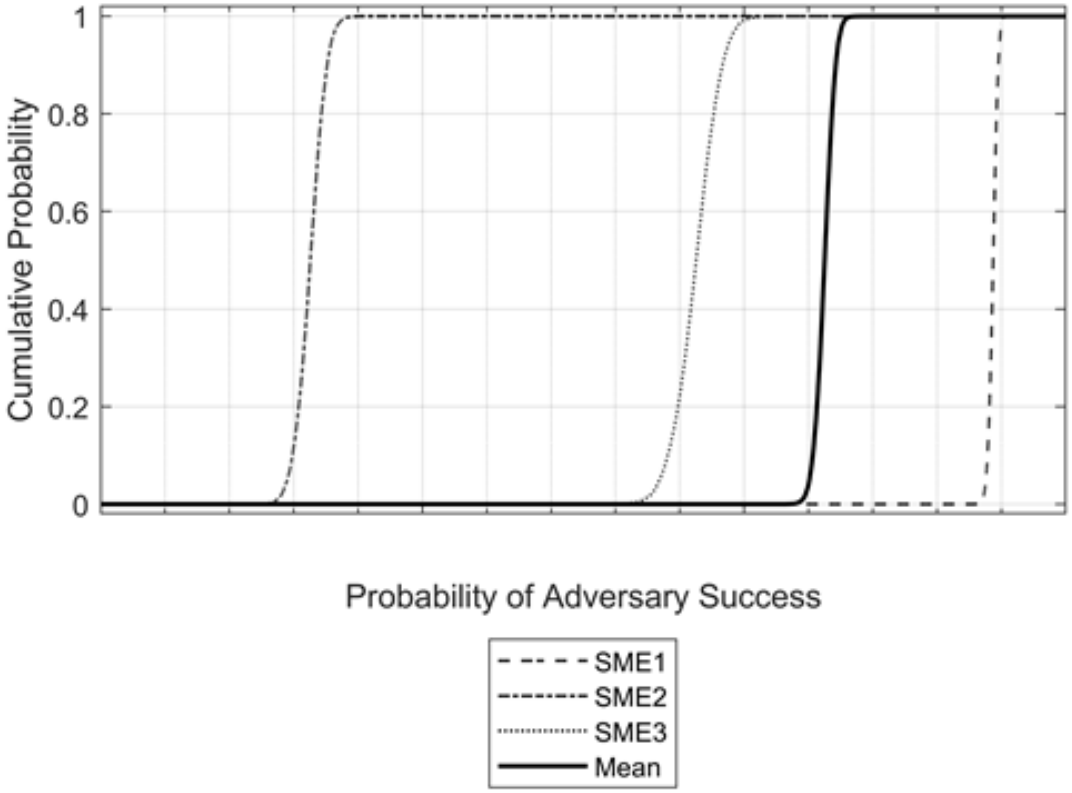
- SME timelines used to generate an event tree
- Timelines were fit with triangular distributions based on min, mean, and max time estimates
  - Allows for the triangular distributions to be skewed, rather than making all distributions symmetric
- Success probabilities were fit with beta distribution approximating the triangular distributions defined by min, mean, and max probability of success values
- For each data set, each individual SME timeline was processed, as well as a set of mean curves in which all SME estimates were averaged
- Current tools exist for doing this type of analysis (ex. SAPPHIRE) and it just requires adjusting the way we generate the timelines to include distributions rather than point data
- There is significant scatter in SME input, resulting in low confidence in the quantitative results
  - Could be resolved by workshopping this with the SMEs involved to discuss their reasoning and update distributions using Bayesian methods
  - Additional test data and/or SME input may also help to increase confidence
  - Even with low confidence, this data may be able to be used to draw useful conclusions

Event Tree Result: Attack Duration



Sandia National Laboratories

Event Tree Results: Probability of Success (without Bayesian Methods Applied)



Sandia National Laboratories

Benefits of Risk Informed Timeline Analysis

- 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 in and out
- Provides a broad understanding of which pathways have the most risk associated with them, allowing prioritization of funds for upgrading physical protection systems
- 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

Sandia National Laboratories

Future Goals for Risk Informed Timeline Development

- Generate a tool that can be used by SMEs to create timelines
  - Standardize methods for timeline development
  - Create GUI that is able to pull performance data from a database to simplify generation of timelines, include probability distributions when feasible
  - Allow SMEs to generate probability distributions for tasks that are not well characterized
  - Generate timeline with automatic references to data source, annotation of tasks that required SME judgement, and probability distribution curves for the time to completion and chance of success for each individual task as well as any combination of tasks
  - Include tools to utilize Bayesian updating if additional information is generated through performance testing or additional SME analysis

Questions?