

Light Water Reactor Sustainability Program

Risk-Informed Adversary Timeline Tool



August 2021

U.S. Department of Energy
Office of Nuclear Energy

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

Risk-Informed Adversary Timeline Tool

Todd Noel, Andrew Thompson, Dusty Brooks, and Douglas M. Osborn

August 2021

**Prepared for the
U.S. Department of Energy
Office of Nuclear Energy**

ABSTRACT

This work has a focus on reducing conservatisms in adversary timelines which potentially lead to over protection of a potential attack path resulting in inefficiencies in areas of a plant's security posture. Applying risk-informed tool to these adversary timelines may reduce some of these conservatisms. This user guide presented in this report is intended to go over the use and execution of the Risk-Informed Timelines tool and Timeline Builder software. This effort utilizes work in Fiscal Year 2020 to demonstrate the effectiveness of these tools.

TABLE OF CONTENTS

1. Introduction.....	8
1.1. Motivation.....	8
1.2. LWRS Physical Security Initiative Purpose and Goals.....	8
1.3. Regulatory Requirements.....	9
1.3.1. Physical Security Requirements.....	9
1.3.2. Additional Security Requirements	10
1.4. Report Structure.....	10
2. Risk-Informed Timeline Tool.....	12
2.1. Description	12
2.2. Tool Use.....	12
2.3. Installation.....	12
2.3.1. Windows.....	12
2.3.2. Linux/OSX.....	12
3. Timeline Builder.....	14
3.1. Start Screen	14
3.2. Timeline Tab.....	15
3.2.1. Event Details Section	16
3.2.2. Trial Data.....	16
3.2.3. Calculation Parameters	16
3.3. Subject Matter Expert (SME) Data Tab.....	16
3.3.1. Export SME Template Button.....	17
3.3.2. Import SME File Button.....	18
3.3.3. SME Details	18
3.4. Run and Export Tab	18
3.4.1. Run.....	19
3.4.2. Export.....	19
4. Results.....	20
4.1. Overall Results	20
4.1.1. FinalResults.csv	20
4.1.2. Final Result Histograms	20
4.2. Event Results.....	21
4.2.1. “event_#_results.csv”	21
5. Running the Risk-Informed Timeline Tool with Arugments.....	22
5.1. Argument Description	22
5.2. Example of Running with Arguments.....	22
5.3. Input Directory	22
5.3.1. Input Directory Description.....	22
5.3.2. Directory format.....	22
5.3.3. Timeline Input File	22
5.3.4. SME Input Files	23
6. Conclusions and Path Forward.....	24

LIST OF FIGURES

Figure 1	Start Screen of the Risk-Informed Timeline Builder Tool.	14
Figure 2	Timeline Screen of the Risk-Informed Timeline Builder Tool.	15
Figure 3	SME Data Screen of the RIT Builder Tool.	17
Figure 4	Execute Screen of the Risk-Informed Timeline Builder Tool.	18
Figure 5	Example of a Delay Histogram Generated by the RIT Tool with 10,000 Runs.	20

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
DBT	Design Basis Threat
DOE	U.S. Department of Energy
DOE-NE	U.S. Department of Energy's Office of Nuclear Energy
LWR	Light Water Reactor
LWRS	Light Water Reactor Sustainability
NPP	Nuclear Power Plant
NRC	U.S. Nuclear Regulatory Commission
PPS	Physical Protection System
RIT	Risk-Informed Timeline
SME	Subject Matter Expert
SNL	Sandia National Laboratories
USG	U.S. Government

This page left blank

1. INTRODUCTION

In fiscal year 2020, the DOE Light Water Reactor Sustainability Program’s Physical Security Pathway explored uses of dynamic risk tools, FLEX equipment, operator action, and Bayesian Methods for application to physical security. Physical security can benefit from risk-informed methods and approaches that are used in nuclear safety and other high consequence industries. This report expands on the fiscal year 2020 work and explores the application of other risk tools for application to physical security applications.

1.1. Motivation

Domestic nuclear power generation faces increasing economic pressures, in part, by post-Fukushima regulatory requirements, an increase in subsidized renewable energy sources, and current low-cost natural gas. The requirements for U.S. nuclear power generation sites, post-9/11, to maintain a large on-site physical security force ranks high for related plant operational costs; ~12% of the overall cost (~\$560 million) for decommissioning a nuclear facility [1]. U.S. nuclear power plants are seeking novel physical security methods and technologies to help deliver on the Nuclear Promise [2].

DOE National Laboratories have extensively studied physical security configurations that couple detect, delay, and response attributes to regulatory required physical security postures. This DOE Office of Nuclear Energy (DOE-NE) Light Water Sustainability (LWRS) Program effort seeks to create tools, methods, and technologies that will:

- Apply aspects of risk-informed techniques for physical security decisions and activities to account for a dynamic adversary;
- Apply advanced modeling and simulation tools to better inform physical security posture;
- Assess benefits from proposed enhancements, novel mitigation strategies, and potential changes to regulations; and
- Enhance the technical basis necessary for operating utilities to reevaluate their physical security posture while meeting regulatory requirements.

1.2. LWRS Physical Security Initiative Purpose and Goals

The primary deliverables for this DOE-NE LWRS initiative are:

- Validated methods which can be used to implement an updated physical security regime and optimize the physical security at domestic nuclear power plants,
- Develop tools that create a robust risk-informed technical basis for physical security decisions,
- Create potential security architectures that incorporate technology to optimize human in-the-loop activities, and

- Implement results of this initiative into National consensus standards.

It is the intent for the LWRS Physical Security Pathway to develop methods, tools, and technologies and generate recommendations that provide the technical basis for an optimized plant security posture. This could consider reducing conservatism in that posture, in order to reduce security costs for the nuclear industry while ensuring adequate physical security.

The LWRS Physical Security Pathway R&D activities will analyze the existing physical security regime (regulations, personnel, technologies, etc.), current best fleet practices, and compare/contrast insights derived from this activity with alternatives and methods that leverage advanced modeling and simulation, modern technologies, and other advanced techniques to enhance approaches for domestic nuclear power plant physical security.

All activities in this Physical Security Initiative will be performed in accordance with the LWRS Program quality assurance (QA) plan. Appropriate QA rigor will be taken for the intended use of the data. Appropriate export control and classification review will be performed to ensure the milestone deliverables are uploaded to DOE's Office of Scientific and Technical Information (OSTI) whenever applicable. Any sensitive information generated by this initiative will be handled in accordance with established DOE requirements.

1.3. Regulatory Requirements

10 CFR 73, "Physical Protection of Plants and Materials," [3] prescribes requirements for the establishment and maintenance of a physical protection system (PPS) that will have capabilities for the protection of special nuclear material (SNM) at fixed sites and in transit and of NPPs in which SNM is used. 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage," [4] requires each nuclear power reactor licensee to implement the requirements of 10 CFR 73.55 through its U.S. Nuclear Regulatory Commission (NRC) approved physical security plan, training and qualification plan, safeguards contingency plan, and cyber security plan referred to collectively hereafter as "security plans."

The requirements of 10 CFR 73.55 are intended to establish and maintain a physical protection program that provides reasonable assurance that activities involving SNM are not contrary to the common defense and security and do not constitute an unreasonable risk to public health and safety. This includes the ability to protect against the design basis threat of radiological sabotage (i.e., significant core damage and spent fuel sabotage). The security plans describe how the 10 CFR 73.55 requirements will be implemented through the establishment and maintenance of a security organization, use of security equipment and technology, training and qualification of security personnel, implementation of predetermined response plans and strategies, and protection of digital computer and communication systems and networks.

1.3.1. Physical Security Requirements

The nuclear power reactor licensee is responsible for maintaining the onsite physical protection program in accordance with NRC regulations through the implementation of security plans and written security implementing procedures. The design of the physical protection program is focused

on a series of target sets that require protection. A critical element of the security plan is the need to demonstrate the ability to meet requirements including the ability of armed and unarmed personnel to perform assigned duties and responsibilities required by the security plans and procedures. That, in turn, leads to development and implementation of a training and qualification program (in accordance with 10 CFR 73.55, Appendix B, Section VI) along with a performance evaluation program (10 CFR 73.55, Appendix B) to ensure the effectiveness of the licensee's armed and unarmed personnel.

1.3.2. Additional Security Requirements

In addition to the physical security requirements, the licensee's security plans include details describing the following related security topics:

- The requirements for the access authorization program as stipulated in 10 CFR 73.56, "Personnel Access Authorization Requirements for Nuclear Power Plants" [5].
- A Safeguards Contingency Plan that describes how the criteria set forth in Appendix C, Section II, "Licensee Safeguards Contingency Plans," of part 73 will be implemented [6].
- A Cyber Security Plan that describes how the criteria set forth in 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," will be implemented [7].

1.4. Report Structure

This report is structured into five main sections; Section 2 provides an overview of the Risk-Informed Timeline software and installation instructions. Section 3 provides an overview of how to use the Risk-Informed Timeline Builder graphical user interface. Section 4 provides a notional example of the results and outputs of the Risk-Informed Timeline tool. Section 5 describes running the Risk-Informed Timeline tool with arguments. Section 6 is the summary conclusions and shows the path forward of using the Risk-Informed Timeline tool beyond LWRS funding.

This page left blank

2. RISK-INFORMED TIMELINE TOOL

2.1. Description

The Risk Informed Timelines tool leverages a new method to modernize how access delay timelines are developed and utilized in physical security system evaluation. This new method utilizes Bayesian methods to combine subject matter expert (SME) judgement and small performance test datasets in a consistent and defensible way. It will also allow a more holistic view of delay performance that provides distributions of task times and task success probabilities to account for tasks that, if failed, would result in failure of the attack. For more information, please refer to the “Risk Informed Access Delay Timeline Development” report [8].

2.2. Tool Use

The Risk Informed Timeline (RIT) Tool is intended to run stand-alone with the results subsequently being used by analysts or in conjunction with Monte Carlo simulation tools.

2.3. Installation

2.3.1. Windows

- Run RIT-Installer.msi and follow instructions
- An icon should appear on your desktop and in your start menu

2.3.2. Linux/OSX

- Install Boost
 - Boost provides free peer-reviewed portable C++ source libraries.
 - Version greater than or equal to 1.76.0
 - <https://www.boost.org/users/download/>
- Install GNUPlot
 - Gnuplot is a portable command-line driven graphing utility for Linux, OS/2, MS Windows, OSX, VMS, and many other platforms
 - <http://www.gnuplot.info/download.html>
- Install NLOpt
 - NLOpt is a free/open-source library for nonlinear optimization, providing a common interface for a number of different free optimization routines available online as well as original implementations of various other algorithms.
 - https://nlopt.readthedocs.io/en/latest/NLOpt_Installation/
- Modify makefile if needed
 - Ensure paths to Boost and NLOpt are correct
- Run makefile
- Run RIT from terminal with arguments

This page left blank

3. TIMELINE BUILDER

The Timeline Builder tool allows users to create timelines and run them through the Risk Informed Timelines algorithm. It contains a simple user interface to set up the timeline, contains tools to allow the import of Subject Matter Export (SME) data, and can run the algorithm.¹

3.1. Start Screen

The Start Screen allows creating a new timeline or loading an existing timeline. Timeline files are saved with the .rit extension.

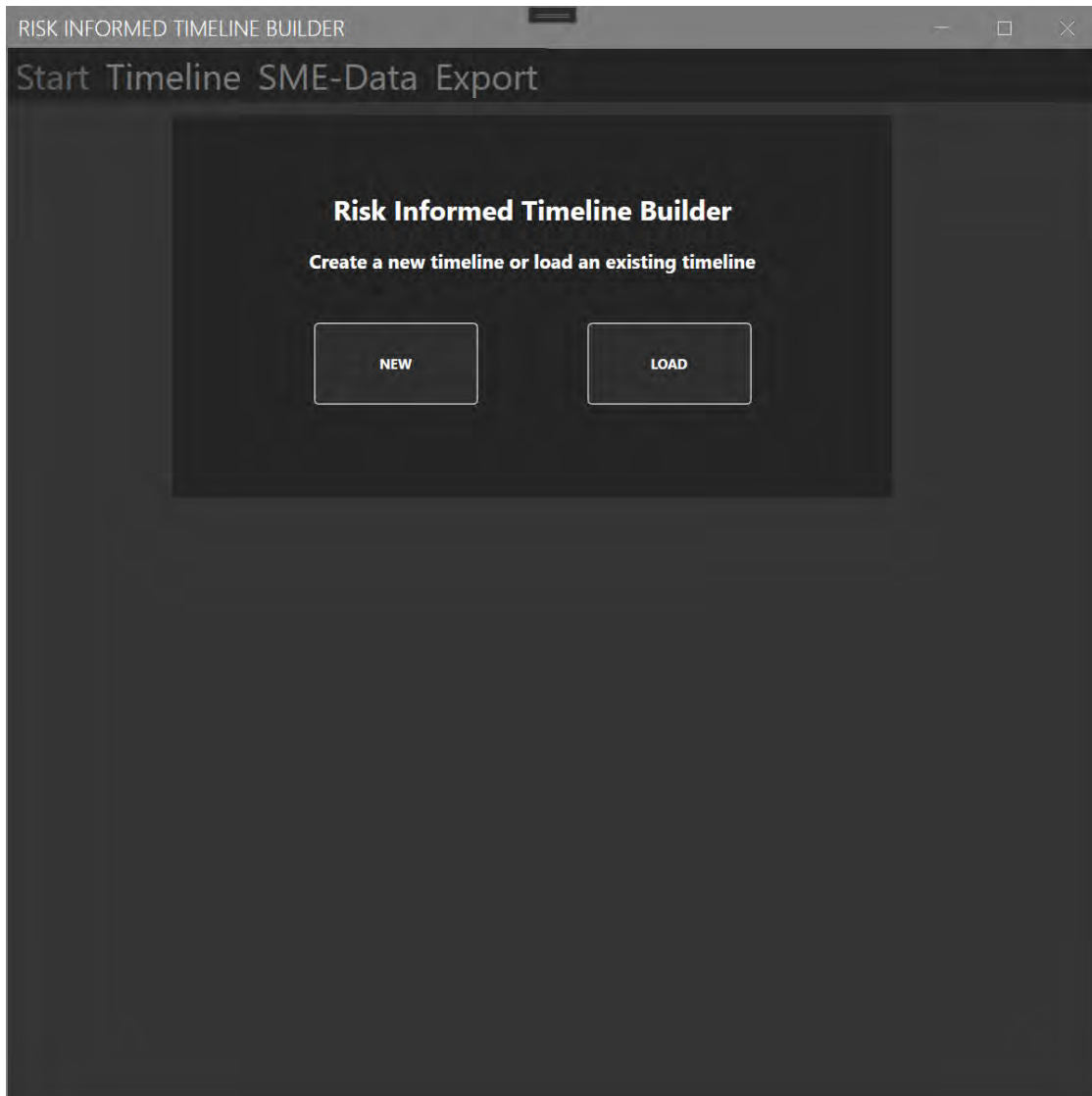


Figure 1 Start Screen of the Risk-Informed Timeline Builder Tool.

¹ The Risk-Informed Timeline (RIT) Builder is a Windows only application. RIT can also be run from a console application. See Section 5.

3.2. Timeline Tab

The timeline screen allows users to add/modify timeline events.

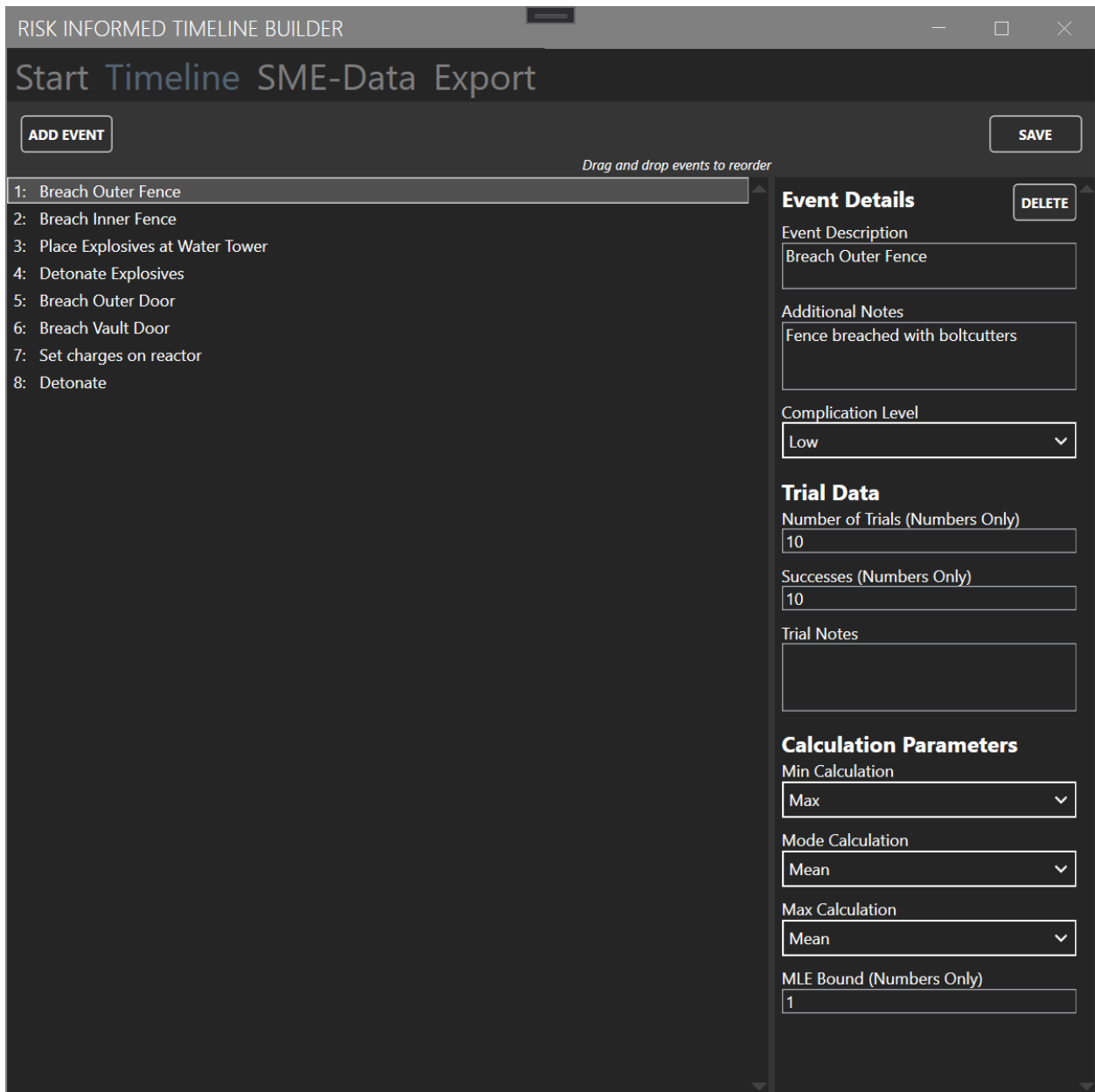


Figure 2 Timeline Screen of the Risk-Informed Timeline Builder Tool.²

² The timeline and data shown are completely notional.

3.2.1. Event Details Section

Event Description: A succinct description of the event

Additional Notes: Details on the event that will be useful for the Subject Matter Expert (SME)

Complication Level: Overall difficulty of completing the event.

3.2.2. Trial Data

Number of Trials: The number of trials conducted

Successes: The number of successful trials. Must be less than or equal to the number of trials.

Trial Notes: Details/Notes on this specific trial

3.2.3. Calculation Parameters

Min/Mode/Max Calculation: The method of merging SME data. For example, if a user selects Max on the Min Calculation section, the RIT tool will take the max value of all SMEs min estimate for that event.

MLE Bound: Upper bound for the Maximum Likelihood Estimation algorithm. This can be modified to ma

3.3. Subject Matter Expert (SME) Data Tab

The SME Data section contains the ability to export a timeline template for SMEs to fill out, the ability to import that template back into the tool, and the ability to view/edit individual SMEs.

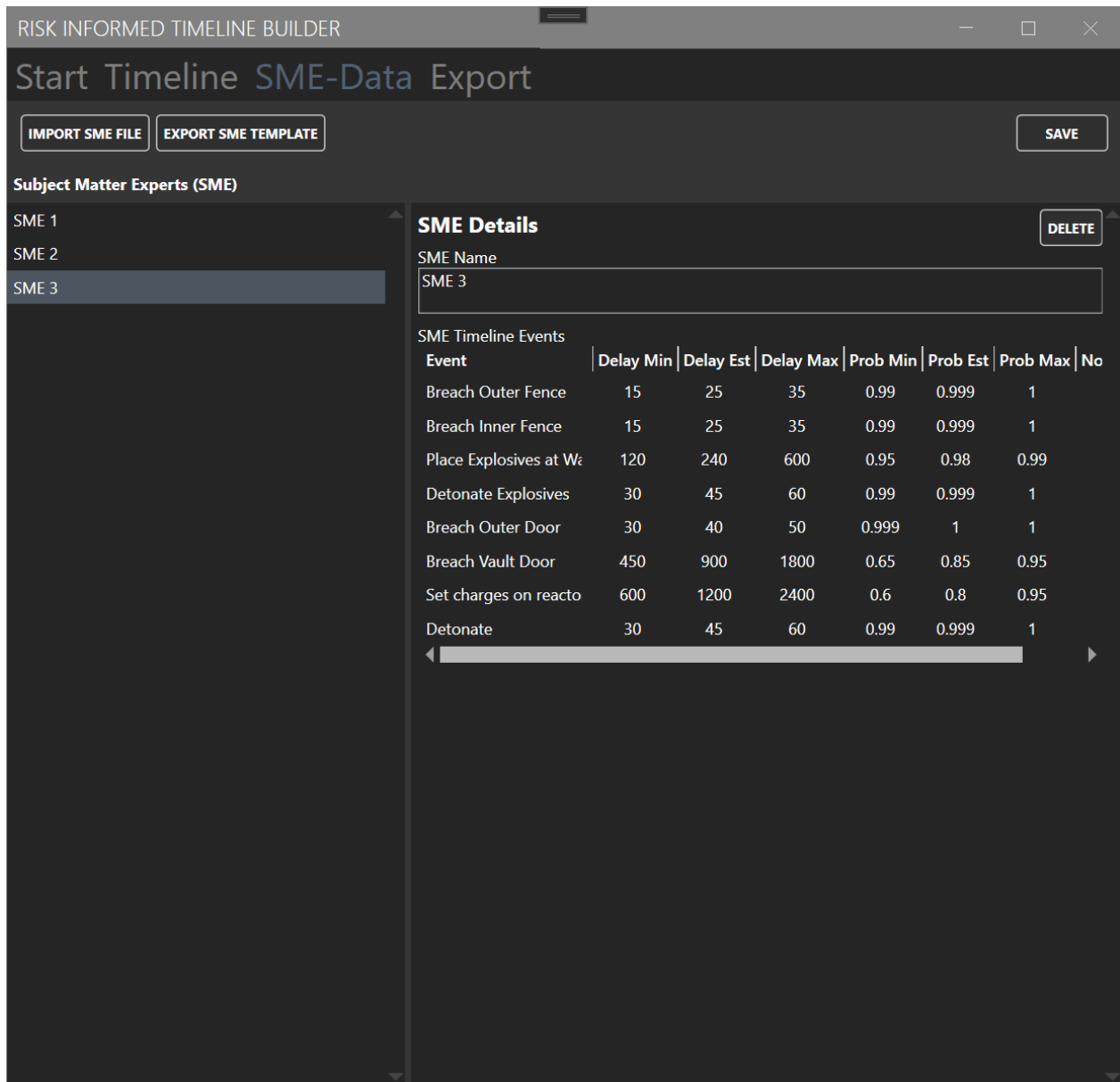


Figure 3 SME Data Screen of the RIT Builder Tool.³

3.3.1. Export SME Template Button

Exporting a SME template will create a spreadsheet representation of the timeline with blank cells for the SME to fill out. The idea is to export the template and send a copy to each participating SME. The SMEs then fill out the timeline with their data and send it back.

³ All data shown is completely notional.

3.3.2. **Import SME File Button**

After following the steps in 2.3.1, simply click the Import SME File button and select the SME file you wish to import.

3.3.3. **SME Details**

After importing SME data, a user can change the name of the SME and view/validate their data in the SME details section.

3.4. **Run and Export Tab**

This tab allows a user to run the algorithm and generate output or export the timeline for use later with the console version of the tool.

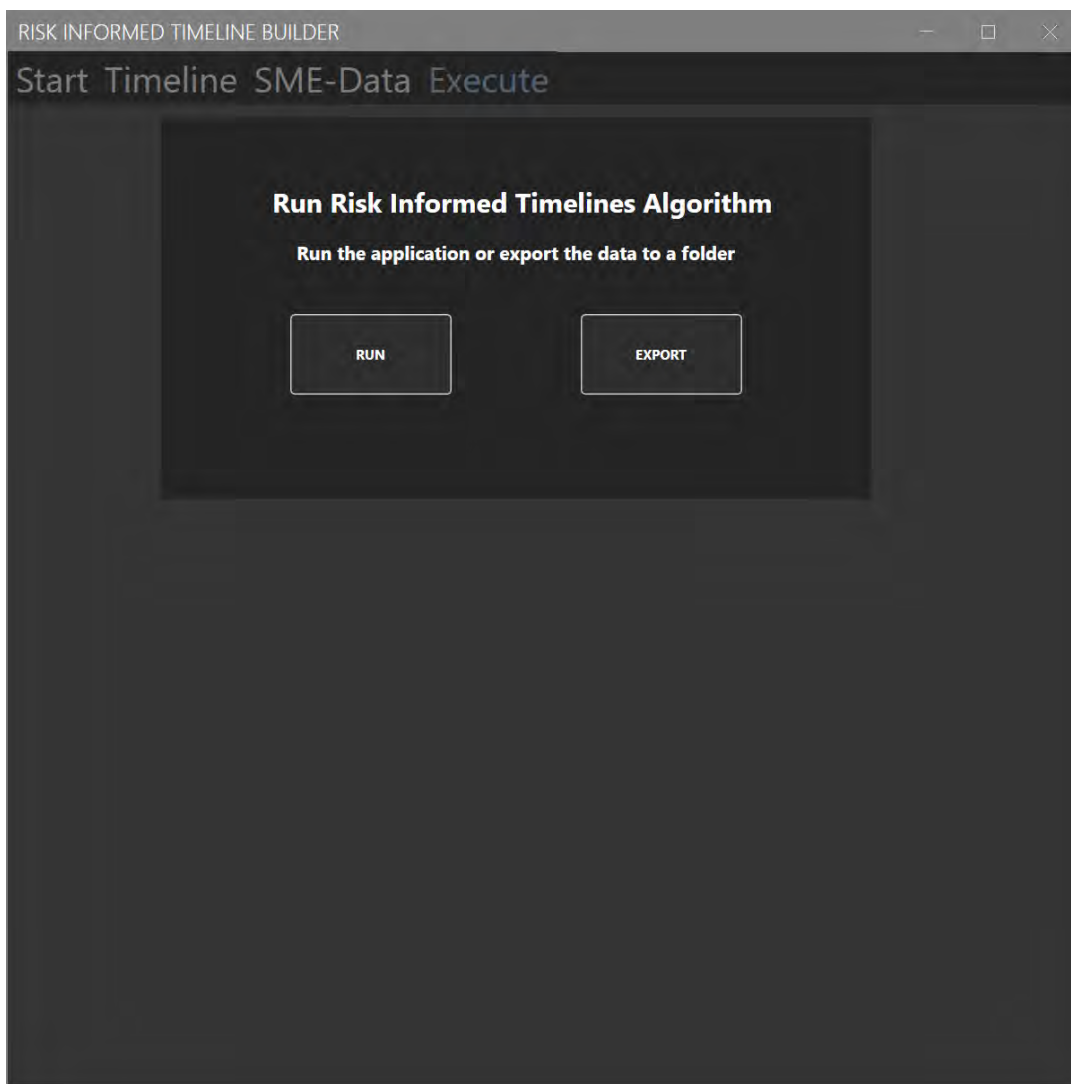


Figure 4 Execute Screen of the Risk-Informed Timeline Builder Tool.

3.4.1. Run

Clicking “Run” will bring users to menu to select an output directory. Once that is complete, the RIT algorithms will run and generate the timelines results. The output folder will then be opened for review.

3.4.2. Export

The data can also be exported the timeline for use in manually running the RIT tool from the command line. Simply click the export button and select the directory you wish to export to. The file structure detailed in Section 2.3 will be exported for use in the RIT tool.⁴

⁴ The RIT Builder is a Windows only application. Timelines can still be generated manually, if needed, on other operating systems.

4. RESULTS

4.1. Overall Results

The risk informed timelines tool provides overall results. This contains a combination of all events delay and success probability.

4.1.1. *FinalResults.csv*

The final results csv contains the overall delay and success probability samples for each run.

4.1.2. *Final Result Histograms*

Included are generated histograms of overall delay and probability samples

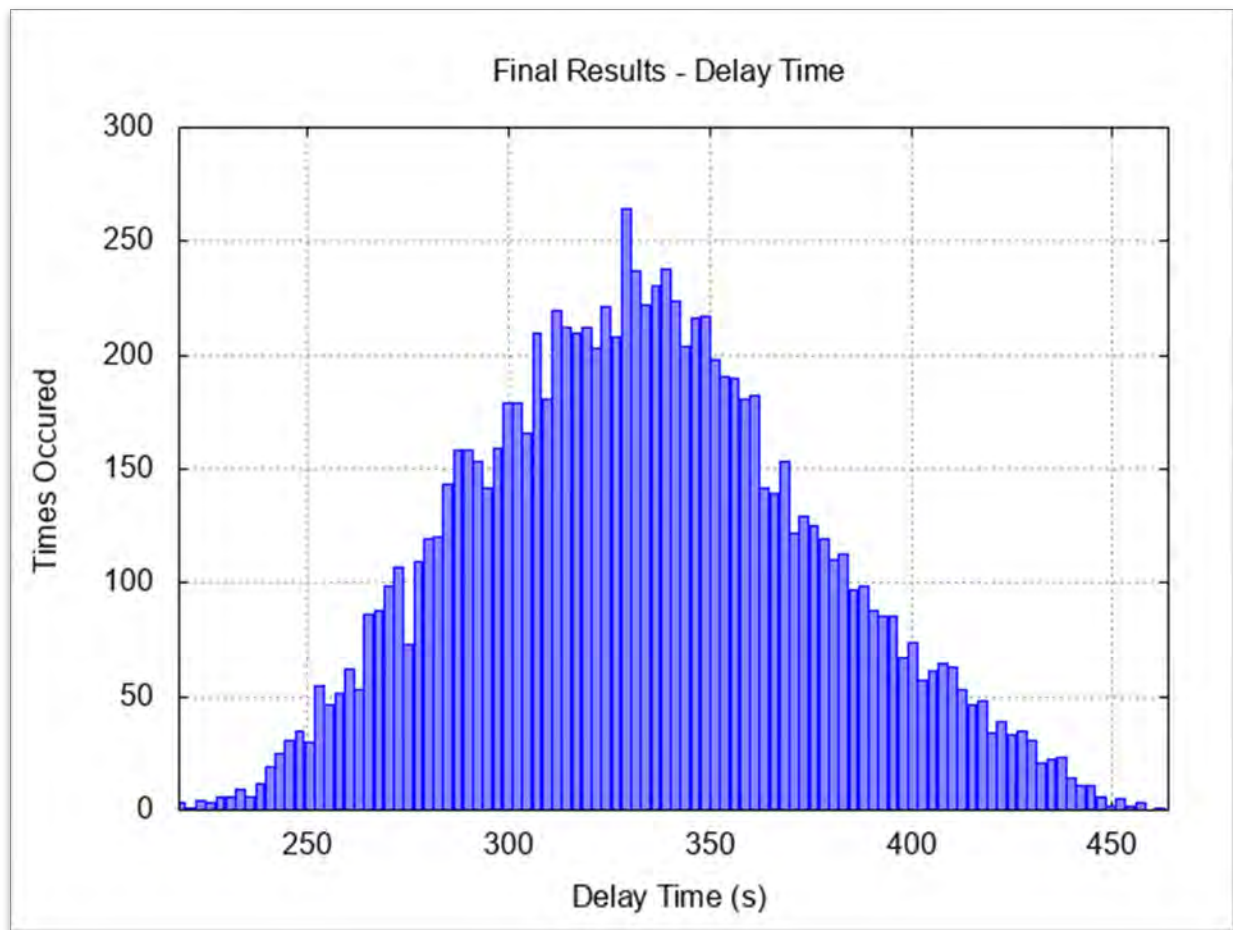


Figure 5 Example of a Delay Histogram Generated by the RIT Tool with 10,000 Runs.⁵

⁵ Data is completely notional

4.2. Event Results

Each timeline event results are contained in the “EventResults” folder as a csv file.

4.2.1. “event_#_results.csv”

Each row in the spreadsheet contains the sample time and probability for that event (Time, Probability). and the time/probability up to (and including) that event on the timeline (Time Up To, Probability Up To).

5. RUNNING THE RISK-INFORMED TIMELINE TOOL WITH ARGUMENTS

5.1. Argument Description

-inputDir <input directory path>

Specifies the location of the input directory (see Input Directory section below for more information).

-outputDir <output directory path>

Optional – Specifies the output directory.
Default: <current directory>/ritResults/

-runCount <number of runs>

Optional – Number of samples that the tool will generate for the timeline
Default: 10,000

5.2. Example of Running with Arguments

```
> rit.exe -inputDir C:/timelines/example-timeline/ -outputDir C:/timelines/example-timeline-output/ -runCount 1000
```

5.3. Input Directory

5.3.1. Input Directory Description

The input directory has a specific layout that must be followed in order for the tool to run successfully. It is recommended to use the **Timeline Builder** software to create a timeline and build the input but it can be created manually if necessary.

5.3.2. Directory format

inputDirectory/smes/

Contains one or more SME csv files

inputDirectory/timeline/

Contains a single timeline csv file.

5.3.3. Timeline Input File

The timeline file is a comma separated values (csv) file that contains all pertinent information and trial data for the timeline that is being analyzed. The **Timeline Builder** tool can generate this file.

Structure:

Event #: The number of the event in the timeline (in sequential order). Use this to reference to events in the SME files or in the output

Description: A brief description of the timeline event

Additional Info: Additional information about the event. Can be left blank

Complication Level: How complicated the event is (Low, Moderate, High, or Very High). Can be left blank

Trials: The number of trials conducted on this timeline event.

Successes: The number of successful trials

Trial Notes: Any notes or information about the trials conducted

Min Calc Type: Method to merge “min” SME data (Min, Median, Mean, or Max)

Mode Calc Type: Method to merge “mode” SME data (Min, Median, Mean, or Max)

Max Calc Type: Method to merge “max” SME data (Min, Median, Mean, or Max)

MLE Bound: Bound for the Maximum likelihood estimation. Default to 1.0

5.3.4. SME Input Files

Each Subject Matter Expert (SME) needs a comma separated values (csv) file containing their delay and probability estimates for each event in the timeline. The **Timeline Builder** has an interface to collect this data in user friendly way.

Structure:

Event #: The number of the event in the timeline (in sequential order). Use this to reference events in the timeline file or in the output.

Delay Min: The SMEs minimum delay for each event.

Delay Est: The SMEs estimated delay for each event.

Delay Max: The SMEs maximum delay for each event.

Prob Min: The SMEs minimum probability of success for each event.

Prob Est: The SMEs estimated probability of success for each event.

Prob Max: The SMEs maximum probability of success for each event.

6. CONCLUSIONS AND PATH FORWARD

Shifting from traditional methods of delay timeline analysis, in which a single value is used to represent a task's duration, to one that provides probability distributions for both task duration and likelihood of success will help analysts and facility operators to better understand the risk associated with various potential attack pathways. This will help nuclear power plant sites prioritize funding to the areas that will buy down the most risk rather than being driven mostly by the pathways with the shortest credible times. Also, this is expected to help nuclear power plant sites improve their security posture without driving up cost excessively and may open opportunities to expand design-basis threat considerations.

The RIT software in this report is meant to enable security risk managers to begin this transition into a more holistic type of delay timeline analysis. The statistical tools are simple, and the methods are structured to utilize analytical solutions for ease of implementation. However, the method will be most useful when the statistical tools are married to timeline construction so the benefit can be gained through targeted, thoughtful use of the method; wholesale application to any timeline should be avoided.

Extensions to this methodology and RIT software can be developed that will enable analysts to explicitly account for correlations between tasks, as well as factors like progressively decreasing adversary performance through fatigue, or progressively increasing performance through practice; correlated variables within the RIT software is an area of future work. Flexibility can be increased by transitioning from Bayesian statistical models with analytical solutions (i.e., beta distribution) to a broader population of models with solutions that can be obtained with sampling. The characterization of uncertainty within the methodology and RIT software could also be advanced through SME training on statistical distributions and elicitation facilitation to enable experts to specify distributions with more flexibility.

The RIT software is currently being integrated into commercial force-on-force modeling software as well as U.S. Government path analysis and force-on-force software. These efforts are occurring outside of the funded LWRS efforts but will have an impact on the ease of usability of the RIT software with the domestic nuclear power fleet.

This page left blank

REFERENCES

- [1] Pacific Gas & Electric Company, “PG&E Company 2018 Nuclear Decommissioning Costs Triennial Proceeding Prepared Testimony – Volume 1,” December 13, 2018. <https://analysis.nuclearenergyinsider.com/pg-e-seeks-decommissioning-head-start-cost-estimates-rise>
- [2] Nuclear Energy Institute, “Delivering the Nuclear Promise,” 2016-2019 <https://www.nei.org/resources/delivering-the-nuclear-promise>
- [3] United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73. “Physical Protection of Plants and Materials.” <https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/>
- [4] United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73 Section 55. “Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage.” <https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0055.html>
- [5] United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73 Section 56. “Personnel Access Authorization Requirements for Nuclear Power Plants.” <https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0056.html>
- [6] United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73 Appendix C Section II. “Licensee Safeguards Contingency Plans.” <https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-appc.html>
- [7] United States Nuclear Regulatory Commission. Title 10, Code of Federal Regulations, Part 73 Section 54. “Protection of Digital Computer and Communication Systems and Networks.” <https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html>
- [8] Brooks, D., A. Thompson, and D. Osborn, “Risk-Informed Access Delay Timeline Development,” SAND2020-9176, Sandia National Laboratories, September 2020.

