Risk-Informed Access/Delay Timeline Development

Dusty M. Brooks and Andrew D. Thompson
Physical Security Pathway

Physical security systems rely on three main elements for protection: detection, delay, and response. Performance and reliability of these systems are tested, but due to the costs with constructing and testing delay barriers, security experts are often forced to work with small datasets that are not well suited to traditional frequentist statistical methods. To provide better insight into overall system performance, the LWRS Program is investigating methods through SNL that leverage Bayesian methods to better integrate subject matter expert (SME) analysis with these small test datasets. This will provide a more holistic view of delay performance, including state-of-knowledge uncertainty.

Historically, delay timelines consist of a set of individual tasks with their associated times—informed by data when feasible and informed by SME judgement when not. Tasks are defined by a single-time data point for the task to be completed. In practice, these tasks have a range of times that can be described by a probability distribution. By shifting from a single-time data point for each task and moving to a probability distribution, Monte Carlo sampling from each task distribution can be used to estimate: (1) the distribution of task times in which the full timeline could plausibly be completed; and (2) the probability that a timeline could be completed given that unrecoverable failures may occur.

This new approach shifts the focus from finding ways to address the shortest potential adversary timeline to a broader view of security that allows the user to gain a deeper understanding of where modifications to the physical security system will have the most impact on reducing overall security risk. Specifically, timelines for a variety of pathways can be developed using these methods. Sensitivity analysis can be used to identify areas where additional delay barriers will provide the greatest effect on overall system performance.

When developing the timelines, Bayesian statistics can be used to formalize how SME judgement can be supplemented by small datasets in a way that is explainable and defensible.

An early demonstration of the output of this capability can be seen in Figure 2. For this example, SNL demonstrated the method by utilizing three sets of SMEs to generate timelines. Additionally, one of the SME groups collected performance test data for select tasks within the timeline. By compiling this data using Bayesian methods, the team produced probability distributions for the time duration of the full path, as well as the likelihood of success.

These probability distributions can also be used in conjunction with other tools for evaluating system performance, such as DANTE [1], AVERT [2], or Simajin/VANGUARD [3]. This new risk-informed approach provides more realistic quantification of scenarios than previous methods and results in higher fidelity simulations of the full physical security system, including detection and response. As this method develops, the team hopes to implement tools to aid security experts in developing timelines that can be used to support risk-informed decision making and improve the overall security at nuclear facilities.

References

1. Sandia National Laboratories developed physical security modeling software, https://www.osti.gov/servlets/purl/1431716.
2. ARES Security Corp. developed physical security modeling software, https://aressecuritycorp.com/avert.
3. Rhino Corps. developed physical security modeling software, https://www.rhinocorps.com/products/.

Figure 2. Example distributions for (left) timeline duration probability and (right) probability of adversary success.