Implementation of Task Variance Model in Security Assessment Models

Sponsor: U.S. Department of Energy Office of Nuclear Energy
Institution: RhinoCorps, Albuquerque, NM
Principal Investigator: Stephen “Dan” McCorquodale
Additional Authors: Mark Snell and Matthew Talbot

http://www.rhinocorps.com

April 2022

SBIR Project Synopsis

- FOA-0002360 DOE-2021 Phase1 Release 2; Topic 39R Advanced and Small Reactors Physical Security Cost Reduction
- The Light Water Reactor Sustainability program developed a new method to modernize how access delay timelines are computed
  - Uses Bayesian methods to combine SME and small performance test datasets
- Proposed integrating this method into our COTS force-on-force modeling and simulation tool (Simajin/Vanguard)
  - A pilot site was used to investigate the conservativism in security assessment process where the assumption is that all tasks are executed without failure
  - Acquired commercial license from Sandia for Risk Informed Timeline (RIT)

Human Performance Basis in Simulation

- Selected a breaching technique used commonly in scenarios
  - Involves throwing a breaching charge that must land close to a barrier to be considered successful
  - In some cases, adversary may throw over multiple fences and in awkward postures that can make evaluating success of task very difficult
  - Collected performance data at multiple distances and throwing positions
- Simulation-based tasks modified to support key mechanics
  - Remote placement, delayed detonation, and probability of failure
  - Explicitly defined contingencies for breach failure
  - Prototype plugin module created to integrate with RIT software

Performance Testing

Prepare and Run Simulations

- Three pre-existing attack scenarios selected for the analysis
  - Modified to incorporate mechanics for throwing and delayed detonation
  - Standard defense configuration used
- Variants of defense created to evaluate post reductions
  - System effectiveness already very high in baseline studies
  - Created variant defense with fewer defenders
- Each attack and defense combination executed with baseline (min time and no failure) vice risk informed basis for task failure probability
  - Developed distributions using RIT as well as other statistical methods
  - Each scenario combination executed 250 times

Example PF Reduction Analysis

- Shows Change in Number of Times Adversary Enter VA

Baseline Number of Times Into VA

Scenario	Base	PF-1	PF-2	PF-3	PF-4
1	5	15	13	15	36
2	0	0	0	9	41
3	63	53	69	137	191

Risk Informed Number of Times Into VA

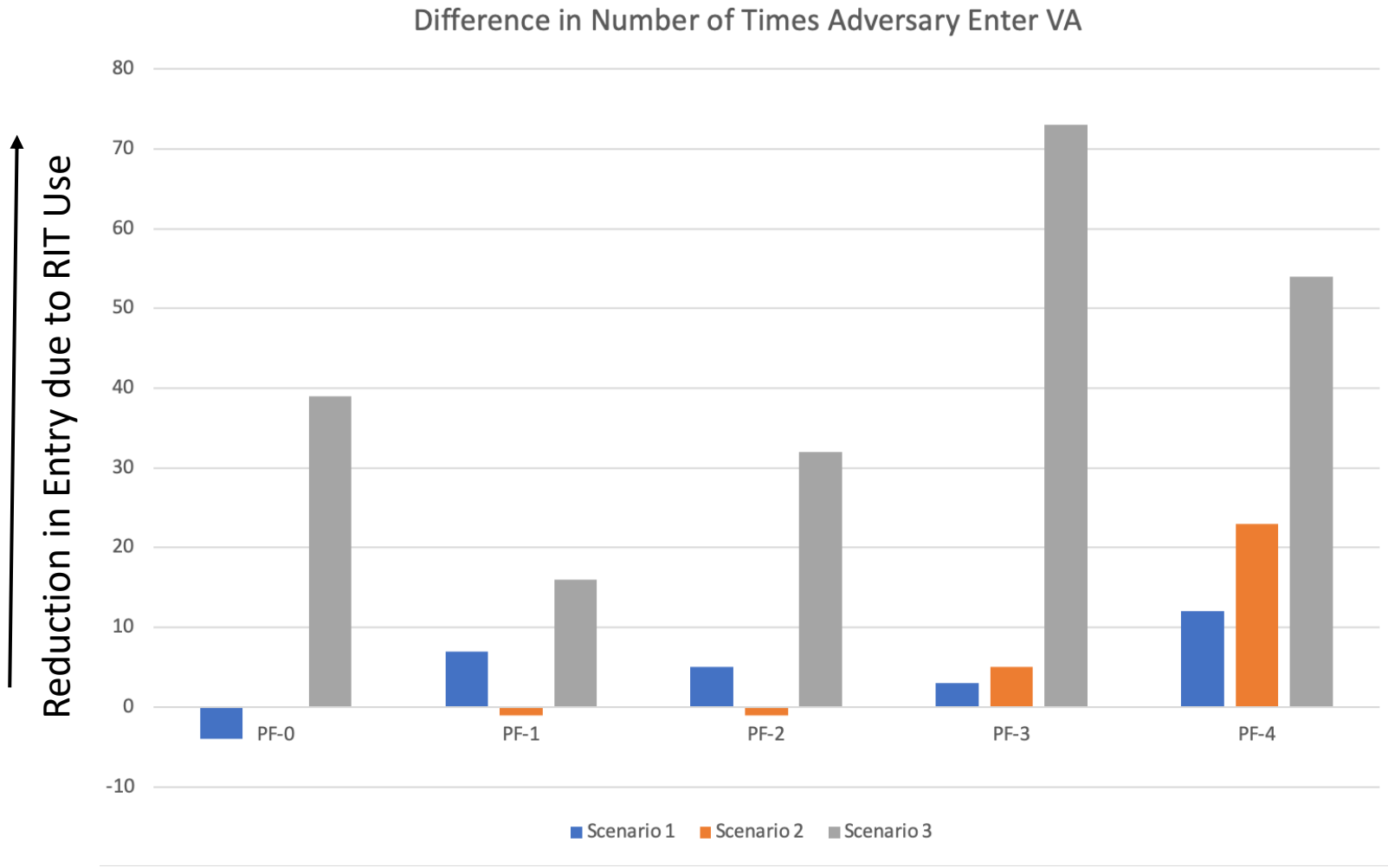
Scenario	Base	PF-1	PF-2	PF-3	PF-4
1	9	8	8	12	24
2	0	1	1	4	18
3	24	37	37	64	137

Change in Number of Times Into VA

Scenario	PF-0	PF-1	PF-2	PF-3	PF-4
1	-4	7	5	3	12
2	0	-1	-1	5	23
3	39	16	32	73	54

Many of the differences are statistically significant.

Risk Informed Timeline Impact



Average increase in time of entry into VA was 7-14 seconds higher using risk informed methodology.

Sample analysis supported the reduction of an additional post (2 versus 3).

Conclusions

- **Risk informed breaching cases all showed improvement or remained constant in win percentage and other measures**
- Quantifying uncertainty for key tasks is important to balance security and risk
- Standardization and statistical analysis of performance test data will require independent support for security departments
  - We have started a conversation in NNSA to evaluate breach failure modes and rates at the M&S TWG (February 2022)
- Generating and managing performance data that covers broader sets of tasks with support from industry or NRC will be helpful

Moving Forward

- Pursue Phase II funding
  - Greater emphasis on advanced reactor and small modular reactor designs
  - Seek to use an advanced reactor for Phase II analysis and testing
- Implement more general representation of random delay and failure probability in simulation-based tasks
  - Especially important to advanced reactor designs
- Advanced and small reactor designs can benefit from security simulation
  - Detailed site plan not required to conduct analysis
  - Performance requirements can be established for security response and delay