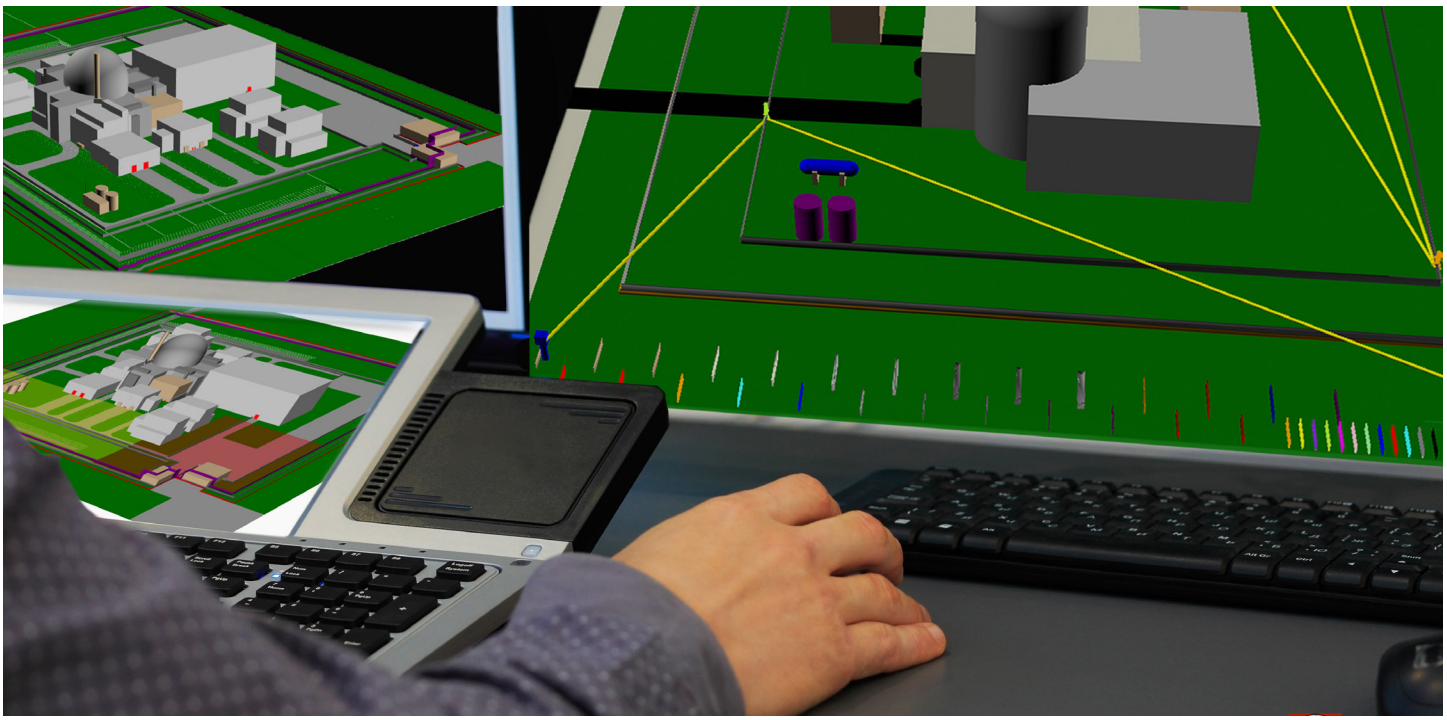
Security Effectiveness Evaluation Software



More Reliable Site Protection in Less Time with Fewer Personnel

As the nuclear industry faces escalating economic challenges, there is an increasing drive to effectively protect plant systems from sabotage threats at a more reasonable cost — all while maintaining exceptional nuclear safety. Through the NEI initiative to Deliver the Nuclear Promise, the industry is rethinking operating practices to improve efficiency and provide reliable site protection.

The scope of this responsibility is constantly changing as new challenges develop and NRC guidance evolves. This results in the need for compensating changes in situational evaluation, training, and tactics to ensure continued high performance in drills and for actual threats. That's why AREVA created the Security Effectiveness Evaluation Software (SEES). SEES was originally developed as part of the licensing effort for the U.S. EPR™ reactor.

Benefits:

- Justify to the NRC the reduction of over-commitments
- Optimizes placement of and number of defenders
- Allows more scenarios in less time with improved accuracy, better reproducibility, and fewer personnel than traditional tabletop evaluations
- Quantitatively evaluates more scenarios with more variations to ensure solid defense against adversaries
- Strengthens plant security by employing exclusive virtual force-on-force evaluations
- Allows for accurate evaluation of the effect of plant modifications on security response
- Generates evaluation documentation with less effort than traditional methods

AREVA NP

AREVA

Security Effectiveness Evaluation Software (SEES)

The Security Effectiveness Evaluation Software was built from the ground up using NEI Security Drill Tabletop methods and capabilities. The output data is similar to debriefs from drills and tabletops to maximize NRC acceptance of model results.

The SEES program has no SGI information embedded, and all protected values are controlled as independent input data. This means that the software does not have to be changed to add or edit features or performance parameters, such as delay times, number of adversaries, or weapons.

Fully adaptable to regulatory changes

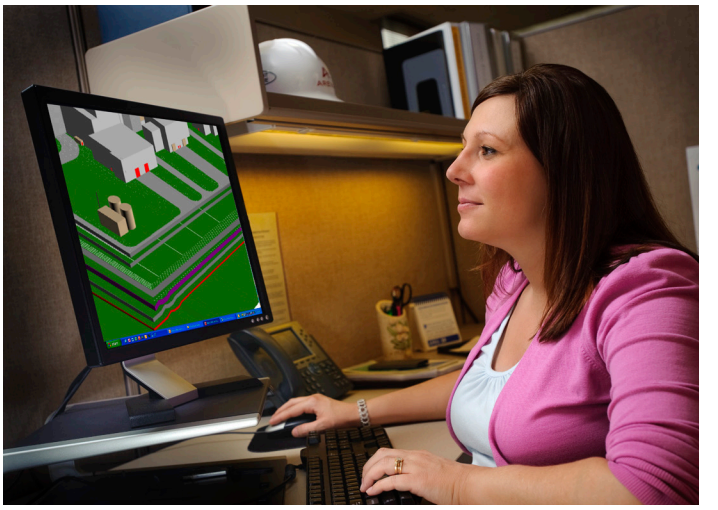
Reproducibility and a standard set of scenarios means that a change to the site strategy or NRC guidance can be made to the input tables. Each stored attack scenario script can be run in a few minutes to determine if the changes significantly affect performance.

Fast-scenario generation and evaluation allow for dozens of models to be run in one day to screen for performance issues. Second-by-second documentation of engagement activities, locations, assets, and distances provide a detailed review of all aspects of the model.

Since the model provides specific performance values, exact degrees of impact can be determined. Mitigation efforts can be added to the configuration and the scenario rerun to demonstrate that there is no degradation in performance. The use of this modeling reduces risk of a weak programmatic strategy by allowing staff to evaluate attack vectors instead of determining the outcome of specific attacks.

Justify to the NRC the reduction of over-commitments

Using a standard set of scenarios and running various defensive post-configurations will provide a quantitative comparison of performance. This optimization of defender placement aids in justifying adjustments in staffing levels by providing quantifiable comparisons of neutralization potential. With this quantification, a case can be made that pathways with very large performance margins can be reduced to be more in line with the average performance margins.



Fact versus opinion

Opinion: Most drills and tabletop scenarios are only as accurate as the staff's skill level and the "impression" of the actual risk.

Fact: Modeling provides specific and direct comparable results that are independent of the skill level of the participants.

AREVA Inc.
Corporate Headquarters
7207 IBM Drive
Charlotte, NC 28262

For more information, contact :
Greg Ott
Product Line Manager
Security and Digital Protection Solutions
Gregory.Ott@areva.com
Phone: 704.805.2032
Mobile: 434.221.5828

us.areva.com