A Virtual Reality Environment for Human Reliability Assessment for Physical Security

PI: Carol Smidts - The Ohio State University

Collaborators: A. Shafieezadeh, A. Yilmaz (The Ohio State University), Ron Boring, Vaibhav Yadav (INL), Tom Myers (Duke Energy).

Program: RC-10: Physical Security Pathway: Evaluation of Physical Phenomena Data Impact and Improvements

ABSTRACT:

Physical security staff, while critical, constitutes approximately 20% of a nuclear power plant workforce and therefore contributes significantly to the costs of operating and maintaining a nuclear power plant. To dedicate an appropriate amount of resources for security staffing, improve performance and reduce threats, modeling and simulation of physical attacks are pursued including efforts that couple Force on Force simulation tools with probabilistic risk assessment. To obtain accurate models, a key is the representation of human behavior and the assessment of the likelihood of failure. Current models have represented the various actions to be performed by the attackers and the defenders on the external boundaries of the plant, the possible use of FLEX equipment, as well as the lack of action. They have not captured, however, erroneous actions, the performance shaping factors (i.e. the factors that influence actors in erring), the progression of the attackers within the plant buildings and the actions that defenders and operators can take within the plant to remedy the situation if attackers were able to penetrate the perimeter. These gaps can lead to overly conservative estimates of risk under physical attacks, possibly distortion of our understanding of relative risks and relative priorities for safety management, and overinflated levels of staffing with the consequent cost penalty.

The current research proposes to address these issues through the development and use of a virtual reality high fidelity simulator that leverages existing tools and couples physics-based simulation for optimal rendering of the environmental conditions surrounding the operators, attackers, defenders and therefore permits meaningful data collection on various human errors and performance shaping factors (via for instance biometric data). Results of data collection will be used to update the models developed so far and therefore provide more realistic estimates of risk, as well as the technical basis to optimize staffing levels. The major impacts of this research are: 1) an empirical basis in understanding human performance of actors involved in physical attack and response beyond the first line of defense, 2) human reliability models that are readily integrable into securing risk analysis frameworks such as dynamic probabilistic risk assessment methods, 3) more comprehensive risk modeling available to utilities to assist with planning and prioritization of defensive postures, and 4) a platform to enable non-intrusive training of protective forces personnel for physical attacks based on the environment created and the understanding of human error sources associated to the research. Major deliverables include the virtual simulation environment, the experimental data and lessons learned to the extent they can be shared under Institutional Review Board protocols. Methods used in the development of the research include design of experiments, surveys, data collection and analysis in simulator environments, human reliability modeling, virtual reality techniques and tools, and physics-based simulation of attack and defense effects.