

# A BAYESIAN NETWORK APPROACH TO QUANTIFY HUMAN ERROR PROBABILITIES IN SECURITY SCREENING OPERATIONS

*Robert Brigantic, Pacific Northwest National Laboratory, 902 Battelle Boulevard, Richland, WA 99352, 509-375-3675, [robert.brigantic@pnnl.gov](mailto:robert.brigantic@pnnl.gov)*

*Bryan Stanfill, Pacific Northwest National Laboratory, 902 Battelle Boulevard, Richland, WA 99352, 509-375-6403, [bryan.stanfill@pnnl.gov](mailto:bryan.stanfill@pnnl.gov)*

*Casey Perkins, Pacific Northwest National Laboratory, 902 Battelle Boulevard, Richland, WA 99352, 509-372-6651, [casey.perkins@pnnl.gov](mailto:casey.perkins@pnnl.gov)*

## ABSTRACT

This presentation provides an overview of an approach that includes a Bayesian network to model and quantify the probability of human errors that may occur in conducting security screening operations. This framework is comprised of three sequential steps. The initial step applies the Human Error Assessment and Reduction Technique (HEART) to first yield the probability of making an inadvertent error by security personnel as they respond to a typical “alarm” at a screening point. The second step then applies a Bayesian network to determine the probability of a violation (e.g., ignore the alarm and not take action) by the security personnel. Finally, the third step again applies the HEART method to determine if the security personnel take the appropriate action in responding to the alarm if no violation was made. In the second step, the Bayesian network considers operational information (e.g., current workflow at the screening point), personnel experience, and personnel motivation to compute the probability of a violation based on particular settings for these parameters.

**Keywords:** Bayesian network, human error, security screening, violation.