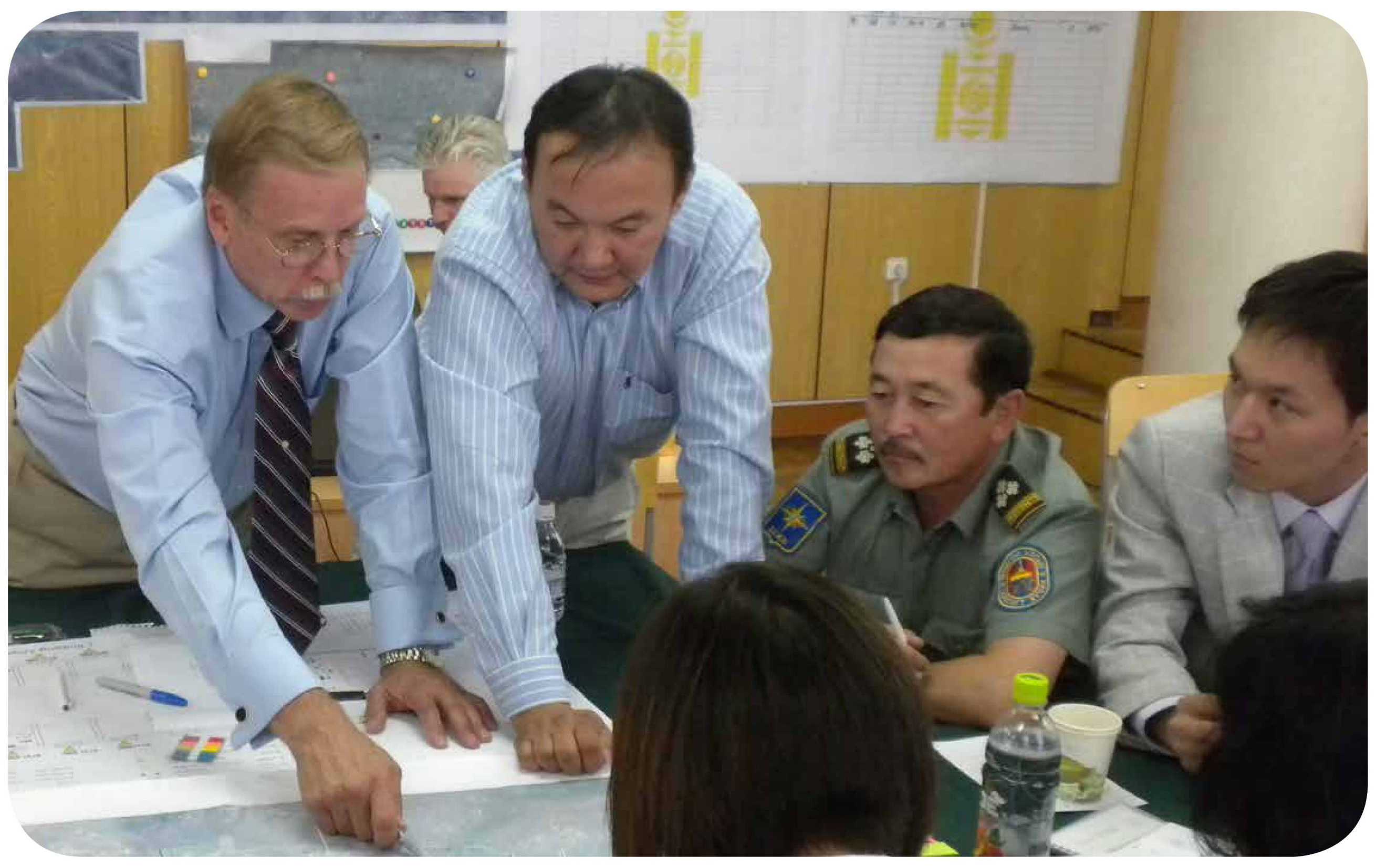
SAND2015-9526C

Exceptional service in the national interest



1st Security Responder Tabletop Exercises

Synopsis

An essential element of research reactor operation is providing assurance that appropriate measures have been taken to prevent potential adverse consequences of nuclear and radioactive materials. From a security standpoint, this assurance must include approaches to assess the effectiveness of the security

AUTHORS:

Matthew Thompson
Sandia National Laboratories

Derek Farr
Sandia National Laboratories

David Ek
Sandia National Laboratories

Dominic Martinez
Sandia National Laboratories

John Pelletier
Sandia National Laboratories

Methodologies

Several approaches for understanding the effectiveness of security measures and security systems have been employed. These include measures to understand the effectiveness of individual components and measures to understand the overall effectiveness of the entire integrated security systems.

These measures include:

- Component analysis
- Performance testing
- Expert Opinion
- Computer models
- Computer simulations
- Tabletop Exercises
- Force-on-Force Engagements

Each of these approaches has strengths and weaknesses. In principle, the employment of multiple approaches with contrasting strengths and weaknesses will lead to a better understanding of security effectiveness than any individual approach. In this presentation, we will focus on the role and value of the first security responder tabletop exercises, including their strengths and weaknesses.

A Tabletop Exercise is a simple method of simulating an adversary attack on a site's existing or proposed Physical Protection System (PPS). These exercises bring together representatives of all the affected organizations that will have a role in an actual engagement at the research reactor. These exercises are used to analyze selected attack scenarios while using an agreed-upon Threat Statement or Design Basis Threat. The Tabletop Exercises considers the appropriateness and interaction of detection, delay, and response elements of a site's existing or proposed PPS, investigates the communication and coordination that exists between staff, guards, and response forces, and provides insight on the level of system effectiveness while exercising the site's Security, Contingency or Emergency Plans. This analysis tool will stress the site's PPS by exploiting potential vulnerabilities and then help identify options/upgrades for mitigating these vulnerabilities.

Phased Approach

A first security responder Tabletop Exercise consists of four phases.

1 PHASE The first phase involves identifying the appropriate stakeholders, formulating a scoping agreement (adversary characteristics, etc.), and creating a Security Force Picture In Time.

2 PHASE The second phase involves the development of attack scenarios, which consist of collecting site-specific data and specific details of an attack within the scope of the defined adversary characteristics.

3 PHASE The third phase is to conduct the tabletop exercise that consists of team assignments (protective force, adversary force, and neutral controllers), reviewing the attack scenarios, simulating an attack, and documenting the events. During this phase, the simulation proceeds in discrete time intervals. For each discrete interval, the activities that occur are identified (e.g., adversary detection, movements of all persons, and engagements). Data from the process is recorded on a timeline to capture notable events and engagements.

4 PHASE The fourth involves tracking any issues that are identified and analyzing these to determine if the issue is an artifact of the tabletop limitations, or a potential real concern with the overall effectiveness of the security system. For each potential issue, changes or upgrades to security that address the issue are developed. The exercise can be repeated to assess the impact of the changes.

Although insights gained from Tabletop Exercises are typically general in nature, the process must be directed by an experienced facilitator in order to guide the participants and their input to achieve a valuable exercise. In this way, participants more readily identify gaps and understand that there are often simple or low-cost solutions that greatly strengthen the overall effectiveness of their security.

Lessons Learned

Over the past 5 years many Tabletop Exercises have been conducted at research reactors and associated facilities in several countries. The results of these exercises have varied based on specific security plans, reactor design and layout, and response communication protocols; however, there have been some common themes to these lessons learned:

- Incorrect assumptions are made by operators and response regarding each other's actions;
- Communication between the operator and the many different responders takes longer, is more difficult, and is at times not as straightforward as expected;
- The apparent balanced and complete security system is often found to have gaps in detection or delay that were not obvious to the operator or regulator—usually on the interaction between equipment and people; and
- Off-site response's unfamiliarity with the facility layout and location of the targets is more detrimental than expected.

The results of the Tabletop Exercise are typically not component based but are, rather, more general in nature and qualitative. However, the Tabletop Exercise provides a unique and valuable perspective and insight of security, as compared to Force-On-Force exercise, computer simulations, and performance tests. In addition, tabletops are inexpensive, simple and safe to run, and quickly executed by experienced staff.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. | SAND2015-XXXX X