Engineered Surety Using the Risk Equation (EnSURE)

Calvin D. Jaeger, William K. Paulus, Ruth A. Duggan and Dennis Y. Matsushita
Security Systems and Technology Center
Sandia National Laboratories
Albuquerque, New Mexico 87185

July 16, 1998

Abstract
Engineered Surety Using the Risk Equation (EnSURE) is a new approach being developed by Sandia National Laboratories for determining and mitigating risk. The EnSURE approach is based on the risk equation, which can be defined by the following equation:

\[ R = (P_A)(1 - P_E)(C) \]

Where \( R \) is risk, \( P_A \) is the likelihood of attack, \( P_E \) is the system effectiveness and \( C \) is the consequence. EnSURE considers each of the components of risk to help in assessing surety (e.g. security, safety, environmental) and providing for the most cost-effective ways to reduce risk. EnSURE is intended to help in evaluating and reducing the risk from either man-caused or natural events. It will help the decision-makers identify possible targets, evaluate the consequences of an event, assess the risk based on the threat and the existing conditions and then help in the application of mitigating measures. EnSURE is in the development stages. It builds on existing and ongoing development activities at Sandia, as well as the considerable work done in the fields of consequence analysis, risk analysis and intelligence. The components of EnSure include consequences, constraints, threat, target/goal identification, facility/process characterization, evaluation and analysis, system improvement, and decision making. This paper will provide a brief description of EnSURE.

Risk Equation
The risk equation is the basis of Sandia’s approach to risk analysis. It can be defined by the following equation:

\[ R = (P_A)(1 - P_E)(C) \]

Where \( R \) is risk, \( P_A \) is the probability of attack, \( P_E \) is the system effectiveness and \( C \) is the consequence.

The probability of attack, \( P_A \), comes from the analysis of the threat. It relies on intelligence, history, capabilities, intentions, targeting, existence of the threat, current security environment and other information to arrive at some indicators of the probability of an event. For the worst case situation, \( P_A \) is considered to be 1.0.

System effectiveness, \( P_E \), is the product of two parts: \( P_I \) and \( P_N \). The probability of interruption, \( P_I \), indicates how effective the protective system is in interrupting an adversary attack. The probability of neutralization, \( P_N \), is how well response measures do in such things as force-on-force conflicts with the adversary given interruption.
DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.
DISCLAIMER

Portions of this document may be illegible electronic image products. Images are produced from the best available original document.
1. provide a near real-time graded approach to risk analysis providing the capability from top-level analysis to more detailed analyses based on user needs.

2. analyze the threat in greater detail to determine when it is possible to use a value for likelihood of attack, \( P_A \), other than the assumed worst case value of 1.0 to be used to help discriminate among the target set.

3. expand the treatment of consequences, \( C \), to include mission importance, criticality and impact from blast, chemical/biological agents and radiological sources. It will link consequences to protection upgrades and mitigation decisions and determine the effects of such changes.

4. consider domestic/host nation constraints such as political, social, cultural, regulatory, legal.

5. provide the capability to import and utilize digital geographic and site information.

6. include a robust information management system and database.

7. include capabilities to analyze resources (people, time, and cost).

8. provide a consistent, single, integrated and systematic approach to determining and mitigating risk.

EnSURE acts as a prism. It focuses the viewpoint of all of the various stakeholders, such as the site manager, security manager, security forces, acquisition and budget personnel, operations, and maintenance and all the available information into an effective focused protection system based on risk. EnSURE can be tailored to meet the needs of the user and provide various levels of detail, rigor, and confidence. Initially, a top-level “tell me if I have any problems” approach may indicate when a more detailed and comprehensive analysis could be performed for certain assets and what tools could be applied. The modularity of EnSURE allows the use of the appropriate tools to achieve the desired risk management answer. The process for EnSURE is represented in Figure 1.

Figure 1. Process flow diagram for EnSURE
determine risk for force protection and security problems. Although many tools are currently available, very few, if any, tools exist which integrate all of various components of the risk analysis process into a single, integrated risk analysis tool (Figure 2). This is the goal of EnSURE (Engineered Surety Using Risk Equation).

<table>
<thead>
<tr>
<th>Component</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Characterize the Asset</td>
<td>☐</td>
</tr>
<tr>
<td>Determine the Consequences</td>
<td>☑</td>
</tr>
<tr>
<td>Define the Threats</td>
<td>☐</td>
</tr>
<tr>
<td>Define Safeguards</td>
<td>☑</td>
</tr>
<tr>
<td>Analyze System</td>
<td>☑</td>
</tr>
<tr>
<td>Make the Decision</td>
<td>☑</td>
</tr>
</tbody>
</table>

![Figure 2. Status of tools to support force protection/security problems.](image)

- ○ = Discusses briefly
- ☐ = Covers with some depth
- ☑ = Covers in great depth

**Summary**

There are a number of approaches/tools available that can help users evaluate risk. However, there does not currently exist a single tool that integrates all of the components of risk analysis. EnSURE is an attempt to achieve this goal. EnSURE will utilize many of the available individual tools and integrate them into a systematic process, and eventually a PC-based tool, for determining and mitigating risk. Its graded approach will allow users to both identify top-level issues and also to provide the necessary detailed analyses for developing cost-effective upgrades and actions.

EnSURE will be particularly valuable in force protection and infrastructure protection applications where a diverse target set exists. It could be used in both government and non-government facilities. It would be equally applicable for large installations, sites, individual buildings or other assets, such as people and/or vehicles. It will help the decision-makers identify possible targets, evaluate the consequences of an event, assess the risk based on the threat and the existing conditions and then help in the application of mitigating measures.

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.