SAND--98-1329C
SAN098-1329C

CONF-980666--

RECEIVED
JUN 30 1998
OSTI

Risk Analysis Tools for Force Protection and Infrastructure/Asset Protection

Session IV: Technical and Policy Focus Group A

Calvin D. Jaeger, Ruth A Duggan and William K. Paulus,
Security Systems and Technology Center
Sandia National Laboratories, MS 0759
Albuquerque, New Mexico 87185
505-844-4986, 505-844-0011(fax)
cdjaege@sandia.gov

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.

DISCLAIMER

Risk Analysis Tools for
Force Protection and Infrastructure/Asset Protection

Abstract

The Security Systems and Technology Center at Sandia National Laboratories has for many years been involved in the development and use of vulnerability assessment and risk analysis tools. In particular, two of these tools, ASSESS and JTS, have been used extensively for Department of Energy facilities. Increasingly, Sandia has been called upon to evaluate critical assets and infrastructures, support DoD force protection activities and assist in the protection of facilities from terrorist attacks using weapons of mass destruction. Sandia is involved in many different activities related to security and force protection and is expanding its capabilities by developing new risk analysis tools to support a variety of users. One tool, in the very early stages of development, is EnSURE, Engineered Surety Using the Risk Equation. EnSURE addresses all of the risk equation and integrates the many components into a single, tool-supported process to help determine the most cost-effective ways to reduce risk. This paper will briefly discuss some of these risk analysis tools within the EnSURE framework.

Risk Equation

The risk equation is the basis of Sandia's approach to force protection and infrastructure/ asset protection. It can be defined by the following equation:

$$R = (P_A)(1 - P_E)(C)$$

Where **R** is *risk*, P_A is the *likelihood of occurrence*, P_E is the *system effectiveness* and **C** is the *consequence*.

The *likelihood of occurrence,* P_A, comes from the analysis of the threat. It relies on intelligence, history, and existence of the threat, current 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 a measure of how well the response forces do in force-on-force conflicts with the adversary given interruption.

The *Consequences,* **C**, involve consequence analysis, which considers mission impact, criticality, and cost. This part of the risk equation takes into account the targets or critical nodes associated with an event.

Risk Management

The Risk Equation results in a mosaic that characterizes the level of risk associated with a set of consequences, threats, and a defined protection system. The risk may be either acceptable or unacceptable, but must be managed effectively in terms of available resources such as budget, people, and schedule. EnSURE uses cost and performance analysis (CPA) to evaluate the performance of the system against these metrics. However, if the level of risk is unacceptable, risk management will also call for consideration of upgrades, enhancements, or redesigns of systems. Over time, the list of protected assets, the consequences, and/or the threat may change, requiring reanalysis, revision of the protection system design, and perhaps changes in risk management strategy. Any changes in the protection system design should be analyzed for risk and the impact of resource limitations before implementation.

User Needs for Force Protection

The challenge is to provide to the users a single, tool-supported process that can be used to determine the risk to people, assets and facilities in a consistent and systematic manner and that can identify ways to mitigate unacceptable risks in a cost-effective manner. Some other specific needs are:

- identification of available tools and their applicability to force protection
- assistance in the identification, collection and integration of needed information into a linked databases
- identification and prioritization of a wide range of potential targets including secondary targets
- identification and assessment of the threat to soldiers, civilian employees, family members, facilities, and equipment
- assistance in determining the criticality and consequences of assets/events
- identification of the impact of any constraints
- identification of any vulnerabilities in protection
- suggestions for necessary upgrades and technologies to be used
- identification of resource (people, time, cost) impacts and help maximize resources
- pertinent data to the decision maker
- training and education activities support
- crisis/consequence management planning and execution support
- ability to do near real-time updates to analysis based on changes

Risk Analysis Tools

Many tools/approaches have been or could be used to evaluate risk for security, force protection and infrastructure/asset protection. Sandia National Laboratories for many years has been involved in the development and use of such risk analysis tools as Analytical System & Software for Evaluating Safeguards & Security (ASSESS) and Joint Tactical Simulation (JTS), particularly in support of customers within the Department of

Energy (DOE) and Department of Defense (DoD). More recently Sandia has also applied the methodology in the Design & Evaluation Process Outline (DEPO) and these tools in support of nuclear reactor facilities, airports, schools, prisons, transportation and critical asset protection. These and other tools listed in Table 1 are some of the tools currently available for application to force protection and infrastructure/asset protection problems.

Table 1. Initial Survey of Tools Currently Used in Threat-Based Risk Assessment

Name	Source	Emphasis	Characterize the Asset	Determine the Consequences	Define the Threat	Define the System	Analyze the System	Make the Decision
Security Eng. Project Development*	Army - AF	Asset Characterization/ Risk	●	○		○	○	○
Vital Issues	SNL	Asset/Consequences		◒	○			●
ALOHA/CAMEO	NSC	Dispersal		◒		◒		
ARCHIE	FEMA	Dispersal		◒				
ERAD	SNL	Dispersal		◒				
Hot Spot V6.5	LLNL	Dispersal		◒				
BlastCAD	SwRI	Explosive Effects		◒	○			
BLASTINW	SwRI	Explosive Effects		◒	○			
CONWEP	ACE	Explosive Effects		◒	○			
Canary	QC, Inc.	Emergency Planning		◒				
EIS InfoBook	EIS Int'l Corp.	Emergency Planning			○	○		
CATS	DSWA	Threats		◒	○			○
IRAS	RMS, Inc.	Natural Threats		◒	○			
MDITDS	DIA	Threat			◒			
Energy Intelligence Information System	SNL	Threat History		◒	◒			
AT Planner	USAEWES	Mitigation		◒	○			
SEDA	ACE	Design				◒		
DEPO*	SNL	Design/Analysis	◒	◒	○	◒	◒	
JTS	LLNL	Response Tactics	○		○	◒	◒	
ALPHA	RETAS, Inc.	Vulnerability	○	○	○	◒	◒	
ASSESS	SNL/ LLNL	Vulnerability	○	○	○	◒	◒	
Analytical Risk Management	CIA	Risk	◒	◒	◒	○	○	○
ARRAMIS	SNL	Risk	○	○	○	○	◒	
Risk Watch Suite	Risk Watch, Inc.	Risk	○			◒	◒	
CPA	SNL	Cost /Performance	◒			◒	◒	
Analytic Network/ Expert Choice	Expert Choice, Inc.	Decisions						●
Logical Decisions	Logical Decisions	Decisions						●

Blank = Does not cover ○ = Discusses ◒ = Covers with some depth ● = Covers in great depth
* = Methodology only, all others supported with software

As can be seen from this table there are many methodologies and tools available that generally meet specific requirements. However, no tool exists which integrate all of various components into a single, integrated risk analysis tool. This is the goal of EnSURE (Engineered Surety Using the Risk Equation).

EnSURE

Engineered Surety Using the Risk Equation (EnSURE) is a new approach for determining and mitigating risk and is based on the risk equation. EnSURE is in its early stages of development. It builds on ongoing activities at Sandia and takes advantage of the considerable work done in the fields of consequence analysis, risk analysis, vulnerability assessments and combating terrorism. Some of the components of EnSURE are:

- Threat Analysis
- Consequence Analysis
- Target Identification and Prioritization
- Constraints Identification and Impact Analysis
- Asset Characterization (Site, Process, Mission, People)
- Vulnerability Assessment
- Resource Analysis
- System Upgrades and Mitigation
- Information Management System and Decision Tools
- Risk Management & Planning

While designed to cover a broad range of asset protection, EnSURE will provide enhanced capabilities to analyze force protection risk in a number of ways. It will:

(1) provide a near real-time graded approach to risk analysis providing the capability from top-level analysis to more detailed analyses based on used needs.
(2) analyze the threat in greater detail to determine when it is possible to use a value for likelihood of occurrence, **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 impact, criticality and impact from blast, chemical/biological agents and radiological sources. It will link consequences to protection upgrades and mitigation decisions and determine the affects of such changes.
(4) consider constraints in such areas as political, social, cultural, regulatory, and legal from a domestic and host nation perspective.
(5) provide the capability to import and utilize digital geographic and site information.
(6) include a robust information management system.
(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 will act 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 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 that may indicate when a more detailed and comprehensive analysis could be performed for certain assets, consequences, and threats and suggest 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.

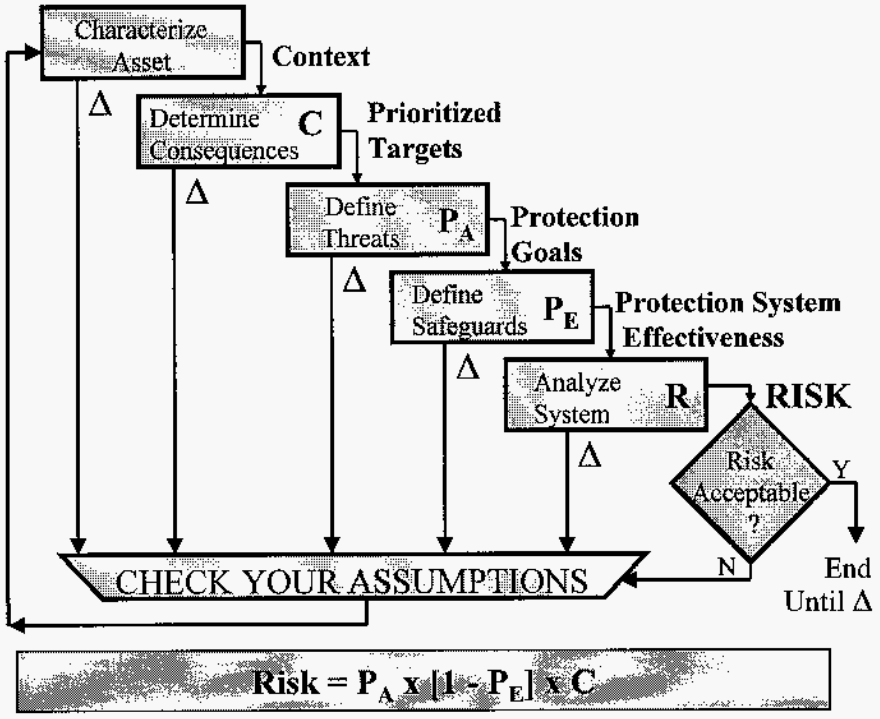

Figure 3. Process flow diagram for EnSURE

Initially EnSURE is intended as a to evaluate all available information concerning the security and force protection posture of an installation and/or asset and help during the planning and assessment phases. It could be integrated with architectural surety (which is designing facilities with surety in mind), awareness education, ES&H assessments, new simulation and modeling tools, collateral damage evaluations, and operations security to name just a few. In addition, EnSURE will provide strong support for possible reactive measures such as emergency operations and crisis/consequence management, and tactical and technical responses to events.

Summary

A number of available approaches/tools address individual parts in evaluating risk for force protection and infrastructure/asset protection. 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 to also provide the necessary detailed analyses for developing cost-effective upgrades and actions.

EnSURE could be applied in force protection and infrastructure protection applications where a wide and 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 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.

Acronym List

ACE	Army Corp of Engineers
ALOHA	Area Locations of Hazardous Atmospheres
ARCHIE	Automated Resource for Chemical Hazard Incident Evaluation
ARRAMIS	Advanced Risk & Reliability Assessment Model Integration Software
ASSESS	Analytical System & Software for Evaluating Safeguards & Security
AT	Anti-Terrorist
CAMEO	Computer-Aided Management of Emergency Operations
CIA	Central Intelligence Agency
CPA	Cost and Performance Analysis
DEPO	Design & Evaluation Process Outline
DIA	Defense Intelligence Agency
DSWA	Defense Special Weapons Agency
ERAD	Explosives Release Atmospheric Dispersion
FEMA	Federal Emergency Management Agency
JTS	Joint Tactical Simulation
LLNL	Lawrence Livermore National Laboratory
MDITDS	Migration Defense Intelligence Threat Data System
NSC	National Safety Council
QC, Inc.	Quest Consultants, Inc.
RETAS	RETA Security, Inc.
RMS, Inc.	Risk Management Solutions, Inc.
SNL	Sandia National Laboratories
SwRI	Southwest Research Institute
USAEWES	U.S. Army Engineer Waterways Experimental Station

Report Number (14) SAND--98-1329C
CONF-980666--

Publ. Date (11) 1998
Sponsor Code (18) DOE/DP, XF
UC Category (19) UC-700, DOE/ER

ph

DOE