SAN097-1353C

CONF-9706109--4

COST AND PERFORMANCE ANALYSIS OF PHYSICAL SECURITY SYSTEMS

M. J. Hicks
Security Systems Analysis and Development Department, 5845
Sandia National Laboratories, Albuquerque, NM 87185-0759, (505) 844-7806, mjhicks@sandia.gov

David Yates, William H. Jago & Alan W. Phillips
Tecolote Research, Inc., 5266 Hollister Ave, Suite 301, Santa Barbara, CA 93111-2089

Dennis F. Togo
Anderson Schools of Management, University of New Mexico, Albuquerque, NM, 87131

ABSTRACT

CPA — Cost and Performance Analysis — is a prototype integration of existing PC-based cost and performance analysis tools: ACEIT (Automated Cost Estimating Integrated Tools) and ASSESS (Analytic System and Software for Evaluating Safeguards and Security). ACE is an existing DOD PC-based tool that supports cost analysis over the full life cycle of a system; that is, the cost to procure, operate, maintain and retire the system and all of its components. ASSESS is an existing DOE PC-based tool for analysis of performance of physical protection systems. Through CPA, the cost and performance data are collected into Excel workbooks, making the data readily available to analysts and decision makers in both tabular and graphical formats and at both the system and subsystem levels. The structure of the cost spreadsheets incorporates an activity-based approach to cost estimation. Activity-based costing (ABC) is an accounting philosophy used by industry to trace direct and indirect costs to the products or services of a business unit. By tracing costs through security sensors and procedures and then mapping the contributions of the various sensors and procedures to system effectiveness, the CPA architecture can provide security managers with information critical for both operational and strategic decisions. The architecture, features and applications of the CPA prototype are presented.

Keywords: security systems design, costs-benefits analysis, software tools, cost effectiveness

1. INTRODUCTION

Security managers are faced with changes in both security threats and security technology alternatives. They need decision support tools that can provide them with easy access to timely analysis of both the cost and the performance of security-systems alternatives.

This paper describes the architecture, output format, and potential applications of Cost and Performance Analysis (CPA), an integrated package of PC-based software tools for evaluation of physical protection systems. CPA was defined, designed and prototyped by Sandia National Laboratories and Tecolote Research, Inc. to support automated definition of a physical protection benchmark. It utilizes ASSESS (Analytic System and Software for Evaluating Safeguards and Security), an existing Department of Energy (DOE) performance analysis tool for physical security systems, and ACEIT (Automated Cost Estimating Integrated Tools), an existing Department of Defense (DOD) life-cycle cost analysis tool. These existing tools are integrated through Microsoft Excel workbooks and macros. CPA makes both tabular and graphic results available to decision makers. In

DISCLAIMER

addition to a predefined set of graphic results generated automatically, the Excel workbook format allows users to customize both data analysis and data presentation.

The architecture of CPA and just a few examples of cost and performance metrics and data presentation are illustrated in Figure 1. The point of initialization for CPA is ASSESS. Data from ASSESS is processed through EXTRACT, a set of utilities written in C++. PERFORM reads the output of EXTRACT and generates an Excel workbook of system and subsystems performance data. CATSS (Cost Analysis Tool for Security Systems), implemented in Excel, is an interactive Excel workbook that organizes the cost data. At the core of CATSS is ACEIT, the data archive and computational engine for the cost analysis.

2. ASSESS (PERFORMANCE ANALYSIS)

ASSESS is an established PC-based physical security performance analysis tool developed for DOE by Lawrence Livermore National Laboratories and Sandia National Laboratories.[1] Although the structure, the data and the vocabulary used in ASSESS were developed for physical protection systems at DOE sites, the methodology has far broader applicability.

The ASSESS software system is composed of a manager and five modules: Facility Descriptor, Outsider Analysis, Insider Analysis, Collusion Analysis and Neutralization Analysis. However, CPA currently extracts data from only three of these modules: Facility, Outsider and Insider.

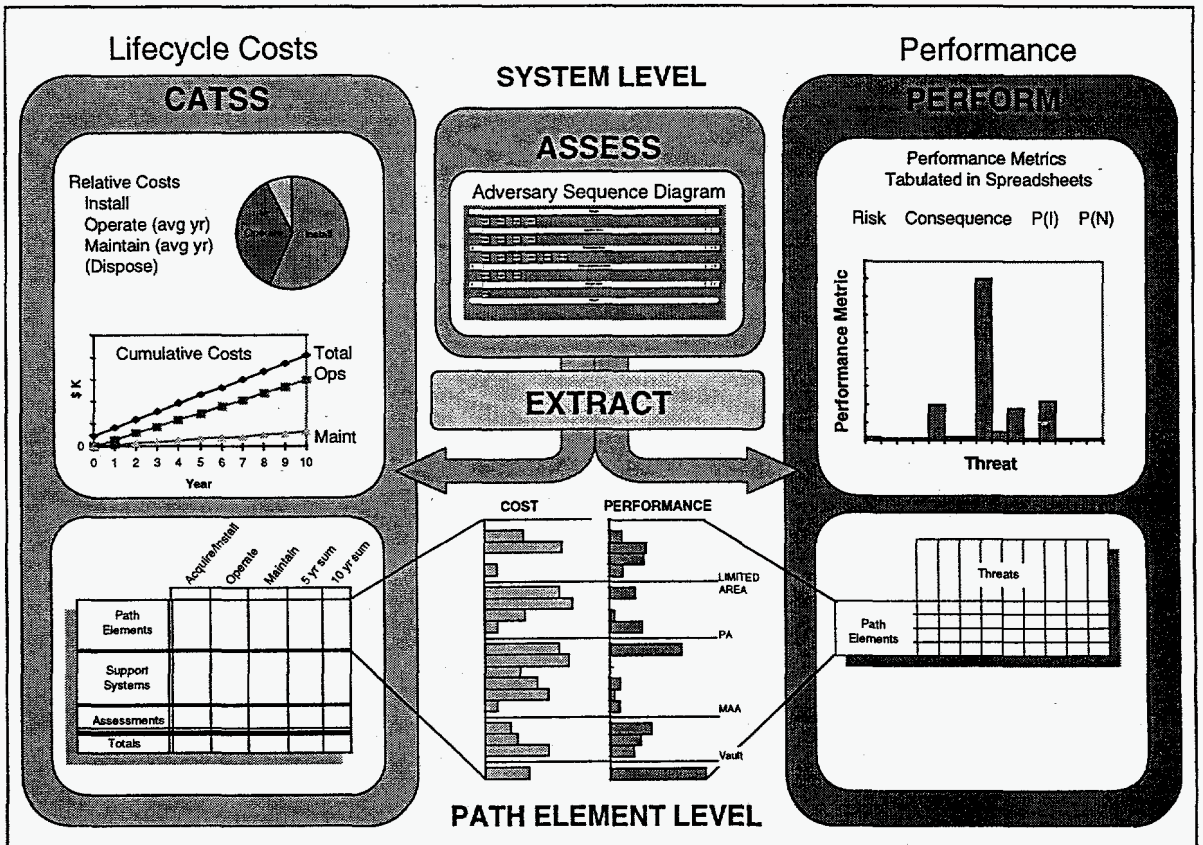

Figure 1. CPA Architecture

In the ASSESS Facility Module, the various components of the physical security system are defined by type and location and are graphically illustrated in an Adversary Sequence Diagram (ASD). The ASD in the upper center of Figure 1 is expanded in Figure 2. The vulnerability analyst uses the ASD to map the physical system into a computer model. The layered approach to physical security systems for depth of defense is evident in the ASD. Path elements provide potential access between protected areas. Path elements function either as barriers (fences, walls, and gates or doors, when closed) or as access control points (gate or doors, when open). Safeguards are associated with both barrier and access control path elements. Safeguards may be sensors; such as, intrusion or contraband detection sensors, or procedures; such as, credential verification or security patrols. Access control path elements are further characterized by the passage authorized (who or what is allowed to pass through) and the details of authorization procedures (automated or manual) applied to passage. All these data describing the physical protection system are used internally by the various ASSESS modules to analyze system performance against user-defined threats. All these data are also necessary to develop life-cycle costs. They are made available to the cost analysis tool (CATSS) and performance analysis tool (PERFORM) through the C++ utilities called EXTRACT.

In the ASSESS Outsider Module, the vulnerability analyst also defines the set of outsider threats of interest and a range of response force times. When executed, the module produces probability of interruption for each threat and each response force time. These and other intermediate data and results are made available to PERFORM through EXTRACT. Similarly, the analyst defines insider threats of interest and executes performance analysis using the ASSESS Insider Module.

There are several methodologies for determining probability of neutralization of the threat by the response force. The Neutralization module of ASSESS uses a probabilistic approach.[2] More sophisticated approaches simulate force-on-force engagements. Currently CPA only receives neutralization probabilities from ASSESS through the Outsider Module.[3]

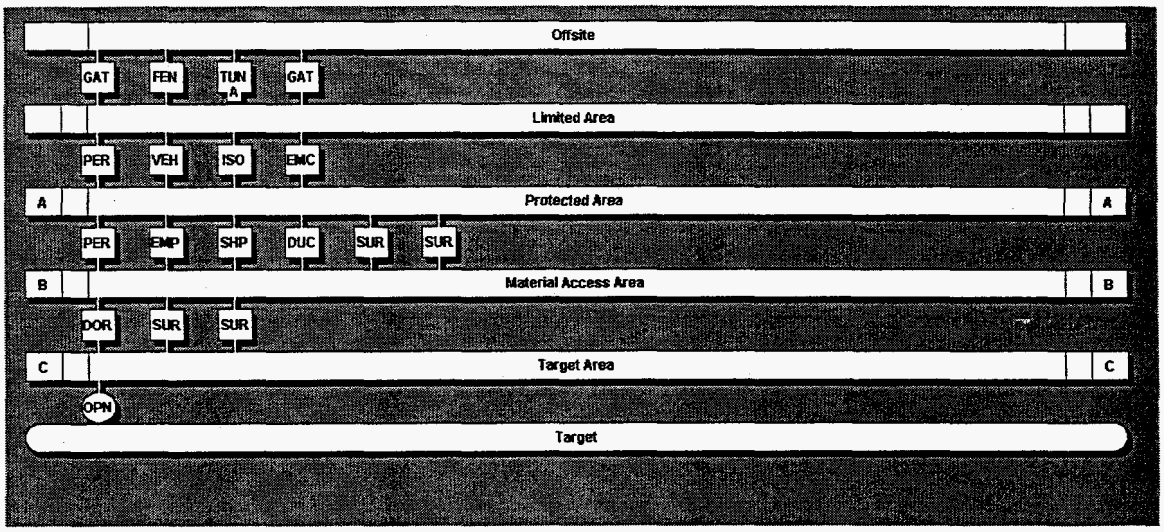

Figure 2. Adversary Sequence Diagram

3. PERFORM (PERFORMANCE DATA COLLATION)

PERFORM is a set of Excel macros that accept data from EXTRACT to develop performance analysis for an ensemble of threats and system conditions defined by the analyst. PERFORM does not generate new data. It does, however, significantly automate the process of collecting, collating and reducing the data available in ASSESS, making the data much more accessible for analysis.

DOE uses the following definition:

$$\text{Risk} = [1 - P(E)] \times C \times P(A), \quad (1)$$

where

$$P(E), \text{ Probability of System Effectiveness, } = P(I) \times P(N), \quad (2)$$

P(I) is Probability of Interruption,
P(N) is Probability of Neutralization,
C is Consequence, and
P(A), Probability of Attack is assumed to be one.

PERFORM presents these data in a format that allows decision makers to quickly identify system risk issues as a function of threat type, and to then identify the relative contributions to risk; that is, C, P(I) and P(N). Risk can be reduced by mitigating consequence or by increasing interruption or neutralization probabilities.

If improved P(I) is desired, then the prototype offers additional detail to decision makers responsible for technology investments. P(I) is a function of response force time; that is, how long it takes for the force to be in position after an alarm is detected; and how long it will take a detected threat to complete its mission. Clearly, early detection and long delays after detection are desirable. For each path element, detection probability, P(D) and delay times, t_d, are tabulated by threat type and threat tactic. The critical path is the path with the lowest P(I). When performance of a security system is analyzed for an ensemble of threats, histograms show how often each path element is in the critical path. (Refer to the bar chart on the right in the lower center in Figure 1). These data at the path element level show the balance of protection across the path elements at each layer. In tabular form, these data also show how much the element performance can be improved before the critical path is likely to be shifted to the next most critical path element in the same layer.

4. CATSS (COST ANALYSIS)

CATSS is a spreadsheet cost analysis tool for physical security systems developed by Tecolote Research, Inc. under contract[4] for Sandia National Laboratories. CATSS is an Excel spreadsheet application consisting of three types of worksheets: output, input and interface. The computational engine for CATSS is seated in an ACE (Automated Cost Estimation) session. The data flow within CATSS is illustrated in Figure 3.

4.1 CATSS output worksheet

All life-cycle costs for a physical protection system are collected into a single Summary Costs Output worksheet in the CATSS Excel workbook. The worksheet is structured as illustrated in the lower left corner of Figure 1 and again in the upper right of Figure 3.

The cost estimation structure (CES) is broken out in the first column of the Summary Costs Output worksheet. The life-cycle costs for the elements identified in the first column are enumerated in the remaining columns. The Excel implementation of the

Summary Costs Output worksheet allows both the CES rows and the life-cycle costs columns to be expanded or contracted to expose or consolidate detail as the user requires.

4.1.1 Cost estimation structure (CES)

The CES is broken into three major groups: physical protection path elements; support systems; and audits and assessments. The CES for the path elements group is defined by the ASD and by some supporting details in the Facility Module of ASSESS. ASSESS does not, however, define all the elements of a physical protection system that incur costs directly attributable to the security function. These additional costs are accounted for in the CATSS model as support systems (infrastructure) costs and assessments costs. Examples of support systems are: all the credentials functions from issuing clearances to issuing badges; all escorting of uncleared visitors and labor; all security awareness training; protective and response force manpower and associated training; and all security systems engineering. The third group, assessments, includes all assessments, from internal security assessments through DOE audits. Because these activities are carried out to assure security, the costs of these activities are attributable to security.

The structure of the CES allows every aspect of life-cycle costs to be identified for each path element and to then be aligned with path-element performance metrics as illustrated in the lower center of Figure 1. It is not, however, necessary to fully populate the Summary Costs Output worksheet to develop useful comparisons of cost and performance of alternatives.

4.1.2 Life-cycle costs

The life-cycle costs are broken into four major categories: acquire and install, operate, maintain, and dispose. For convenience, columns reporting 5 and 10 year cumulative costs are also included.

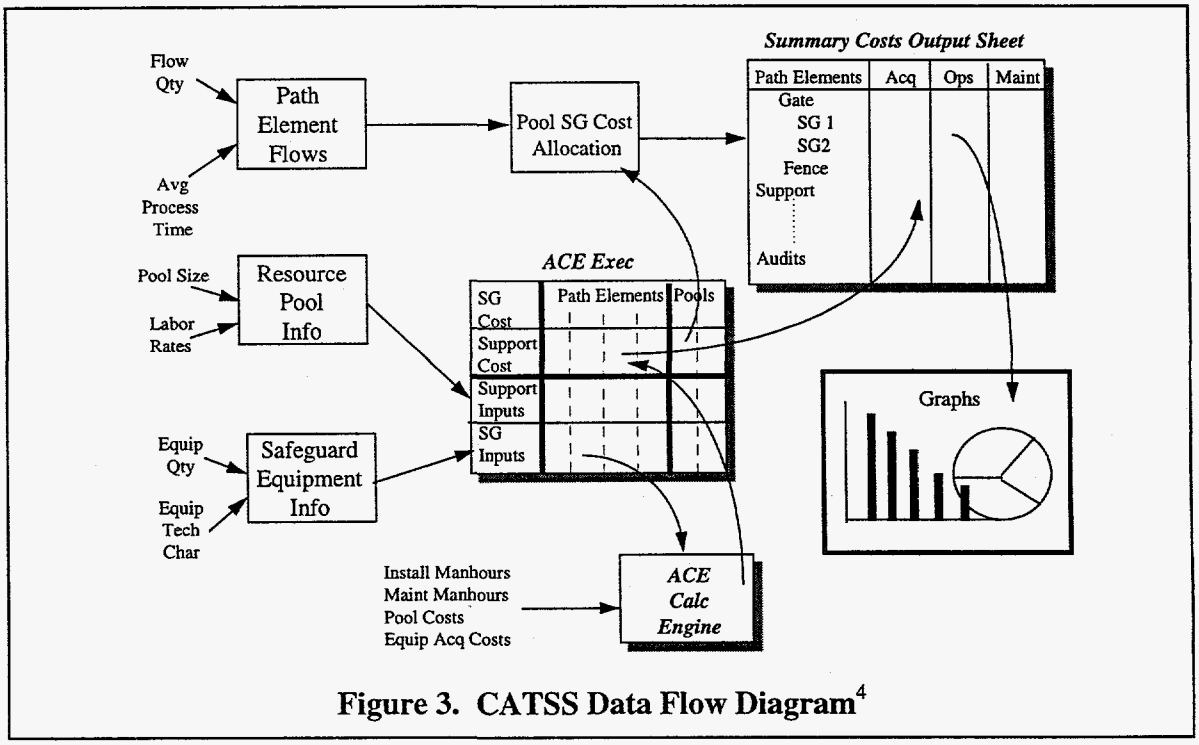

Figure 3. CATSS Data Flow Diagram[4]

Within each life-cycle category, total costs within the category are further broken down into costs of labor (reported in both hours and dollars) and materials.

Under acquisition and installation, materials costs are the procurement costs of the components of the physical security system. Acquisition and installation labor costs are the loaded costs for labor and all necessary equipment to support that labor.

Labor for annual average operating costs can be drawn from one of two labor pools: Security Inspectors or MC&A (Material Control and Accountability). For operational costs, both labor hours and labor dollars are reported for each of these labor pools. Material costs for operations are allocated to labor hours and then to path elements according to the allocation of labor hours to path elements.

Labor for annual average maintenance is drawn primarily from a single labor pool: the technical security labor pool.

This breakout of labor costs by category and task times by labor category supports activity-based cost (ABC) estimation at the path elements.[5]

Life-cycle costs can be grouped as: 1) non-recurring costs; that is, acquisition and installation costs, and 2) recurring costs; that is, operations and maintenance costs. Disposal costs can be either: 1) non-recurring; that is, disposal occurs only upon termination of the system or element; or 2) recurring; such as a component with a very limited life and significant disposal costs, which must be replaced several times over the useful life of the system. The CATSS model allows decision makers easy access to the relationships between non-recurring and recurring costs and their relative significance over time as illustrated in the upper left of Figure 1.

4.2 CATSS input worksheets

There are three major types of input worksheets: 1) Facility, 2) Personnel, and 3) Access-Control Flow.

There is one Facility input worksheet in each CATSS workbook. Although it is not required, this is the logical place for the costs analyst to start. While the path element portion of the CES can be extracted from ASSESS, ASSESS only identifies components by type, not by number or dimension. The Facility Input worksheet is designed to take the system definition for ASSESS and then allow the analyst to provide additional definitions of facility hardware and structures, such as length of fences or numbers of gates.

There is also only one Personnel input worksheet in each CATSS workbook. The current implementation allows for three types of personnel or labor: Security Inspectors (SI), Material Control and Accounting (MC&A), and Technical Security (who maintain the sensor systems.) Labor within each of these three groups is further divided into direct and indirect (support or administrative) labor. This worksheet allows analysts to enter the mix of these labor categories (numbers of management and staff); to enter the loaded labor costs; and to enter the average percentage of paid overtime and the associated overtime premium. The labor required to support activities, such as posted assignments, access control functions, and material flow functions, at path elements is drawn from the SI and MC&A labor pools.

There are as many Access Control Flow sheets in the workbook as there are access control path elements in the ASD. The average annual traffic into and out of each layer through the associated type of path element is recorded on this sheet by type of traffic (e.g., pedestrian, driver, vehicle, etc.). If ASSESS reports a posted SI then this worksheet must show the number of SI's posted during all facility conditions (e.g., open and closed). Time required by SI and MC&A labor to execute every security procedure carried out at the path elements is recorded on these Flow worksheets. Labor hours required to support these activities are then determined by the time required to complete a procedure, multiplied by the average number of times that procedure is executed annually, as defined by the traffic. If the size of the labor pool is not large enough to support path element requirements, then the appropriate row in the support system section of the Summary Costs worksheet will show negative cost and negative labor hours.

CATSS tracks labor hours and labor costs at a level of detail that provides considerable insight into the costs of operations.

4.3 CATSS interface worksheet

Data from the three types of input worksheets are sent to a hidden labor-allocation process and to a visible ACE*EXECUTIVE interface worksheet. This interface worksheet maps multiple safeguards and multiple occurrences of single safeguards to the various path elements. The functions of these worksheets are transparent to the user.

4.4 ACE — the computational engine in CATSS

ACE, a cost analysis tool developed by Tecolote Research, Inc. for the DOD, is the computational engine of CATSS. ACE is the repository for cost constants, cost variables, cost estimation relationships (CERs), and pointers to their supporting documentation. ACE allows costs for multiple manufacturers of a single type of safeguard to be catalogued and supports the estimation of acquisition costs that are phased over time with the effect of inflation included.

5. FUTURE WORK

CPA is in the very early stages of development. Next steps in the development of this tool fall into two major categories: 1) full implementation of what has been prototyped; and 2) expansion beyond prototype design. The following tasks fall under the first category: make the interface from ASSESS to PERFORM robust; expand the automated data post-processing in PERFORM to include methods of defeat, automate the launching of CATSS through EXTRACT, and fully populate the cost data base. Tasks that fall under the second category, expansion beyond the prototype design, include: interfaces to performance analysis tools other than ASSESS; explicit linking between the costs of infrastructure and system performance; and automated analysis of multiple alternatives.

6. SUMMARY

The architecture for CPA, a prototype integration of existing PC-based cost and performance tools for physical security systems, has been presented and the functions and capabilities of its various components have been reviewed. Although this new tool was developed to support definition of a physical protection benchmark, potential applications are numerous. A few examples of potential applications are planning and management of operations, evaluation of both technology and policy alternatives, and development of quantitative requirements for technology improvements.

7. ACKNOWLEDGMENTS

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

8. REFERENCES

1. J. C. Matter, R. A. Al-Ayat & T. D. Cousins, "A Demonstration of ASSESS—Analytic System and Software for Evaluating Safeguards and Security," *Proceedings of the INMM 30th Annual Meeting,* Orlando, FL, July 1989.

2. B. H. Gardner, Mark K. Snell & William K. Paulus, "Comparison of ASSESS Neutralization Module Results with Actual Small Force Engagement Outcomes," *Proceedings of the INMM 32nd Annual Meeting,* New Orleans, LA, July 1991.

3. Byron H. Gardner, William K. Paulus & Mark K. Snell, "Determining System Effectiveness Against Outsiders Using ASSESS," *Proceedings of the INMM 32nd Annual Meeting,* New Orleans, LA, July 1991.

4. David Yates, William H. Jago, Alan W. Phillips, *Cost Analysis Tool for Security Systems (CATSS), CR-0839*, Tecolote Research, Inc., 30 September 1996.

5. Dr. Dennis Togo & Dr. Alistair Preston, "Activity-Based Cost Analysis of Security Services for a Nuclear Materials Site," prepared by Robert O. Anderson School and Graduate School of Management for Sandia National Laboratory under Contract No. DE-AC04-94ALL85000, December 16, 1996.