CONF-890736--10

A Demonstration of ASSESS—Analytic System and Software for Evaluating Safeguards and Security

J. C. Matter
Sandia National Laboratories,* Albuquerque, NM 87185
R. A. Al-Ayat
Lawrence Livermore National Laboratory,† Livermore, CA 94550
T. D. Cousins
Department of Energy, Office of Safeguards and Security
Washington, D.C. 20545

SAND--89-1605C

DE89 014803

ABSTRACT

This paper demonstrates the use of the Analytic System and Software for Evaluating Safeguards and Security. ASSESS is an integrated approach for evaluating the effectiveness of safeguards against theft of special nuclear material by different types of adversaries: insiders, outsiders, and colluding insiders and outsiders. ASSESS consists of six modules: System Manager, Facility Descriptor, Insider Analysis, Outsider Analysis, Neutralization Analysis, and Collusion Analysis. This paper introduces the modules, describes their scope, and highlights the interactions among them. Separate papers will provide detailed discussion and demonstration of each of the modules. The ASSESS code runs on the IBM PC family of computers with 640K RAM, the DOS operating system, and Microsoft Windows. The Windows environment provides a very efficient and convenient graphics user interface as well as drivers for many types of output devices. ASSESS is being developed jointly by Lawrence Livermore National Laboratory and Sandia National Laboratories under the sponsorship of the Department of Energy (DOE) Office of Safeguards and Security. The first version of the ASSESS code was delivered to DOE/OSS in March 1989.

INTRODUCTION

ASSESS (Analytic System and Software for Evaluating Safeguards and Security) is an integrated software package for evaluating system effectiveness against theft of special nuclear material by a spectrum of adversaries: outsiders, insiders, and an insider colluding with outsiders. A preliminary paper describing this new product was presented at the INMM Annual Meeting in 1988 [1]. This poster paper presents a demonstration of the ASSESS V1.0 software delivered to the US Department of Energy's Office of Safeguards and Security (DOE/OSS) in March 1989. The ASSESS software package is written in the C language and runs on personal computers (IBM compatible) using the Microsoft Windows environment. This paper will focus on the interaction and relationship among the six modules in the ASSESS package: Manager, Facility, Insider, Outsider, Neutralization, and Collusion [Figure 1].

ASSESS includes new capability not available in the ET and SAVI analysis packages currently being used at DOE's nuclear facilities. An integration system manager controls flow between modules, aids planning of the site analysis, and performs file management of the input data and evaluation results. A facility descriptor is used to specify the site's physical configuration, target attributes, and safeguards system for all analyses. The probability of detection for each nonviolent insider adversary type is calculated using a reference database of adversary attributes, defeat methods, strategies, and detection performance. Probability of interruption is calculated for an outsider threat spectrum of terrorists, criminals, psychotics, and extremists. The probability of neutralization of violent adversaries is calculated using a small force engagement attrition model. A probability of system win is calculated for uncorrelated handoff of theft material by various insiders in collusion with outsiders. This paper focuses on the software, and a complementary paper describes the models, the calculations performed, and the results generated by ASSESS [2].

COMPUTING REQUIREMENTS

To gain acceptance by safeguards and security analysts, ASSESS was designed to use on personal computers (IBM compatible), provide easy-to-use human interfaces, and allow a wide variety of output devices (displays, printers, plotters).

Hardware

The following generic hardware is recommended for use with ASSESS:

- 80286 or 80386 personal computer
- 80287 or 80387 math coprocessor
- 640K RAM or expanded memory

*This work was supported by the United States Department of Energy under contract DE-AC04-76DP00789.

†This work was supported by the United States Department of Energy under Contract W-7405-ENG-48.

ANALYTIC SYSTEM AND SOFTWARE FOR EVALUATING SAFEGUARDS AND SECURITY

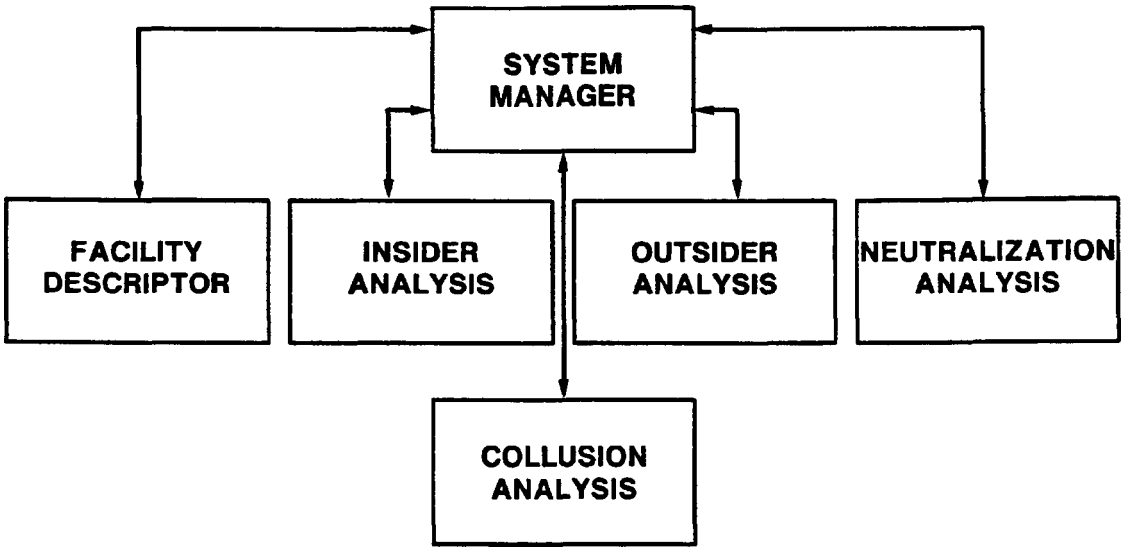

Figure 1. ASSESS block diagram

- removable hard disk
- color monitor
- EGA or VGA graphics adapter card
- mouse pointing device

Software

The following software is needed to run ASSESS:

- DOS operating system V2.0 or later
- Microsoft Windows V2.0 or later (Note: Windows/386 is used with an 80386 PC.)

SYSTEM MANAGER

The System Manager performs or provides three functions for the user:

- Control – facilitates and controls movements among the six ASSESS software modules;
- Planning – provides a spreadsheet for planning analyses and summarizing status; and
- File Management – assists in file retrieval and saving for each module and in tracking the associated site analysis file set.

An example of the main Manager screen is shown in Figure 2. User interaction with the Manager module is performed using its menu structure:

File	Edit	Applications	Help
New	Cut	Facility	
Open	Copy	Insider	
Save	Paste	Outsider	
Save As	Clear	Collusion	
Print		Neutralization	
Printer Setup			
Merge	Insert File		
	Delete File		
Exit			
About Manager	Show Info		
About ASSESS			

The use of this menu to accomplish the manager functions is discussed in the next three sections.

Control Function

The Applications pull-down menu is used to select any of the other five ASSESS modules. Before selecting an application from the menu, the analyst can use the mouse to preselect a file from the Manager screen to be used in the selected application. To return to the Manager module and its spreadsheet screen from any application, the user selects the Exit option in the File menu of that application module.

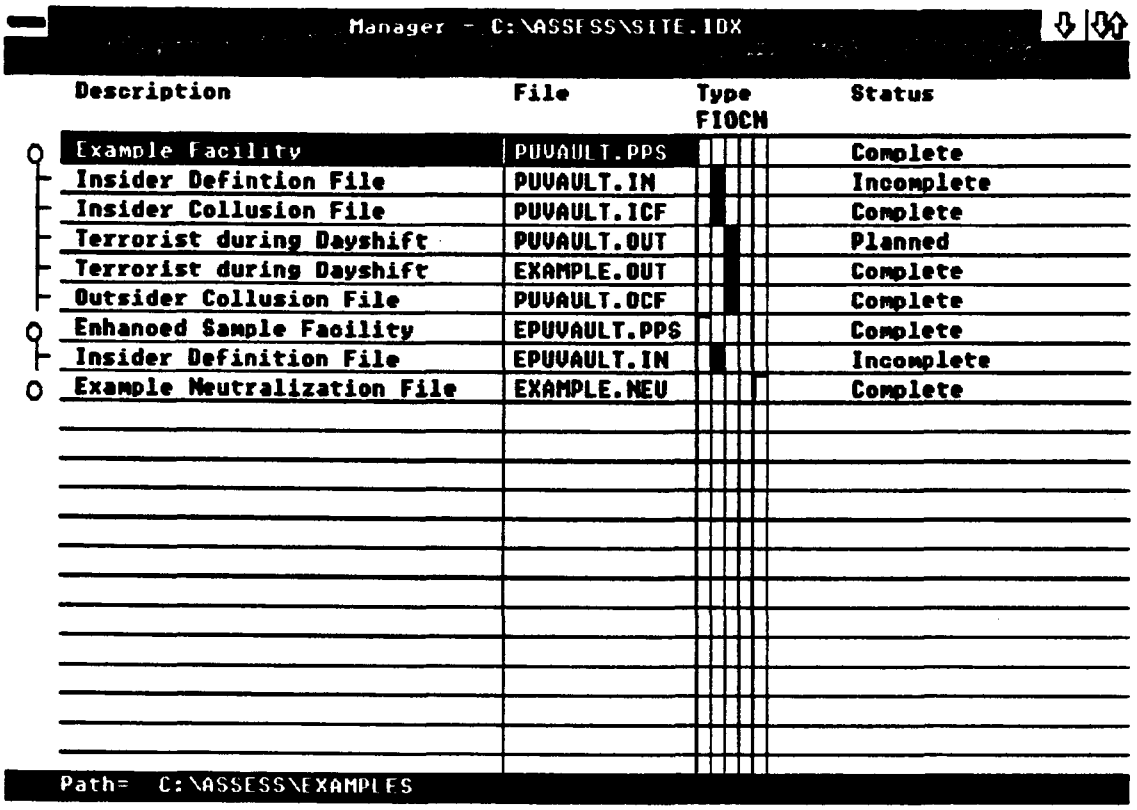

Figure 2. Manager spreadsheet screen

Planning Function

The planning of a site analysis is assisted by using the spreadsheet screen provided by Manager. The information associated with this screen is saved by Manager in an index file (.IDX). Several categories of file information are presented on the screen (see Figure 2): Description, File, Type, and Status. The information on this screen is composed using the Manager Edit menu. The user specifies the type (corresponding to one of the other five application modules), filename, and description. The filename extension must be consistent with the file type: .PPS for Facility, .IN for Insider, .OUT for Outsider, .COL for Collusion, and .NEU for Neutralization.

Symbols to the left of the file description designate whether it is a base file or a dependent file. A base file (marked by large dot) is either a Facility file (.PPS) or a Neutralization file (.NEU). A dependent file (marked by line branch) is associated with a particular base file and can be Insider (.IN, .ICF), Outsider (.OUT, .OCF), Collusion (.COL), or Neutralization (.TYP) files. (Note: .ICF, .OCF, and .TYP are files created by the Insider, Outsider, and Neutralization modules, respectively, and are tracked by Manager.)

Manager tracks the status of each file: Planned, Complete, Incomplete, or Obsolete.

- Planned – file has been inserted in the index, but has not been saved by its application module.
- Complete – base file that is done or updated, or dependent file with results computed since base file has been updated.
- Incomplete – base file that is not done, or dependent file that is not complete for its original base file.
- Obsolete – dependent file that has not been completed (recalculated) since its base file was modified.

A new analysis starts with a blank spreadsheet on which the user adds files by means of the Edit menu. The Edit menu is also used to delete files and change file descriptions. This information is saved in the site index file (SITE.IDX) by default, or it can be renamed by the user with the same filename extension. Manager also tracks and displays, at the bottom of the spreadsheet screen, the file path directory where a given (selected) file was saved by its application module.

File Management Function

The file management function of System Manager consists of three parts.

First, as mentioned in the control function description, files can be preselected from the spreadsheet screen before an application module is opened.

Second, as mentioned in the planning function description, file status is tracked when an application is run. File status will change for the following conditions:

- Creation – Saving a new file in an application will add it to the site index with a status of either Complete or Incomplete.
- Review – An Obsolete file status will be changed to Complete or Incomplete when it is saved again after a session in its application.
- Results calculation – An Obsolete or Incomplete file status will be changed to Complete when it is saved after calculation of results in its application module.

Third, the file management function assists the user in retrieving or saving files in the application modules. This is done by providing Open and Save As dialog boxes in each module. As shown in Figure 3, the Open dialog box allows the user to select a file from the current site index (from the left list box) or to select a file from the current path or other subdirectories and drives. As shown in Figure 4, the Save As dialog box allows the user to save a file with either a default name or a new name (which will be inserted in the site index file) and in either the current path or a new subdirectory.

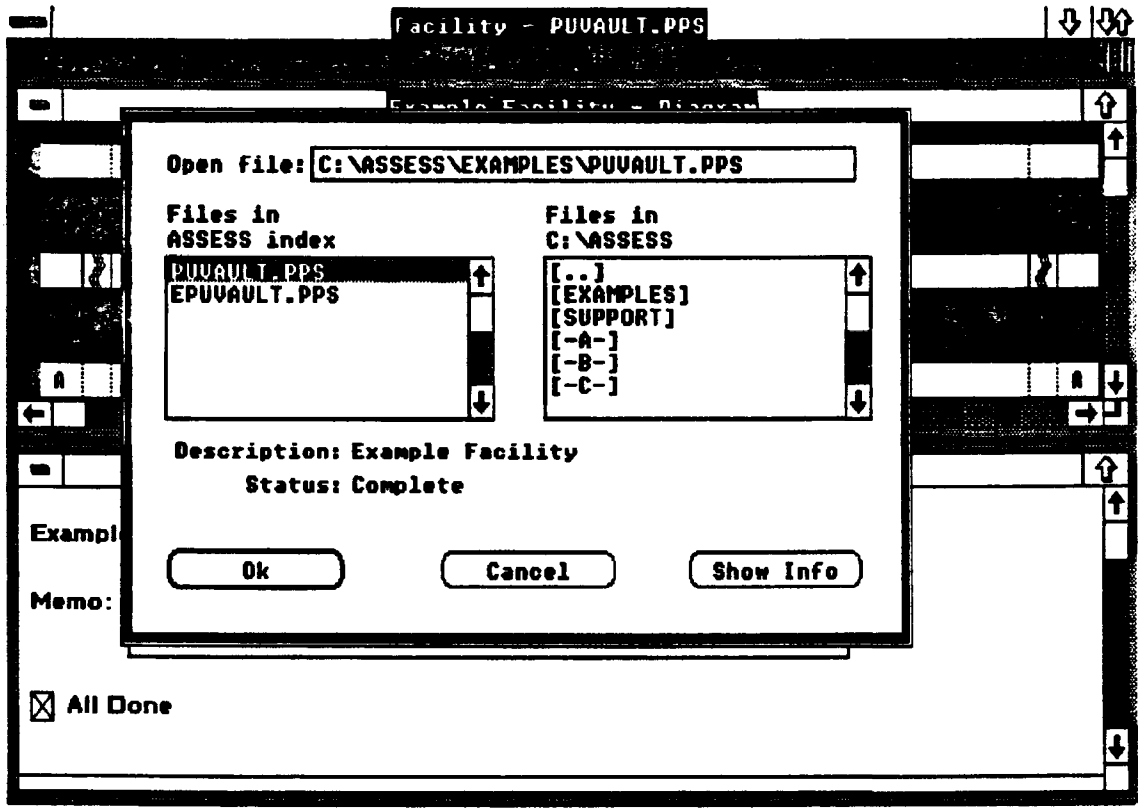

Figure 3. Application Open dialog box

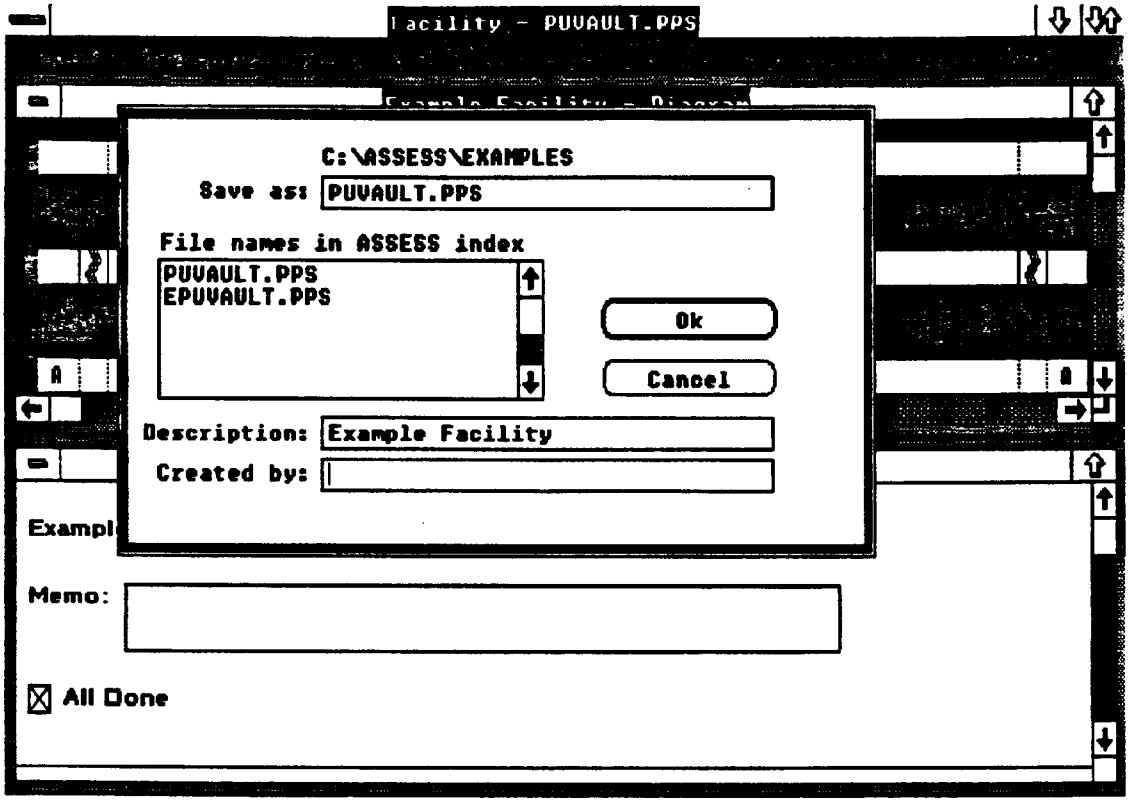

Figure 4. Application Save As dialog box

FACILITY DESCRIPTOR

The Facility module is used to describe the site configuration, target attributes, and safeguards components and procedures for two operational facility states. The site configuration establishes the adversary sequence diagram. Attributes, components, and procedures are defined using an internal database and report windows. User-defined component performance for outsider analysis is defined in Facility.

The Facility module is accessed from the System Manager using the Applications pull-down menu. Either a new facility description is entered using the Facility File New option, or an existing facility description is reviewed or modified using the Facility File Open option. Facility data are stored in .PPS files using the Facility File Save As option.

The Facility Descriptor module is described further in Reference 3.

INSIDER ANALYSIS

The Insider module is used to describe the insider personnel categories, their associated access and authority, and multilayer defeat strategies. Insider analysis results for Probability of Detection are presented by graphs and tables for overall PD summary by personnel type and detail for paths, areas, path elements, and strategies. User-defined element performance for insider analysis is defined in Insider.

The Insider module is accessed from the System Manager using the Applications menu. A Facility file (.PPS) is needed by Insider to conduct an analysis; this file is either preselected in Manager or selected using the Insider File menu. Insider results are stored in .IN files using the Insider File Save As menu option. Collusion data are stored in .ICF files using the Insider File Save Collusion Data option.

The Insider Evaluation module is described further in Reference 4.

OUTSIDER ANALYSIS

The Outsider control panel is used to define the threat type, response strategy, intrusion methods, facility state, and response force time range. Outsider analysis results for probability of interruption, detection potential, and time remaining after interruption are presented for the ten most vulnerable Paths by path displays, path detail listings, and vulnerability and sensitivity graphs. Neutralization results are combined with Outsider results to provide probability of system win.

The Outsider module is accessed from the System Manager using the Applications menu. Either a Facility file (.PPS) or an Outsider file (.OUT) is needed by Outsider to conduct an analysis. One of these files is opened using

either the Outsider File New option (.PPS) or the Outsider File Open option (.OUT). For each adversary type, outsider results are stored in an .OUT file using the Outsider File Save As option. Outsider collusion results are automatically saved to an .OCF file with the same filename as the active .PPS file when the Outsider File Save Collusion Data option is selected. Outsider collusion data are appended to this outsider collusion file for each adversary type and operational state with the same facility file (.PPS). If the .OCF file already contains data for that adversary type/operational state, then the new data replace the old.

The Outsider Analysis Module is described further in Reference 5.

NEUTRALIZATION ANALYSIS

The Neutralization module is used to describe the engagement event parameters and individual combatant parameters. User guidance windows are provided to assist the analyst in determining the active number of combatants per side. A library of combatant types is available and can be added to by the user. Neutralization results present the Probability of Neutralization with time function and sensitivity study graphs.

The Neutralization module is accessed from the System Manager using the Applications menu. The small-force engagement is modeled in Neutralization and does not use a Facility file (.PPS). A new engagement description is created using the Neutralization File New option, and an existing engagement description is retrieved using the Neutralization File Open option. Neutralization results are stored in .NEU files using the Neutralization File Save As option. These files may also be accessed by the Outsider module to retrieve Probability of Neutralization results to combine with Probability of Interruption calculations to obtain Probability of System Win numbers. The analyst must correlate response-force time data input to the Outsider and Neutralization modules to obtain consistent System Win results. Neutralization also stores user-defined individual combatant parameter date in .TYP files.

The Neutralization module is described further in Reference 6.

COLLUSION ANALYSIS

The Collusion Analysis module is used to select the insiders and outsiders to be considered in the collusion analysis. Collusion results are Probability of System Win with tabular or graphical displays sorted by most vulnerable insider-outsider combinations, insiders, or outsiders. Path detail information includes the handoff area.

The Collusion module is accessed from the System Manager using the Applications menu. To calculate handoff collusion results, three input files are needed by this module: a Facility file (.PPS), an Insider file (.ICF), and an Outsider file (.OCF). These necessary files are obtained by using either the Handoff File Load options or the Collusion File Open Handoff option. Handoff collusion results are stored in .COL files using the Handoff File Save As option.

The Collusion module is described further in Reference 7.

SUMMARY

ASSESS V1.0 is a new modular, integrated software package for use on personal computers to help evaluate the effectiveness of safeguards and security. The site configuration, targets, and safeguards are modeled with the Facility module. The Insider, Outsider, Neutralization, and Collusion modules calculate system effectiveness against a nonviolent insider (detection), outsiders (interruption and neutralization), and insiders colluding with outsiders (handoff). This paper has focused on the System Manager, which integrates the other five modules through its functions of control, planning, and file management. Thus ASSESS provides new personal computer capability for the vulnerability assessment function.

REFERENCES

1. "Overview of the Integrated Vulnerability Assessment Tool," R.A. Al-Ayat, T.A. Renis, J.C. Matter, and A.E. Winblad, INMM 29th Annual Meeting Proceedings, 1988.

2. "An Overview of ASSESS – Analytic System and Software for Evaluating Safeguards and Security," T.D. Cousins, R.A. Al-Ayat, and J.C. Matter, INMM 30th Annual Meeting Proceedings, 1989.

3. "The ASSESS Facility Descriptor Module," Sabina Erteza Jordan, Alfred Winblad, Brad Key, Scott Walker, Therese Renis, and Richard Saleh, INMM 30th Annual Meeting Proceedings, 1989.

4. "A Comprehensive Method for Evaluating Safeguards Against the Insider Threat," R.A. Al-Ayat, T.A. Renis, R. Saleh, and C.J. Patenaude, INMM 30th Annual Meeting Proceedings, 1989.

5. "The ASSESS Outsider Analysis Module," Al Winblad, Mark Snell, Sabina Erteza Jordan, Bryan Bingham, Brad Key, and Scott Walker, INMM 30th Annual Meeting Proceedings, 1989.

6. "The ASSESS Adversary Neutralization Module," Bill Paulus, Sabina Erteza Jordan, Martha Moore, and Junko Mondragon, INMM 30th Annual Meeting Proceedings, 1989.

7. "Hand-off Collusion Module of the ASSESS Program," D.S. Fortney, W.A. Romine, and M.K. Snell, INMM 30th Annual Meeting Proceedings, 1989.