

REFERENCE COPY
C.2

SANDIA REPORT

SAND91-2498 • UC-706

Unlimited Release

Printed January 1992



SAND91-2498
0002
UNCLASSIFIED

01/92
35P STAC

The Benefits of Automation in a Site Information Network

David R. Ek

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-76DP00789

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: 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, nor any of their contractors, subcontractors, or 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, any agency thereof or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
Office of Scientific and Technical Information
PO Box 62
Oak Ridge, TN 37831

Prices available from (615) 576-8401, FTS 626-8401

Available to the public from
National Technical Information Service
US Department of Commerce
5285 Port Royal Rd
Springfield, VA 22161

NTIS price codes
Printed copy: A03
Microfiche copy: A01

The Benefits of Automation in a Site Information Network

David R. Ek
Survivability and Security Systems Division
Sandia National Laboratories
Albuquerque, New Mexico 87185

Abstract

This study examines how automation can benefit several nuclear weapon surety programs. The benefits expected are timesavings, improved management across programs, and new ways of interpreting data. The types of data managed and the data flow paths for twelve programs are identified. We believe that automation will make it possible to gain new insights into the nuclear weapon surety status. Though we recognize that there are obstacles to overcome, we recommend the development of a Site Information Network.

Sponsored by the Defense Nuclear Agency under IACRO 90-881

Contents

1. Introduction.....	5
2. Value of Automation/Integration.....	5
3. Summary of Studied Security Programs.....	6
4. Methodology.....	7
5. Results of the Study.....	11
6. Obstacles to Overcome.....	12
6.1 Procedural/Political Organization.....	12
6.2 Communication.....	13
6.3 Security Issues and Need-to-Know.....	14
7. Conclusions and Recommendations.....	15
7.1 Conclusions.....	15
7.2 Recommendations.....	15
Reference.....	16
Appendix: Nuclear Surety Programs and Activities.....	17
Tables	
1 Measurable Values Vs. Benefits.....	9
2 Types of Data Managed.....	9
3 Relative Usefulness of Data in Security Programs.....	10
4 Relative Importance of Access Time of Data in Security Programs in an Emergency Environment.....	11

The Benefits of Automation in a Site Information Network

1. Introduction

Sandia National Laboratories undertook a study to determine the benefits of automation to several nuclear weapon surety programs in conjunction with the Site Information Network prototype project. The goals of the study, as outlined in the Statement of Work, were to:

- Understand current management of security programs
- Assess the value that automation might have for each program
- Determine the benefits that would result from combining the information from all of the study programs into an integrated database.

Our approach was to develop the methodology and perform the work to achieve the second and third goals above (i.e. to assess the benefits of automation in a stand-alone and integrated environment).

2. Value of Automation/Integration

Computer technology has been responsible for dramatic improvements in the workplace. These improvements range from scientific computation and modeling to information management and analysis, and finally to report and letter composition. This value is derived from the computer's ability (versus man's relative inability) to store, retrieve, and perform analytical operations on large quantities of data and to do it quickly. Additionally, advances in communication technology have multiplied the advantages of computer automation by increasing the accessibility to the data.

The fusion of the computer and communication technologies would benefit nuclear surety management. Furthermore, the impact of automation to surety information management could be increased several fold as data from many related surety programs were integrated into a single data system. With such a system, a question involving information from several different programs could be answered quickly by a single person

with a single database query. Currently, this task requires that several different people, perhaps housed in different locations, rummage through their files. The result of automated management would be that the artificial boundaries between programs within the surety umbrella would disappear, and this would yield a broader, more accurate, and more complete view of nuclear surety at a moment's notice.

This could all be achieved by using relatively low-cost computer hardware; data processing, communication and presentation software; and a digital network to transmit the information. A system such as this, along with its benefits, was visualized in our Future Look report, "Information Technologies to Enhance Survivability and Security."¹

3. Summary of Studied Security Programs

For the purposes of the study, a cross section of nuclear surety programs and activities were selected. This cross section appears to represent the breadth of surety programs at USEUCOM; these programs should provide a good basis for evaluating the benefits. The programs are listed below with a short description. For more information, see the Appendix to this report.

1. WAIVERS AND EXCEPTIONS: Management of security requirement deviations.
2. PAL INFORMATION MANAGEMENT: Management of nuclear release codes.
3. RECAPTURE/RECOVERY SITE FOLDERS: Site Imagery.
4. INSIDER PROTECTION: Deterrence or detection of insiders.
5. ENTRY CONTROL/ACCESS CONTROL: Site entry tracking
6. SITE VISITS: Communication and monitoring of site visits and requests
7. FORCE-ON-FORCE TRAINING: Required training activity.
8. WEAPON INVENTORY: Nuclear weapon stockpile monitoring.
9. WEAPON MOVEMENTS: Tracking planned movement of nuclear weapons.

10. SECURITY SYSTEM MAINTENANCE: Managing maintenance of security sensors.
11. PERSONNEL RELIABILITY PROGRAM (PRP): Tracking personnel assigned to nuclear weapons.
12. CUSTODIAL UNIT STATUS REPORT (CUSR): Summary of site security status.

4. Methodology

Through quantifiable, objective metrics (such as time and manpower savings), assessing value and determining benefit would be a relatively straightforward effort of comparing numbers. Without a metric, the methods of evaluation are much more subjective, because they are based on the qualitative comparisons like "better" and "worse." The value and benefit of surety program automation is not obviously quantifiable due to the lack of empirical data.

In order to mitigate the subjectivity of the evaluation of values and benefits, a methodology for the study will be developed. This methodology will attempt to relate the benefits of automation to measurable quantities. These benefits can be categorized as follows:

- Timesavings by reducing clerical tasks related to data processing and communication
- Improved management through improved access, accuracy, and presentation of surety data
- Benefits identified as new capabilities would be uncovered and could result in fundamental changes in the way data is managed and interpreted.

The last of these benefit categories, although it often has the greatest long-term impact, is also the one which cannot be predicted. Because it cannot be predicted, it will be ignored in our study. However, the first two benefits, which are believed to be predictable, can be further defined. The list below divides the first benefit category into two parts and the second into three parts.

Timesavings

- Less time required to summarize the data
- Less time necessary to communicate data or to remotely access data

Improved Management

- Improved analysis of data
- Standardized organization and storage of data
- Synergistic increase in information resulting from data interrelationships.

From the program data listed in the Appendix, several measurable attributes are available:

- Types and amounts of data managed
- Reporting required
- Offices/commands interested in the data.

By comparing the potential benefits of automation with these measurable attributes, some understanding of the relationships between the two can be seen. Table 1 presents the correlation between the measurable attributes and the benefits.

The highest correlation to the benefits is the types and amounts of data managed in the various programs; this attribute will be a good indicator of the degree of benefit each receives from automation. Therefore, the data managed will be used as the program criteria on which the benefit is based.

The next step is to identify the types of data managed in the various studied security programs. Table 2 summarizes the information contained in the Appendix.

Table 1. Measurable Attributes Vs Benefits

(H = High Correlation M = Medium Correlation L = Low Correlation)

<u>Benefits</u>	<u>Data Managed</u>	<u>Reporting Required</u>	<u>Offices/ Commands</u>
Summary Time	H	H	L
Communication Time	L+	L+	H
Data Analysis	H	M	L
Data Storage	H	L+	L
Synergistic Effects	H	M	L

Table 2. Types of Data Managed

1. Site Identification and Location
2. Command Structure
3. Security Requirements, Deviations, and Compensatory Measures
4. Delivery Unit
5. Weapon Inventory
6. Weapon Movements
7. Regional Maps
8. Site Layouts
9. Site Images
10. Security Force Information
11. Regional Logistics Data
12. Personnel Data
13. Personnel Clearances
14. Visit Information
15. Weapon Data
16. Weapon Operational Status
17. Weapon Maintenance Performed
18. PRP Information
19. Communications Data
- *20. Personnel Movements Intra-Site
- *21. Weapon Movements Intra-Site
- *22. Personnel Biometric Data
- *23. Exercise Information
- *24. Security System Information
- *25. Security System Maintenance Information

*Numbers 20 through 25 are not currently required by any program, but are data with possible additional benefits.

Finally, we 1) develop a matrix of the types of data managed (from Table 2) versus the studied security programs (from Section 3), and 2) determine how useful the data is to the program. This is done in Table 3, using the following criteria:

- Data type currently required by the program: R
- Data type closely related or useful to the program: U.

Table 3. Relative Usefulness of Data in Security Programs*

Type of Data	<u>Security Program</u>												
	<u>WX</u>	<u>PAL</u>	<u>R/R</u>	<u>Insid</u>	<u>Entry</u>	<u>Visit</u>	<u>Train</u>	<u>Invtr</u>	<u>Move</u>	<u>Scrtv</u>	<u>PRP</u>	<u>CUSR</u>	
1	R	R	R	U	R	R	U	R	R	U	R	R	12
2	R	U	U		U	U					U	U	7
3	R		U	U			U			U		U	6
4		R										R	2
5		R	U	U				R	U			U	6
6		R	U	U				U	R				5
7			R			U	U		U			U	5
8	U		R	U			U			R		U	6
9	U		R	U		U			U	U		U	7
10	U		R				U					R	4
11			R				U					R	3
12				U	R	R			U		R		5
13				U	R	R				R			4
14						R			U				2
15	U	U	U				U	R	R			R	7
16		U	U					R	R				3
17			U					R			U		3
18				U			U				R		3
19		U										R	2
20											U		2
21				U				U					2
22				U	U	U			U			:	4
23	U		U				U						3
24	U		U	U						U		U	5
25	U			U						U			3
	60	44	82	70	32	46	49	36	53	42	33	72	

*The meaning and interpretation of the numbers at the ends of the rows and columns in this table will be explained in Section 5 below.

All data types should not carry the same weight. One of the benefits that automation affords is decreased access time. It stands to reason that those programs in which access time is or can be critical (e.g. in a nuclear incident/accident) could benefit an extra degree from automation. Table 4 lists selected data types from Table 2 and places a relative ranking of the importance of immediate access in an emergency environment.

Table 4. Relative Importance of Access Time of Data
In Security Programs in an Emergency Environment

<u>Types of Data</u>	<u>Incident/ Accident</u>
Site Identification and Location	M
Command Structure	L
Deviations/Compensatory Measures	M
Delivery Unit	L
Weapon Inventory	H
Weapon Movements	M-H
Regional Maps	M
Site Layouts	H
Site Images	H
Security Force Information	H
Regional Logistics Data	M
Personnel Data	M
Personnel Clearances	L
Visit Information	L
Weapon Data	H
Weapon Operational Status	L
Weapon Maintenance Performed	L
PRP Information	L
Communication Data	H

5. Results of the Study

From Tables 3 and 4, we can draw five results.

Result 1. The existence of multiple "R" entries in any row in Table 3 implies that data is concurrently being managed by more than one program, and that therefore a manpower/time savings can be realized by eliminating this redundant management. Of the data types listed, those redundantly managed include Site ID and Location, Site Layout, Weapon Data, Personnel Data, and Personnel Clearances.

Result 2. The existence of "U"s down columns in Table 3 gives a measure of the degree of benefit that any program might realize through integration of data from other programs. This benefit would manifest itself in

improved surety decisions as a result of improved information available. Recapture/recovery site folders and insider protection show the most benefit in an integrated environment.

Result 3. The number of "R"s and "U"s in rows (i.e., the numbers at the end of the rows in Table 3) gives a measure of the value that certain data types add in an integrated environment. Those data types that appeared to be most useful include: Site ID and Location, Command Structure, Security Requirements Deviations and Compensatory Measures, Weapon Inventory, Site Layouts, Site Images, and Weapon Data.

Result 4. By assigning a weighted value to each data type equal to the number of "R"s and "U"s in its row and then summing these weighted values along columns (i.e. the numbers at the bottom of the columns in Table 3), a measure of the programs which benefit from commonly managed data can be obtained. This weighting determined that Waivers and Exceptions, Recapture/Recovery, and the Custodial Unit Status Report are most closely managing the same data; Insider Protection, Force-on-Force and Weapon Movements utilized similar data types.

Result 5. Table 4 ranks those data types which benefit from automation whether integrated or not. These include: Weapon Inventory, Weapon Movements, Site Layouts and Images, Security Force Information, Weapon Data, and Communication Data.

6. Obstacles to Overcome

The obstacles below were identified during the investigation and must be overcome in order to implement a Site Information Network:

- Procedural/political organization of security programs within the military
- Communication equipment available for secure communication
- Data security and need-to-know restrictions.

These obstacles are described below.

6.1 Procedural/Political Organization. The data flow path diagrams for each program (see the Appendix) show that the security information which is generated at the site is quickly dispersed throughout the military arena. As a result, there is not a single repository for security information, or a

single office with responsibility for all security information. This leads to a fragmented approach to managing security. The security vision from any office is dimmed by programmatic partitions, narrowly defined job descriptions and limited security responsibility. The result of all of this is an incomplete, and therefore inaccurate, view of security status.

The Site Information Network assumes that there is value in providing a single repository for security information, and that access to a complete set of security data will assist managers of each program at all levels to make better decisions. For this to come about, some changes in the manner in which data is presently managed will need to take place.

6.2 Communication. The movement of electronic data as proposed in the Site Information Network requires that either existing or planned communication hardware be available at each node. The type of hardware depends on the network features desired such as:

- bandwidth
- frequency of network access
- duration of network access
- availability and survivability of network
- security considerations.

At present there are not many classified, moderate bandwidth systems in Europe which could support the SIN. The choices appear to be WWMCCS, DISNET 1, and the STU III phones.

WWMCCS. This World Wide Military Command and Control System is a Top Secret network tying Burroughs nodes to a central host. The bandwidth of the system is 56K bits/s. Due to its classification, access to the nodes is limited and its operation somewhat unfriendly.

DISNET 1 The DISNET 1 is a fairly new, Secret level, packet-switching network with dial-up capability. Access to the network would be from terminals, through leased phone lines to a host. The bandwidth of the network would be limited by the leased phone lines (4800 baud) making imaging difficult (but possible). Encryption is currently accomplished with KY-84 devices. New technologies may simplify this. Operation of the network is maintained by DCA-Europe.

STU-III. The STU-III allows point-to-point Top Secret and Secret communication at low bandwidth (1200 baud) and low cost. Experience has shown that there are problems with the noise on some of the European

phone lines. These problems should be addressed if this communication medium is pursued.

6.3 Security Issues and Need-to-Know

Several issues are of concern in this arena. These include the "Big Brother" concern, unauthorized access to data, circumventing of command channels, and reduction in insider controls.

Big Brother. The concern exists of "Big Brother" watching over the shoulder of the site commanders and program managers. This "concern" also identifies an opportunity, even though some may see the concern as unnecessary micro-management. In previous studies, we have often found that policies get considerably filtered from top to bottom. The goal is to provide a means of getting needed policy rapidly and accurately to the sites. Although it is true that quick access to information is made possible by the network, it is probably incorrect to assume that this access will be detrimental to present stewardship of surety responsibility for the reasons given below.

First. Most managers do not have the time nor the desire to perform another's duty. Access to the data in the system is prompted by real questions or concerns requiring his/her attention.

Second. Permitting questions to be answered without requiring site personnel will save effort.

Third. If there are problems, upper management should be kept informed, rather than left in the dark.

Unauthorized Access. It is possible, through technological means, to provide access to only certain sets of classified data.

Circumventing Command Channels. The network does permit circumvention of command channels (the site can send E-Mail to HQ, HQ can review unapproved information, etc.). However, this ability was not uniquely introduced by the computer, but is also possible with the telephone or facsimile. Procedural requirements which today protect this from occurring could similarly apply to the network. In addition, technological means could be incorporated into the system to discourage or prevent its occurrence.

Insider Concerns Among other reasons for compartmentalizing the data, is the desire to limit the overall knowledge of an insider. Rather than

hinder this effort, the system, through password control and personnel responsibilities, could help identify potential insiders.

7. Conclusions and Recommendations

7.1 Conclusions. Nuclear surety programs would benefit from automation in both a stand-alone and an integrated environment. Some programs benefit from automation in a stand-alone environment because of the time savings and improved management. Waivers and exceptions automation illustrates this. Recapture/recovery site folders would benefit because of the amount of potentially beneficial data and the need for rapid access to the information in an emergency environment. Much of the data currently required by the studied security programs is also required by other programs or is closely related or useful to other programs. For this reason, the greatest benefit of automation is in an integrated environment. The results of this study support this conclusion, yet these results are very conservative because we ignored what are potentially the greatest long-term benefits; we ignored those benefits which are identified as new capabilities and which can result in fundamental changes in the way data is managed and interpreted.

Automation has the potential to gain new insights into the nuclear weapon surety status. We found in the study that no single office has responsibility for all security information. Rather, the information is dispersed throughout the military arena. (See the Appendix for details.) A single repository of all security information or a system which makes the information readily accessible by a single office would allow new insights. These insights could lead to identifying some of the following:

- redundancies and potential cost savings
- undesirable trends which when detected early can be reversed
- root causes which can be addressed rather than dismissed by treating their symptoms
- vulnerabilities not previously identified.

7.2 Recommendations. Develop the site information network. The waivers and exceptions automation project, the Site Information Network prototype project, and the results of this study all argue the benefit to nuclear surety of an automated, integrated security information database

and network. This study serves as a starting point in identifying appropriate programs and data to include in the Network. This effort should continue, ultimately resulting in a system based on the SIN concept.

Reference

- 1 David R. Ek and James R. Caruthers, Future Look. Volume II.E. Information Technologies to Enhance Survivability and Security, Albuquerque, NM: Sandia National Laboratories, June 1991.

**Appendix:
Nuclear Surety Programs and Activities**

Appendix: Nuclear Surety Programs and Activities

1. Waivers and Exceptions

A) Requirements for Data/Purpose of the Program: ACE Directive 80-6 outlines the security requirements for nuclear storage sites in Europe and a plan to monitor non-compliance to these regulations. The waivers and exceptions program documents deviations to security requirements, including the proposed corrective action and interim measures taken to compensate for the created vulnerability.

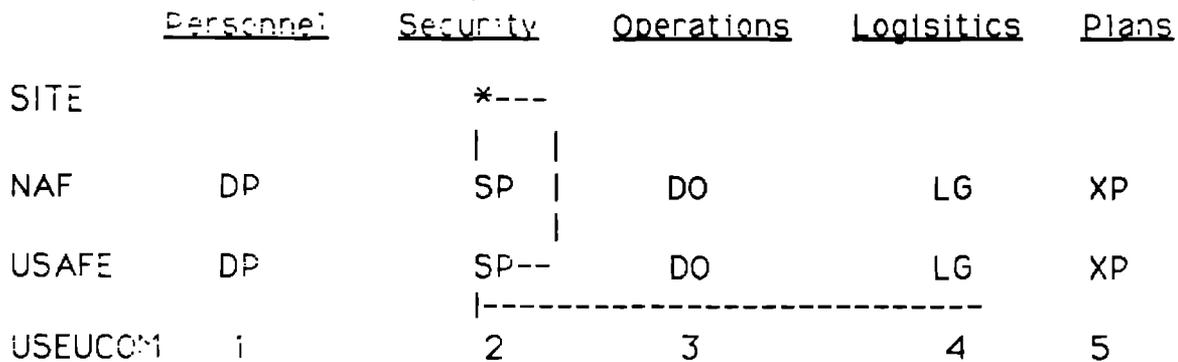
B) Types of Data Managed:

- Site Identification and Location
- Command Structure
- Requirement Deviated/Description of Deviation
- Schedule and Cost of Correction
- Interim Compensatory Measures
- Points-of-Contact and Approvals.

C) Frequency of Data Update/Reporting.

- As Deviations are Identified,
- As Approvals Expire (Annually, Biannually)

D) Data Flow Path.



E) Flow Channels: Data is up and down the flow path through classified mail channels. (Prototype W/X automation moves data with STU III phones.)

F) Perceived Benefits of Automation:

- Quicker/better determination of deviation/compensatory measure. System can help minimize errors in selecting requirement deviated against and appropriate compensatory measures through on-line help.
- Quicker approval of solution
 - Electronic communication of forms can speed up the transmission of 250-R forms.
 - There is better analysis of W/X data. Searches, comparisons, and summaries can be performed on any field or combination of fields in the database.
 - There is better understanding of vulnerabilities. Through the analysis above, a clearer and more complete picture of site security status can be drawn.

2. PAL Information Management

A) Requirement for Data/Purpose of the Program. The PAL code plan is needed for both release and recode. It is contained in the USEUCOM Emergency Action Procedures. Some historical PAL recode data is contained on paper records which accompany the weapon. Should problems arise, the historical data is used for troubleshooting.

B) Types of Data Managed

- Site Identification and Location
- Delivery Unit (Weapon)
- Code Designator

- History of Recode:
 - Reasons for recode
 - From what code designator?
 - To what code designator?

- Weapon Inventory
- Weapon movements.

C) Frequency of Data Update/Reporting:

- Code Plan: Updates with each recode cycle
- Historical Data: Updates whenever a PAL operation is performed.

D) Data Flow Path:

	<u>Personnel</u>	<u>Security</u>	<u>Operations</u>	<u>Logisitics</u>	<u>Plans</u>
SITE	DP	SP	DO	-----*	XP
NAF	DP	SP	DO	LG	XP
USAFE	DP	SP	DO	LG-----	XP
USEUCOM	1	2	3-----	4	5

E) Data Channels:

- Code Plan: STU III.

F) Perceived Benefits of Automation (Automation of the PAL recode information and process is currently underway.)

- Reduced recode manpower requirements
- Fewer recode errors
- Better tracking of recode history.

3. Recapture/Recovery Site Folders

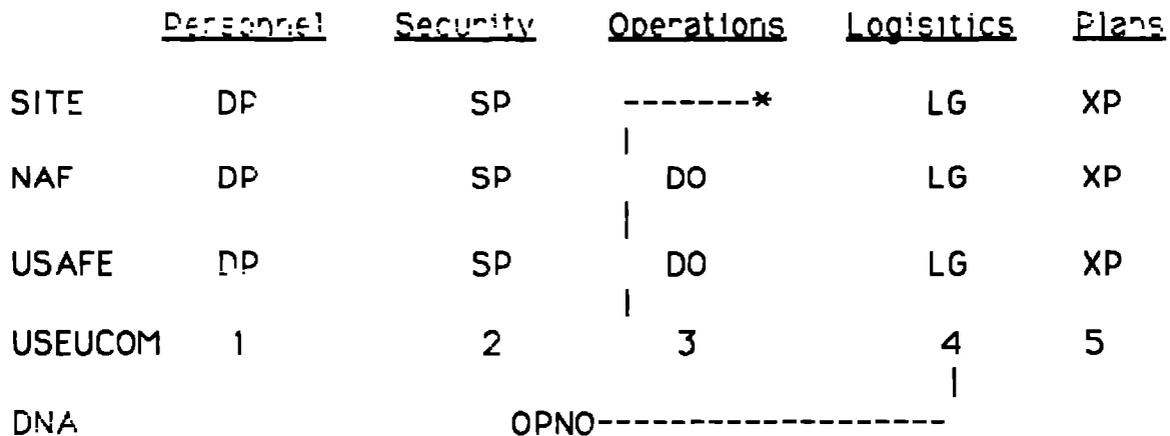
A) Requirement for Data/Purpose of the Program. The purpose of the folders is to provide sufficient information, in a timely manner, to the proper people in order to plan and execute a recapture and recovery operation.

B) Types of Data Managed:

- Site Identification and Location
- Regional Maps
- Site layouts and Utility Schematics
- Site Images
- Site Security Force Information
- Regional Logistical Details (Airports, police departments, security force locations).

C) Frequency of Data Update/Reporting. Updated every five years or as major changes are made to the site. Available at a moment's notice if needed.

D) Data Flow Path:



E) Flow Channels. Classified mail of Film from updates, Classified Mail updates to storage locations/users

F) Perceived Benefits of Automation:

- Better consistency between volumes at different locations
- Faster/easier updates
- Updates by remote personnel possible
- Cleaner storage/smaller space
- Faster Data access
- Better data presentation/Intuitive.

4. Insider Protection

A) Requirement for Data/Purpose of the Program. ACE Directive 80-6 discusses the need to minimize the insider threat; however, insider protection is not a formal program. The purpose of the emphasis is to minimize the possibility that an insider could be in a position to compromise security information.

B) Types of Data Managed: Currently None.

C) Frequency of Data Update/Reporting: None.

D) Data Flow Path: None.

E) Flow Channels: None

F) Perceived Benefits of Automation:

- Permits continuous analysis/recording of personnel
- Permits continuous monitoring of special equipment.

5. Entry Control/Access Control

A) Requirement for Data/Purpose of the Program:

- Entry Control is a DoD requirement.

- Data is used to assure that unauthorized persons cannot gain access to weapons or weapon information.

B) Types of Data Managed:

- Current:
 - Site Identification and Location
 - Personnel Data:
 - Name/Grade/Title
 - Job Description
 - Date/Time of entry/exit
 - ID Number/Passport Number
 - Escort Required
 - Clearance of Personnel
- Possible Types:
 - Personnel Data:
 - Biometric Data (fingerprints, hand geometry, weight, retina scan, etc.)
 - Images
 - Personnel Movements Intra-Site
 - Material Movements Intra-Site

C) Frequency of Data Update/Reporting: Reported as the site is entered or exited.

D) Data Flow Path: None

E) Flow Channels: None

F) Perceived Benefits of Automation:

- Improved real time analysis of personnel entering the facility
- Historical data set for analysis/trends
- Can be combined with biometric information (finger/hand print, retinal scan, etc) and images for failsafe identification
- Information could be moved between sites and command levels using communication mediumia such as RF, copper cable and fiber optics.

6. Site Visits

A) Requirement for Data/Purpose of the Program. A site visit is an activity controlled by HQ USEUCOM, the service commands, and ultimately the site commanders.

B) Types of Data Managed:

- Current:
 - Site Identification and Location
 - Personnel Data:
 - Name/Grade/Title
 - Organization
 - ID Number/Passport Number
 - Clearances of Personnel
 - Nationality
 - Clearance Information
 - Visit Information:
 - Purpose of visit/need-to-know
 - Date/duration of visit
 - Specific areas to which entry is required
 - Escort information

- Possible Types
 - Personnel Data
 - Biometric Data
 - Images

C) Frequency of Data Update/Reporting: Notification to sites as visits are scheduled.

D) Data Flow Path

	<u>Personnel</u>	<u>Security</u>	<u>Operations</u>	<u>Logistics</u>	<u>Plans</u>
SITE	DP	*----	*---	LG	XP
NAF	DP	SP	DO	LG	XP
USAFE	DP	SP -----	DO	-----LG	XP
USEUCOM	1	2	3	-----4	5

E) Flow Channels: Message traffic.

F) Perceived Benefits of Automation:

- Potential to incorporate failsafe personnel identification (biometrics, images)
- Analysis of number of visits to sites/by persons for threat assessment.

7. Force-on-Force Training

A) Requirement for Data/Purpose of the Program:

- Force-on-force training is required annually for each European storage site. ACE 80-6 outlines the training requirement, including recommended use of MILES-type simulation equipment. The training is to prepare the security force to defend the site and prevent the theft/sabotage of weapons.
- No military requirements for formal documentary information have been identified; however, this is possibly the single most important exercise in site security. Data from these exercises could be used to strengthen support for security improvements and for correcting deficiencies which are identified during the exercises. Computer simulation on force training is possible for security commanders; however, it is of little benefit to the troops.

B) Types of Data Managed:

- Current: None.
- Possible Types:
 - Site Identification and Location
 - Site Layouts
 - Security Force Information
 - Weapon Data (to be protected)
 - Personnel Data
 - Name/Grade/Title
 - ID Number/Passport Number
 - Training Record
 - Exercise Information
 - Force Composition
 - Weaponry (Offensive and Defensive)
 - Results

C) Frequency of Data Update/Reporting: Annual requirement for training.

D) Data Flow Path: None

E) Flow Channels: None

F) Perceived Benefits of Automation:

- Single repository for force-on-force results
- Identification of common problem areas
- Identification of common equipment failures
- Analysis capabilities of defensive/offensive weapon effects.

8. Weapon Inventory

A) Requirements for Data/Purpose of the Program: Joint Chiefs of Staff Publication 1-03.7 outlines the requirement and procedure for the program. The purpose is to track the location and status of every weapon in the stockpile.

B) Types of Data Managed:

- Site Identification and Location
- Weapon Data
 - Type
 - Serial Number
 - Quantity
- Weapon Movements
- Weapon Operational Status
- Maintenance Performed.

C) Frequency of Data Update/Reporting: Daily as changes.

D) Data Flow Path

	<u>Personnel</u>	<u>Security</u>	<u>Operations</u>	<u>Logistics</u>	<u>Plans</u>
SITE	DP	SP	*	LG	XP
NAF	DP	SP	DO	LG	XP
USAFE	DP	SP	DO	LG	XP
USEUCOM	1	2	3	4	5
FCDNA					

E) Flow Channels

- Autodin
- WWMCCS.

F) Perceived Benefit of Automation:

- More accurate inventory
- Improved reporting of inventory
- Faster communication channels with less errors.

9. Weapon Movements

A) Requirements for Data/Purpose of the Program. There is no current DoD requirement to track weapon movements, but rather a trail of message traffic.

B) Types of Data Managed:

- Site Identification and Location
- Weapon Data
 - Type
 - Serial Number
 - Quantity
- Movement Data
 - Call Sign
 - Hazards
 - Courier Information
 - Transportation Mode
 - Destination

C) Frequency of Data Update/Reporting: As moves are planned/made

D) Data Flow Path:

	<u>Personnel</u>	<u>Security</u>	<u>Operations</u>	<u>Logistics</u>	<u>Plans</u>
SITE	DP	SP	*----	LG	XP
NAF	DP	SP	DO	LG	XP
USAFE	DP	SP	DO-----	LG-----	XP
USEUCOM	1	2	3	4	5

E) Data Channels: Message traffic (autodin)

F) Perceived Benefits of Automation:

- Improved realtime tracking of movements
- Common data source for all movements

10. Security System Maintenance

A) Requirements for Data/Purpose of the Data. There is no requirement for security system maintenance data. The user nation is responsible for this function. The only requirements are those of security system functionality.

B) Types of Data Managed:

- Current: None
- Possible Types:
 - Site ID and Location
 - Site Layouts
 - Surveys
 - Contractor drawings
 - Security System Information
 - Sensors (Models, Serial Numbers)
 - Positions
 - Expected Useful Life
 - Statistic failure rate of similar components
 - Maintenance Information
 - Actual Hours of Use
 - Service/Replacement Dates.

C) Frequency of Data Update/Reporting:

- None required
- Data entered as maintenance is performed
- Removed as needed for analysis.

D) Data Flow Path: None.

E) Flow Channels: Currently none.

F) Perceived Benefits of Automation:

- Single repository of sensor operation data
- Improved tracking of scheduled maintenance
- Trend analysis of failures
- Improved cost accounting/projection.

11. Personnel Reliability Program

A) Requirements for Data/Purpose of the Program: DoD 5210.42, AR 50-5 (Para 3-11), and AF 35-99. The purpose of the program is to ensure the highest possible standards of individual reliability in personnel assigned to perform duties associated with the nuclear stockpile

B) Types of Data Managed:

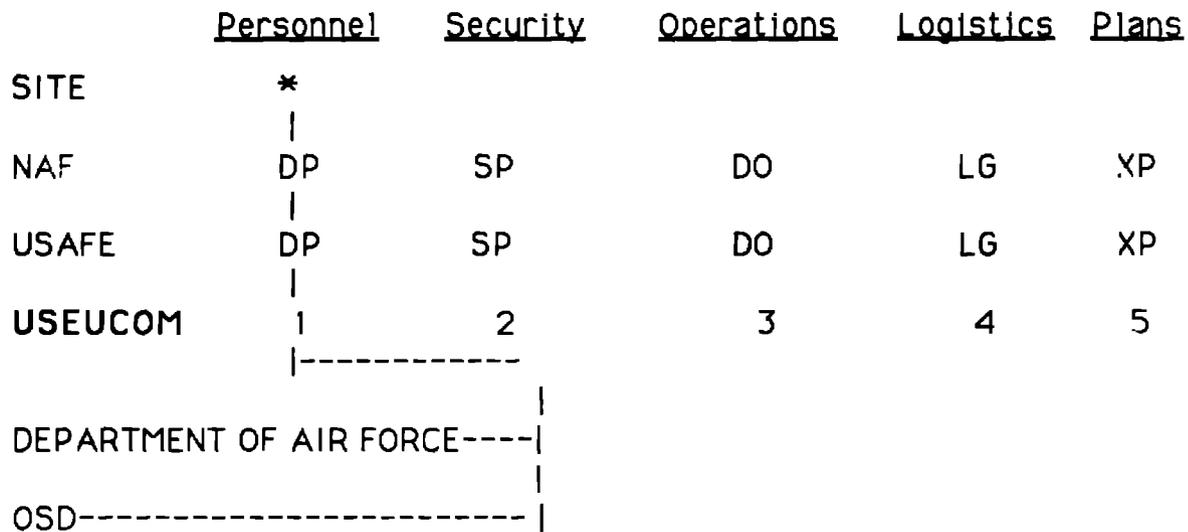
- Current:
 - Site Identification and Location
 - Personnel Data
 - Clearance Data
 - PRP Information
 - Medical Data
 - Removal Reason

- Possible Types:
 - PRP Activity History.

C) Frequency of Data Update/Reporting:

- Annual summary for DoD
- Data entered as changes in status or personnel occur.

D) Data Flow Path:



E) FLOW Channels:

- Autodin?
- Mail?

F) Perceived Benefits of Automation:

- Improved tracking of program
- Fewer errors/infractions due to DQ's assigned
- Increase in data managed equals increased analysis capability
- Trend analysis possible.

12. Custodial Unit Status Report

A) Requirements for Data/Purpose of the Program: ACE Directive 80-6 directs each custodial unit to submit an annual status report. The report summarizes the site with details and schematics/maps so that surety managers can access data. The details of the report are contained in the Appendix to ACE Directive 80-6.

B) Types of Data Managed:

- Site Identification and Location
- Delivery Unit

- Weapon Data
- Communication Data
- Security Force Information
- Regional Logistics Data.

C) Frequency of Data Update Reporting:

- Annual Report
- Amendments as Needed.

D) Data Flow Path:

	<u>Personnel</u>	<u>Security</u>	<u>Operations</u>	<u>Logistics</u>	<u>Plans</u>
SITE				*---	
NAF	DP	SP	DO	LG	XP
USAFE	DP	SP	DO	LG---	XP
USEUCOM	1	2	3	4---	5

E) Data Channels: Flow down via classified mail channels.

F) Perceived Benefits of Automation:

- Better site analysis tools
- Regional/Command summary reporting.

Unlimited Distribution:

- 10 Hq DNA/OPNS
Major Bernard E. Beldin
6801 Telegraph Road
Alexandria, Virginia 22310-2298

- 5 Hq USEUCOM
Col. Frank Willingham, USAF
ECJ4-LW
Unit 30400
APO AE 09128

- 1 5120 W. R. Reynolds
- 1 5150 K. D. Nokes
- 1 5313 J. E. Marion
- 1 9500 D. S. Miyoshi
- 1 9520 J. W. Kane
- 1 9521 D. E. McGovern
- 10 9522 J. R. Caruthers
- 1 9522 D. R. Ek
- 1 8523-2 Central Technical Files
- 5 3141 S. A. Landenberger
- 8 3145 Document Processing for DOE/OSTI
- 3 3151 G. C. Claycomb