INTERIM REPORT September 29, 1980

Accession No.__________
Contractors Report No.__________

Contract Program or Project Title: Material Control and Accounting Effectiveness Evaluation Development

Subject of this Document: Progress reported for July 1980

Type of Document: Informal monthly progress report

Author(s): Andy Poggio

Date of Document: September 5, 1980

Responsible NRC Individual and NRC Office or Division:

Robert L. Shepard, Safeguards Research Branch, SAFER:RES

is document was prepared primarily for preliminary or internal use. It has not received full review and approval. Since there may be sutstantive changes, this document should not be considered final.

Prepared by
Lawrence Livermore Laboratory
P.O. Box 808
Livermore, California 94550

Prepared for
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

NRC FIN No. A0115

DISTRIBUTION
O. Chambers
M. Fadden
H. Tovmassian
B. Mendelsohn
E. McAlpine
R. Gramann
J. Montgomery

INTERIM REPORT

8010220 651

INTERACTIONS WITH NRC/TECHNICAL MEETINGS

The Institute for Nuclear Materials Management Meeting was held in Palm Beach, Florida, during 30 June - 2 July 1980. The Lawrence Livermore National Laboratory (LLNL) Nuclear Systems Safety/Safeguards Program (NSS/Safeguards) staff made several contributions to this meeting, namely:

The Safeguards Vulnerability Analysis Program, by F. M. Gilman, M. H. Dittmore, W. J. Orvis, and P. S. Wahler.

Value-Impact Analysis of Regulations for the Nuclear Industry, by R. Al-Ayat, B. Judd, and J. Huntsman.

Evaluation and Analysis of USNRC Material Accounting to Support an Upgrade Rule Reducing the Threat of Insider Falsification, by J. J. Lim, J. G. Huebel, P. D. Chilton, and J. L. McDonnel.

In addition, A. J. Poggio served as chairman of a session entitled, "Safeguards Trends".

A. J. Poggio attended a seminar at Los Alamos Scientific Laboratory during 7-9 July 1980 entitled "Data Generation and Evaluation for Safeguards".

The LLNL NSS/Safeguards Program hosted R. L. Shepard, E. W. Richard of NRC/RES and H. Werner of NRC/IE during 21-23 July 1980. The progress of the Material Control and Accounting (MC&A) project and the Inspection Methods for Physical Protection (IMPP) project were reviewed during this time. Also, some intense discussions were held on the following important subjects:

1. The feasibility of integration of the physical protection and material control and accounting compliance inspection procedures.

2. The review and identification of existing analytical models for integration with LLNL methodologies for use in physical protection adequacy assessment.

In order to further the Physical Protection (PP) and MC&A integration activities, discussions were held which included the NRC staff members mentioned above, the LLNL MC&A project staff, the LLNL IMPP project staff, Battelle Pacific Northwest Laboratories (PNL) representatives, and SRI International representatives. Presentations were made during these meetings to familiarize the attendees with the scope of work being performed for the NRC in PP and MC&A inspection methods and automated methodology development. The following presentations were made:

E. W. Richard and R. L. Shepard (NRC/RES).	Overall purpose of discussions
A. J. Poggio (LLNL):	Overview LLNL Safeguards Program
A. W. Olson (LLNL):	Inspection Methods for Physical Protection
R. Sorensen, S. Haeberlin (PNL):	PNL work for NRC/IE on MC&A inspection program
S. Scala (SRI):	Methodologies for adequacy assessment
R. Al-Ayat (LLNL):	Aggregated Systems Model
D. R. Dunn (LLNL):	Safeguards Vulnerability Assessment Program

A follow-on discussion on 23 July was held with E. Richard and R. L. Shepard of the NRC and R. Al-Ayat of LLNL, with A. W. Olson and A. J. Poggio of LLNL attending, concerning the possible role of the Aggregated Systems Model (ASM) in the NRC Office of Inspection and Enforcement (IE) activities. Also discussed were the resources needed to develop the ASM into a user-oriented tool.

TASK 1. APPLICATION AND FURTHER DEVELOPMENT OF AUTOMATED SAFEGUARDS ASSESSMENT TOOLS

Contributors: W. Orvis, C. Patenaude, A. Poggio, P. Wahler

The technical activities in July 1980 focused on the application of the Safeguards Vulnerability Analysis Program (SVAP) to the SLIP facility physical security system and on the continued upgrade of the Structured Assessment Approach (SAA) data input package. Progress in these areas is described below.

ASSESSING THE SLIP FACILITY

The SAA assessment of the physical security system at the SLIP facility was completed (with the exception of tampering analysis) during the April-June quarter of 1980. During July a formal request was made of NRC for the additional information required for an SAA tampering analysis.

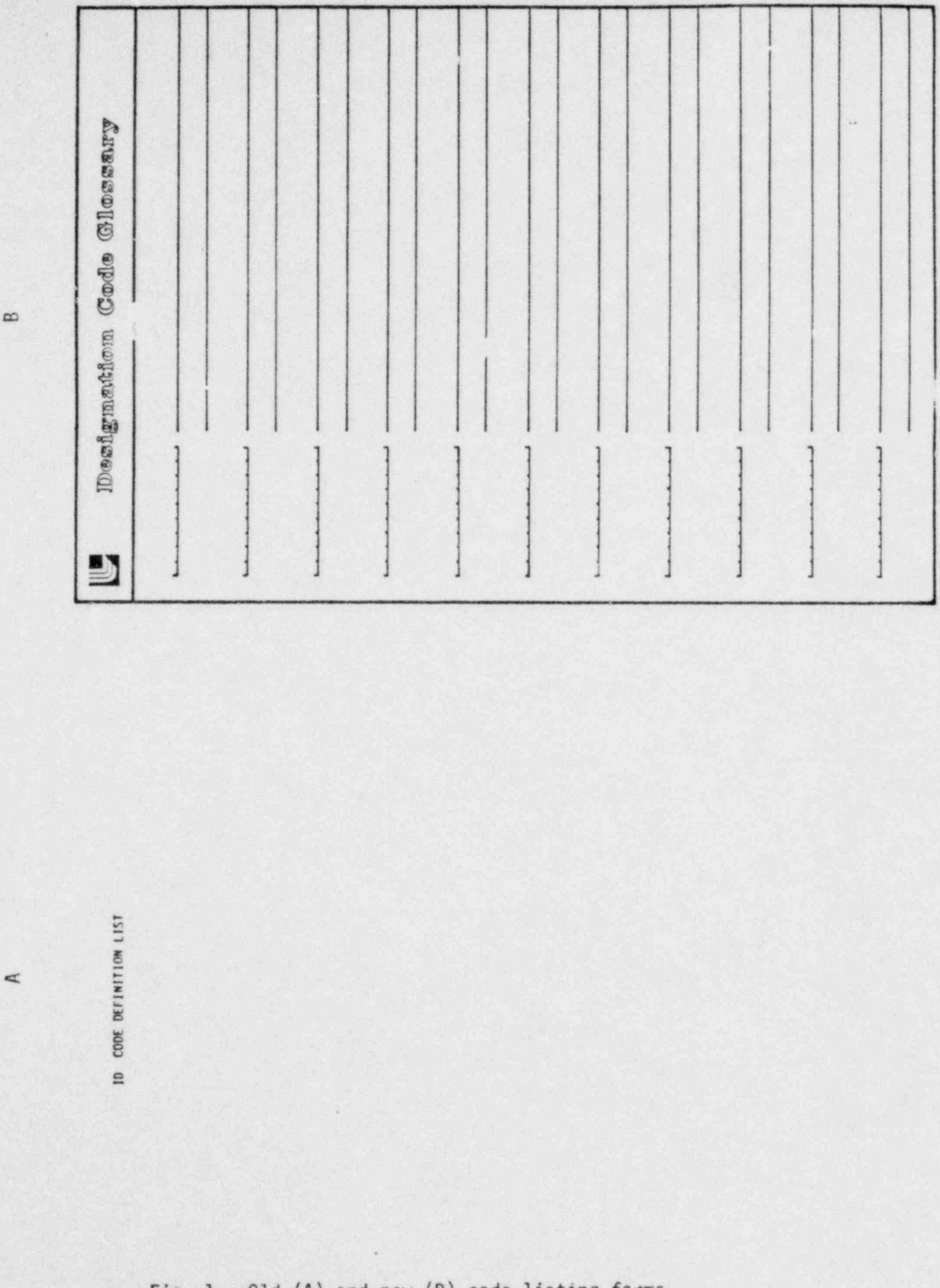
A SVAP vulnerability assessment will be performed on the SLIP facility physical security system in the near future. During July, the process of converting data used for the SAA analysis into the SVAP format was begun. This was accomplished by taking the original data and filling out the Safeguards Vulnerability Analysis Program (SVAP) Data-Gathering Handbook.[1] The data are presently being provided to the SVAP program via the Tektronix 4054. After the assessment is completed in late August or early September, a detailed report on the SLIP assessment will be completed.

UPGRADING THE STRUCTURED ASSESSMENT APPROACH

The SAA upgrade effort during July 1980 dealt with improving the preprocessor design and developing the data-gathering handbook. These efforts are described briefly below.

The SAA preprocessor is now in the advanced design stage. During July, the emphasis was on the driver or executive program. This program, for use with the Tektronix 4054, presents the various options to the user, asks for choices, and maintains overall control of preprocessor functions. The driver calls various overlays during preprocessor operations. The overlays are subprograms called from external computer memory, which are used in the main memory by the driver then erased and replaced by a subsequent overlay for a following operation. The first overlay for area edits has been completed and work is progressing on additional overlays.

Because of the recent changes in the design of the SAA preprocessor, seventy-four rather than fifty-one data-gathering forms are now required. During the course of these modifications, several improvements were made in the forms. For example, Figs. 1, 2, and 3 illustrate the improved "professional look" of several pages in the handbook. Further improvements are illustrated in Figs. 4, 5, and 6. The original SVAP data collection and recording forms shown in Fig. 4 are comparable to the improved versions in the SAA handbook shown in Figs. 5 and 6. The advantages of the improvements, in addition to better overall visual impact, include shortened requests for information, visually designated input data size constraints, and photo-ready forms for convenient report reproduction. The handbook will be completed during August 1980.



ID CODE DEFINITION LIST

Designation Code Glossary

Fig. 1. Old (A) and new (B) code listing forms

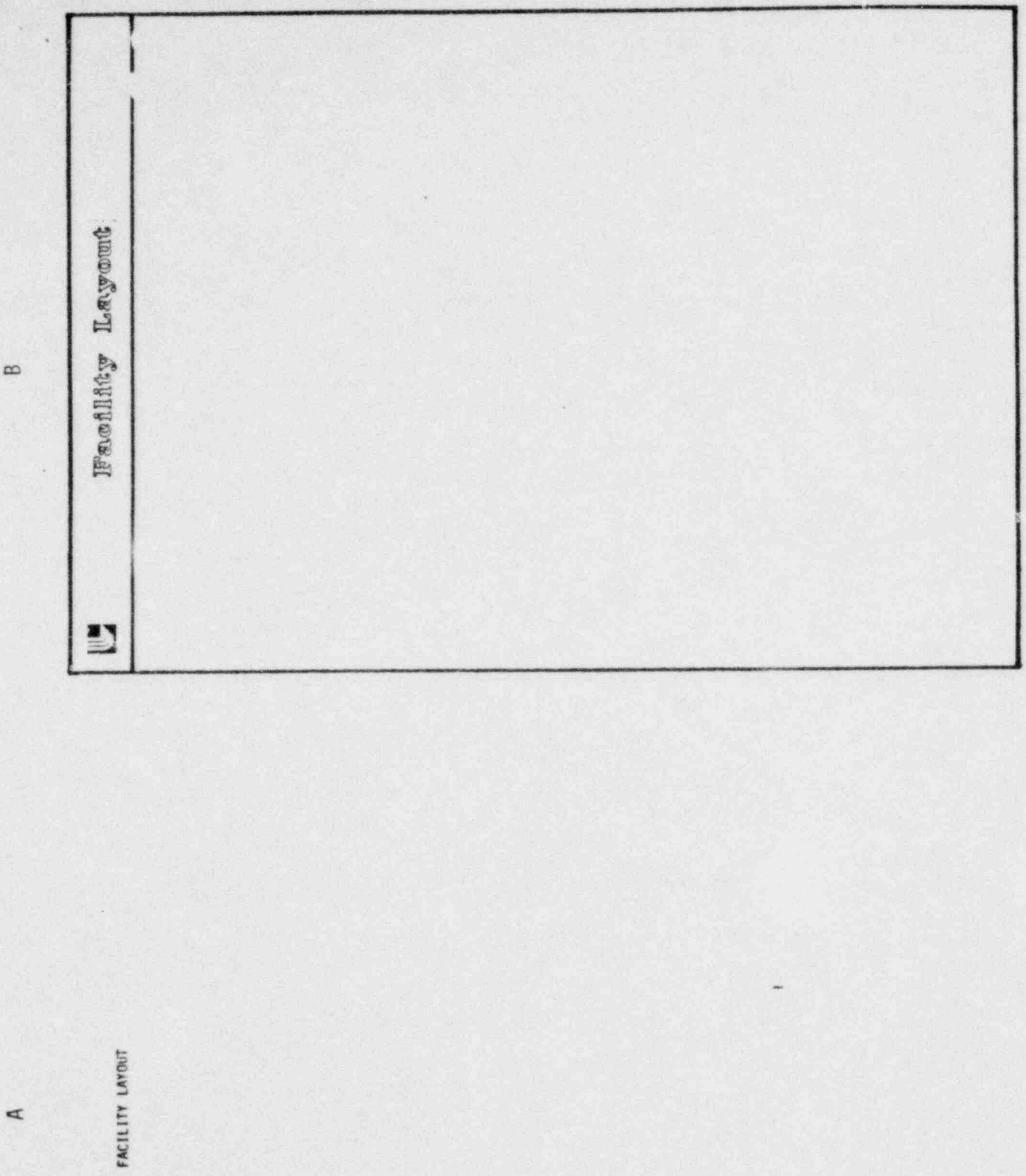
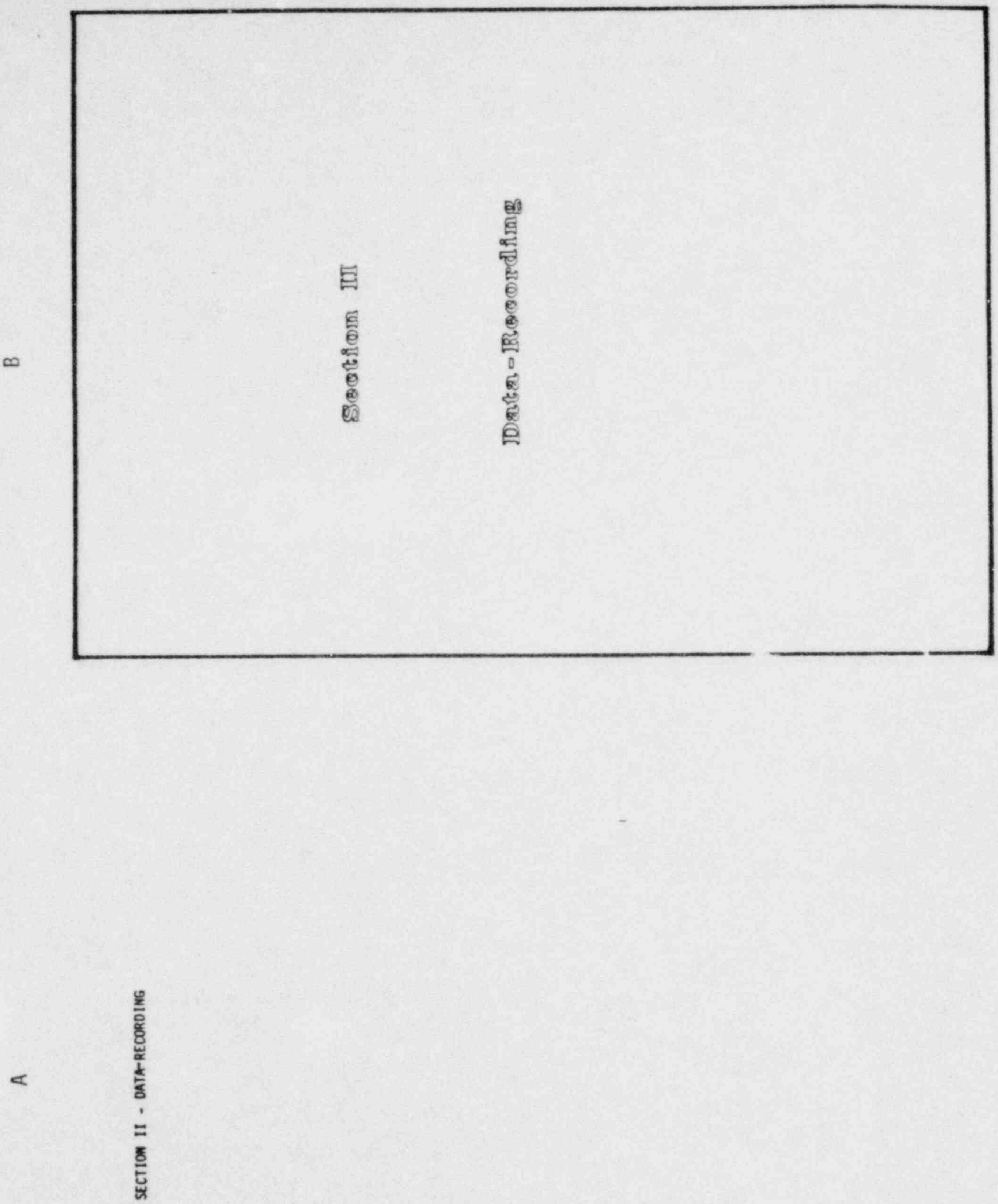


Fig. 2. Old (A) and new (B) facility layout sheets



A

SECTION II - DATA-RECORDING

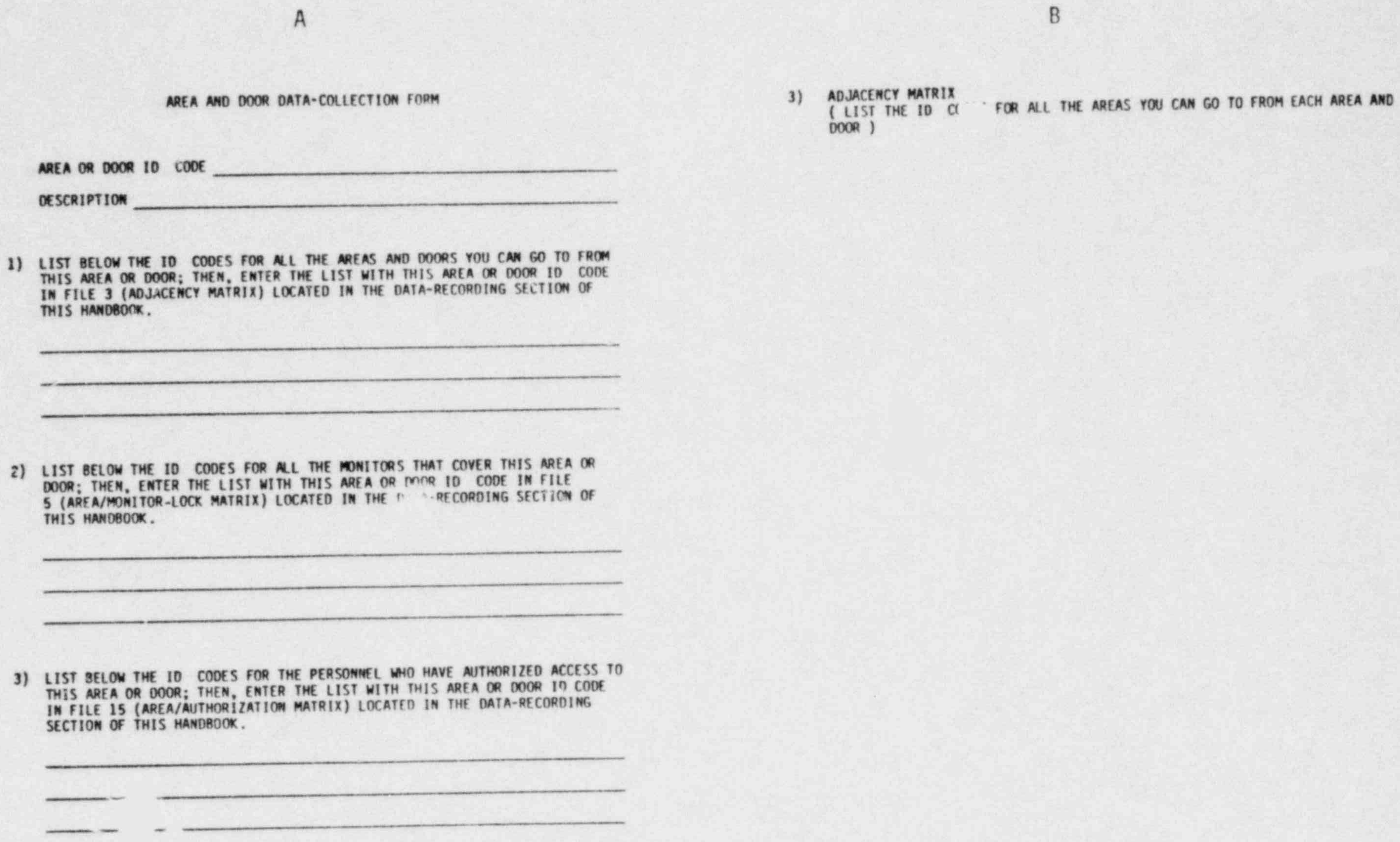
B

Section II

Data-Recording

Fig. 3. Old (A) and new (B) section II sheets

POOR ORIGINAL



A

AREA AND DOOR DATA-COLLECTION FORM

AREA OR DOOR ID CODE ______________________

DESCRIPTION ______________________

1) LIST BELOW THE ID CODES FOR ALL THE AREAS AND DOORS YOU CAN GO TO FROM THIS AREA OR DOOR; THEN, ENTER THE LIST WITH THIS AREA OR DOOR ID CODE IN FILE 3 (ADJACENCY MATRIX) LOCATED IN THE DATA-RECORDING SECTION OF THIS HANDBOOK.

____

____

____

2) LIST BELOW THE ID CODES FOR ALL THE MONITORS THAT COVER THIS AREA OR DOOR; THEN, ENTER THE LIST WITH THIS AREA OR DOOR ID CODE IN FILE 5 (AREA/MONITOR-LOCK MATRIX) LOCATED IN THE DATA-RECORDING SECTION OF THIS HANDBOOK.

____

____

____

3) LIST BELOW THE ID CODES FOR THE PERSONNEL WHO HAVE AUTHORIZED ACCESS TO THIS AREA OR DOOR; THEN, ENTER THE LIST WITH THIS AREA OR DOOR ID CODE IN FILE 15 (AREA/AUTHORIZATION MATRIX) LOCATED IN THE DATA-RECORDING SECTION OF THIS HANDBOOK.

____

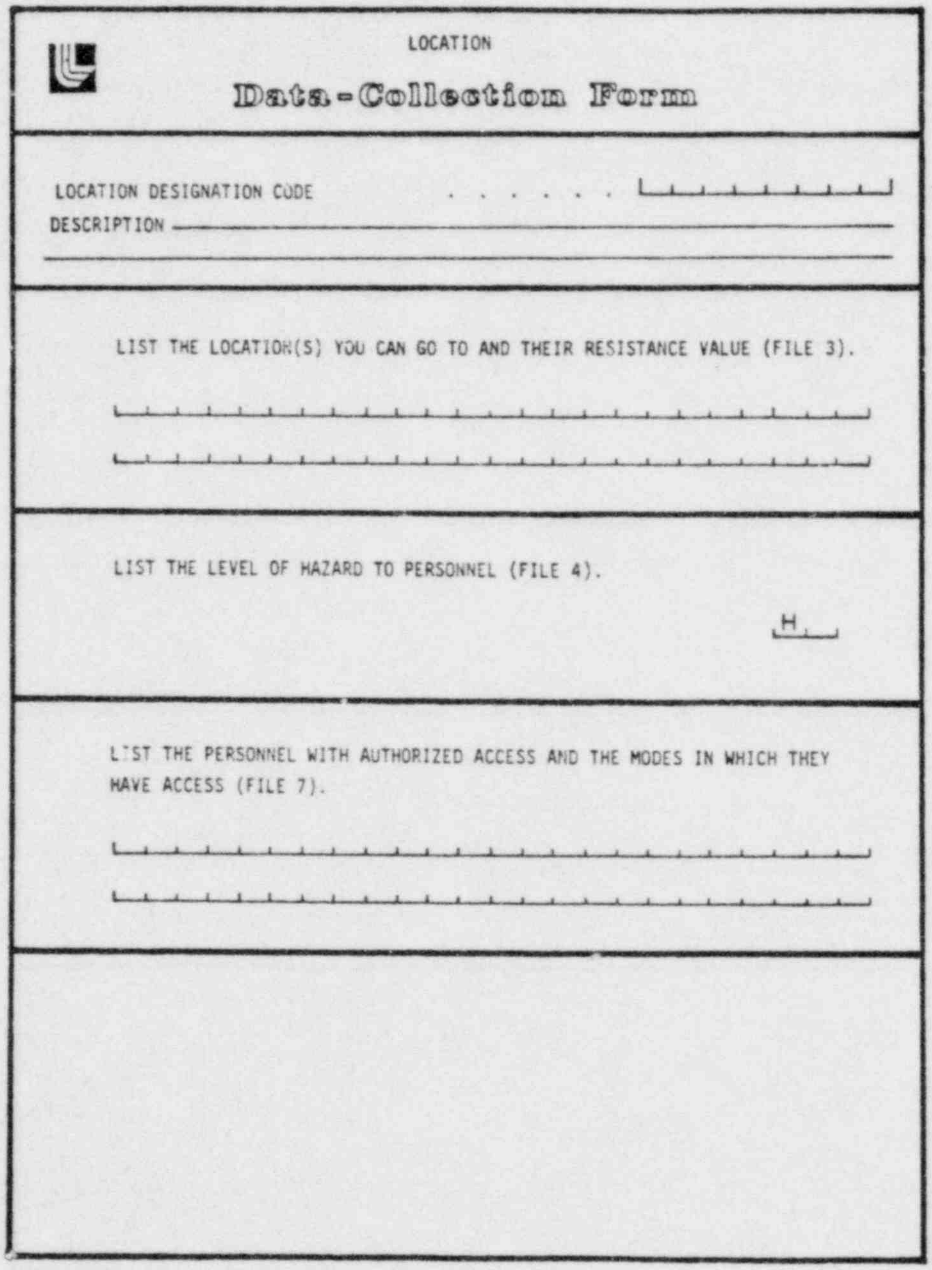
____

____

B

3) ADJACENCY MATRIX
(LIST THE ID C[illegible] FOR ALL THE AREAS YOU CAN GO TO FROM EACH AREA AND DOOR)

Fig. 4. Old data-collection (A) and data-gathering (B) matrix forms



LOCATION

Data-Collection Form

LOCATION DESIGNATION CODE . . . . . . ________

DESCRIPTION ________________________________

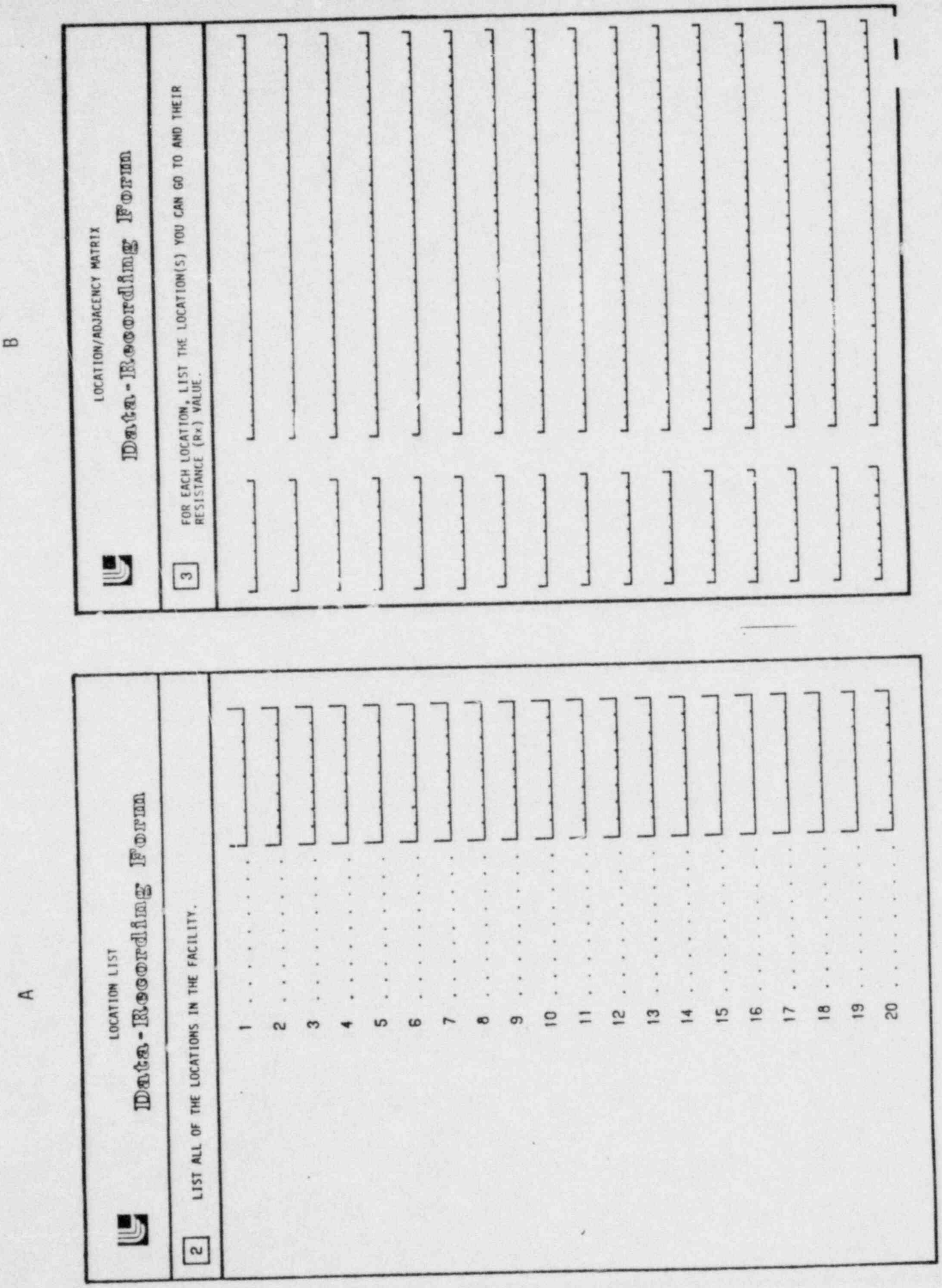
LIST THE LOCATION(S) YOU CAN GO TO AND THEIR RESISTANCE VALUE (FILE 3).

LIST THE LEVEL OF HAZARD TO PERSONNEL (FILE 4).

H

LIST THE PERSONNEL WITH AUTHORIZED ACCESS AND THE MODES IN WHICH THEY HAVE ACCESS (FILE 7).

Fig. 5. Revised data-collection form



A

LOCATION LIST

Data-Recording Form

2 LIST ALL OF THE LOCATIONS IN THE FACILITY.

1 . . . .
2 . . . .
3 . . . .
4 . . . .
5 . . . .
6 . . . .
7 . . . .
8 . . . .
9 . . . .
10 . . . .
11 . . . .
12 . . . .
13 . . . .
14 . . . .
15 . . . .
16 . . . .
17 . . . .
18 . . . .
19 . . . .
20 . . . .

B

LOCATION/ADJACENCY MATRIX

Data-Recording Form

3 FOR EACH LOCATION, LIST THE LOCATION(S) YOU CAN GO TO AND THEIR RESISTANCE (Rx) VALUE.

Fig. 6. Revised data-recordin, list (A) and matrix (B) forms

TASKS 2 and 3. DEVELOPMENT OF VALUE-IMPACT METHODOLOGY

Contributors: R. Al-Ayat, J. Huntsman,** and B. Judd**

TECHNICAL ACTIVITIES

In response to the NRC questions and comments during our June working session, several memos were completed and forwarded to Nuclear Material Safety and Safeguards (NMSS). Here we highlight the memo regarding the sensitivity of the model output to the adversary set used in our base case analysis. This memo describes the procedure used for first enumerating all possible types of safeguards threats and then systematically pruning the list to a manageable size. The pruning process reduces the requirements for data assessment and the subsequent analysis.

The procedure begins with a checklist of generic adversary characteristics reflecting material type, adversary goal quantity, adversary collusion, etc. Next, adversary scenarios are generated by forming combinations of these characteristics. At this stage, the number of unique adversary scenarios is so large that analyzing every strategy is infeasible. The next step in the analysis is pruning. The list is pruned based on several considerations, such as feasibility, logical consistency, and coalescence of identical threats. In our base case, the above process reduced the number of representative scenarios from 419 to 41 unique diversion scenarios which we feel represent the range of threats confronting an MC&A system.

B. Judd is developing a simple model which can be used to predict the frequency of attempts for various diversion and falsification strategies. These frequencies are required in the ASM to evaluate the overall safeguards performance against the variety of adversary sCenarios in the model. The model requires two types of inputs: 1) numbers of employees and the types of strategies they might use, and 2) probabilities that individual employees might attempt these strategies. The output of the model is the frequency of attempts for each strategy. Several assumptions are made regarding the formation of adversary teams and regarding the dependence among adversary probability. The model and the assumptions used will be discussed in a forthcoming project memo entitled "An Adversary Frequency Model for the ASM".

**Applied Decision Analysis (ADA), Inc., Menlo Park, CA

TASK 4. DEVELOPMENT OF IMPROVED GUIDANCE CAPABILITIES FOR MC&A SYSTEMS

Contributors: P. Chilton,* D. Dunn, G. Kufahl,*
J. McDonnel,* and A. Vergari*

TECHNICAL ACTIVITIES

This study was undertaken for the purpose of developing or recommending

1) concepts, principles and methods for protecting material accounting (MA) data from falsification
2) MA checks and balances for detecting theft or diversion
3) MA organizational criteria which support safeguards effectiveness.

We have used as a basis for this effort an LLNL study completed in 1979 which involved the systematic evaluation and critique of current MA regulations. The 1979 study led to the development of a generic, minimal material accounting (GMMA) system and a vulnerability assessment of its associated information flow diagrams.

Our approach was to investigate the vulnerability events of the GMMA system from the point-of-view of satisfying objectives 1 and 2 listed above. During the course of this task, four protection principles were identified which have the potential of providing both checks and balances, and protection against data falsification. The basic ideas embodied in the four protection principles are:

1) Assurance that there are sufficient controls involved in the use of MA data, such as in the introduction of original data into a system. This assurance can be achieved in many ways, one of which is called the Data Control (DC) rule.

2) Assurance that control procedures, which function to insure integrity and accuracy of measurements, and original data are themselves adequately protected or controlled. This principle is called a Control on Controls

*Advanced Technology Associates (ATA), Inc., Dublin, CA.

procedure (CC) and is intended to protect against improper changes in control procedures (e.g., quality control, operational procedures, etc.).

3) A verification process that requires assurances that data provided to MA elements such as consistency checks are properly used, and that correct data is reported to the next echelon level. This is called Skip Echelon Verification (SEV).

4) Another verification process that requires a parallel reporting of results by a sender to the usual receiver and to the next echelon above the normal recipient. The alternate report, as with SEV, can be used to verify other formal reports and then may be destroyed. This principle is called Secondary Echelon Forwarding (SEF).

To tie in the four protection principles with the MA organizational criteria objective of this study, we have chosen as a safeguards effectiveness measure the number of colluders required to tamper with and defeat an MA system. That is, the number of colluders necessary to compromise an MA system defines the degree of protection against data falsification and SNM diversion. For the illustrative examples developed for this study, the degree of safeguards effectiveness was considered adequate if no combination of two insiders in collusion could compromise the MA system. We wish to emphasize that this study is only concerned with vulnerabilities to personnel with authorized access to safeguards and accounting system elements.

Documentation for this task has started and is approximately 25% complete.

TASK 5. ANALYSIS OF THE ROLE OF AN INTER-FACILITY SNM ACCOUNTING SYSTEM FOR NRC SAFEGUARDS ASSURANCE

Contributors: D. Dunn, J. McDonnel,* and R. Mullin*

TECHNICAL ACTIVITIES

This task addresses two basic concerns. One concern is to identify the current NRC safeguards value of data currently being reported. The other concern is to identify what could reasonably be reported and what its impact would be. For this task, both concerns are considered from the point of view of NRC's capability to detect internal licensee MC&A system falsifications that could result in theft or diversion of a significant quantity of special nuclear material (SNM).

The first step in the study was to review documentaion on the two existing reporting systems, the Nuclear Materials Management Safeguards Systems (NMMSS) and the Safeguards Status Report System (SSRS). A data flow chart which includes both systems and which identifies the many interactions between licensees and the NRC was developed and reported in the April-June Quarterly Report. Identifying the many interactions was difficult because many are informal (i.e. not mandatory in a formal sense) and are not consistently accomplished.

Activity this month focused on the analysis of the formal data ultimately received (or is available) by the NRC. These data are the Transaction Reports (Form 741) and Material Status Reports (Form 742) submitted directly by licensees, and the Inventory Balance Reports (Form 327) prepared and submitted by the Regions for each licensee.

The purpose of the analysis was to consider the present and potential value of the reported data as external controls to protect against accounting fraud. The approach we took was to address the following questions from an auditor and systems analyst perspective:

1) How is present data analyzed?
2) What are some current practical problems?
3) What additional data might be collected and how should it be analyzed?

*Advanced Technology Associates (ATA), Inc., Dublin, CA.

The sytems analyst devoted considerable thought to the administrative aspects of the data (RIS number, transaction number, name, address, nature of transaction, etc.) while the auditors essentially dismissed these data. A subtle point can be made or deduced from the result. A clue to a fraud attempt may well be as simple as a misspelled word. To be successful, the perpetrator of a fraud must know how controls work. He cannot afford the luxury of any data errors if he is not sure of the forthcoming response.

Several issues or statements have been identified based on an incomplete analysis. These issues or statements are presented here without attempting to organize or order them.

1) As indicated earlier, any reporting error could be a fraud clue. Statistics on errors by specific licensees could be useful.
2) Keeping the licensees unsure of responses to errors or other reported data could be useful. Some response should always be made, of course.
3) Transmitting encrypted data would obviate some fraud scenarios.
4) The use of serialized and accountable forms would eliminate some fraud scenarios.
5) Data corrections could be crypto-keyed to transaction report numbers.
6) Duplication or redundancy of data reporting could be beneficial (if not otherwise a burden) provided the data is compared by someone. Shipper and receiver data are examples, so are last ending inventory and new beginning inventory.
7) Verification by independent entities of data transmitted could prevent some fraud scenarios. Encryption of data is an obvious possibility.
8) It would seem to be worthwhile to send a 742 report as of each physical inventory.
9) Monthly informal material balances could be compared with 742's plus 741's if 8 above were required.
10) Monthly loss and discard reports would balance the books with 8 and 9 above.
11) Real time transmission of data could be useful if it could be analyzed by NRC.

12) Some informal reporting should be formalized.

13) Audits by Regions can detect fraud but not necessarily in a timely fashion. A redundancy of important data that could be checked and compared any time would be ideal.

14) Consider requiring independent additional verification of data depending on the ratio of ID reported and LEID.

15) Perform trend analysis on shipper/receiver differences.

16) Perform trend analysis on ID data.

17) Standardize the data in SSRS and NMSS.

18) Transmit data as received by Regions to the appropriate NRC safeguards analysis group.

Task 5 is progressing well and draft documentation has beer startea.

REFERENCES

1. P. S. Wahler, Safeguards Vulnerability Analysis Program (SVAP) Data-Gathering Handbook, Lawrence Livermore National Laboratory, Livermore, CA, NUREG/CR-1169, Vols. 1 and 2; UCRL-52731, Vols. 1 and 2 (1980).