27
8/3/81
Hic
24th TTLS (1)

B6122

UCID- 18974

MASTER

A FRAMEWORK FOR THE SYSTEMATIC ASSESSMENT OF A
MATERIAL CONTROL AND ACCOUNTING SYSTEM

Richard S. Schechter
Lawrence Livermore National Laboratory

Ivan J. Sacks
Analytic Information Processing, Inc.

22 April 1981

This is an informal report intended primarily for internal or limited external distribution. The opinions and conclusions stated are those of the author and may or may not be those of the Laboratory.

This work was supported by the United States Nuclear Regulatory Commission under a Memorandum of Understanding with the United States Department of Energy.

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

FOREWORD

This paper provides a framework for the systematic assessment of a Material Control and Accounting (MC&A) system, as described by a license applicant in an MC&A Plan. The assessment methodology could be used by both the license applicant and the NRC license reviewer, to determine compliance with the proposed MC&A Upgrade Rule.* The inputs to the assessment will consist only of the commitments documented in the applicant's MC&A Plan. The assessment will incorporate no implicit assumptions as to how the applicant's system should function, and will grant no credit for safeguards measures not explicitly described in the MC&A Plan.

We have assumed that the license applicant's MC&A Plan will follow the Standard Format and Content Guide proposed by LLNL in Task 4 of the "Development of Guidance for MC&A System Design" project (FIN A0289-0). The present paper constitutes the contract deliverable for Task 5 of this project.

*This paper is keyed to the draft version of the MC&A Upgrade Rule dated December 16, 1980. This version has since been revised as the MC&A Reform Amendment, but has not yet received the final endorsement of NRC management.

TABLE OF CONTENTS

	<u>Page</u>
FOREWORD	iii
ABSTRACT	ix
I. INTRODUCTION.	1
II. TYPES OF ASSESSMENT PROCEDURES.	9
III. FRAMEWORK FOR VULNERABILITY ASSESSMENT.	15
1.0 Objectives.	17
2.0 Vulnerabilities of Individual Components.	22
2.1 Vulnerabilities Due to Authorized Control	26
2.2 Vulnerabilities Due to Component Location	28
2.3 Vulnerabilities Due to Related Components	37
3.0 Vulnerabilities of Detection Subsystems	42
3.1 First Order Assessment.	48
3.2 Second Order Assessment	67
IV. FRAMEWORK FOR STATISTICAL ASSESSMENT.	71
1.0 Objectives.	73
2.0 Outputs of Statistical Assessment	76
2.1 Bulk Loss Detection Subsystems.	78
2.2 Item Loss Detection Subsystems.	89
2.3 Joint Performance of Bulk Loss and Item Loss Detection Subsystems.	92
2.4 Overall Facility False Alarm Rate	97
3.0 Details of Statistical Assessment	99
3.1 Bulk Loss Detection Subsystems.	100
3.2 Item Loss Detection Subsystems.	124
3.3 Response Subsystems	126
V. APPLICATION OF ASSESSMENT PROCEDURES.	137
1.0 Preliminary Assessment Procedures	139
2.0 Assessment for S70.83: Detection Capability.	141
3.0 Assessment for S70.85: Response Capability	145
4.0 Assessment for S70.86: Assurance Structure	148
5.0 Assessment for S70.87: Protection Against the Design Basis Threat	153
6.0 Assessment for S70.94: Record Keeping.	154
APPENDIXES	A-1
Appendix I. Relationship of I&C Response Sheets to the Statistical Assessment.	A-3
Appendix II. Example Subsystem Description	A-10
Appendix III. Example I&C Response Sheets for Detection Subsystem Components.	A-15
Appendix IV. Response to NRC Concerns of 5 February 1981	A-21

LIST OF FIGURES

	<u>Page</u>
Figure III-1. Integration of Vulnerability Sets for PP and MC&A Subsystems	21
Figure III-2A. "OR GATE"	23
Figure III-2A. "AND GATE"	23
Figure III-3. Unit Model for an Unprotected Accounting Form	31
Figure III-4. Protection of a Component From Compromise Through its Location.	33
Figure III-5. Self Closure of Unit Model Chain.	35
Figure III-6. Compromise of a Component Through a Related Component	39
Figure III-7. Components "Wired in Parallel".	41
Figure III-8. General Format for Detection Subsystem Description.	43
Figure III-9. Measurement Element of a Hypothetical Detection Subsystem	49
Figure III-10. Module A for Measurement Element.	51
Figure III-11. Module B for Measurement Element.	53
Figure III-12. Reference Element of a Hypothetical Detection Subsystem	55
Figure III-13. Module D for Reference Element.	57
Figure III-14. Comparison Element of a Hypothetical Detection Subsystem	59
Figure III-15. Threshold Determination Element of a Hypothetical Detection Subsystem	61
Figure III-16. Threshold Test Element of a Hypothetical Detection Subsystem	63
Figure III-17. Response Initiation Element of a Hypothetical Detection Subsystem	65
Figure III-18. Reconciliation Procedure.	69
Figure IV-1. Component Performance	79
Figure IV-2. Subsystem Performance (No Loss)	79
Figure IV-3. Subsystem Performance	81
Figure IV-4. Action Threshold.	81
Figure IV-5. Detection and False Alarm Probability	83
Figure IV-6. Results of Volume Measurement Procedure Simulation.	85
Figure IV-7. Variance Reduction.	87
Figure IV-8. Typical Item Loss Detection Subsystem Performance	91
Figure IV-9. Overall Detection Performance for Combined Item and Bulk Diversion of 5 FKG	93
Figure IV-10. Composite Detection Performance	95
Figure IV-11. General Format for Detection Subsystem Description.	103
Figure IV-12. Expansion of Measurement Element.	105
Figure IV-13. Simulation Concept.	109
Figure IV-14. Measurement Procedure Simulation.	111
Figure IV-15. Pneumatic Density/Height Measurement System	113
Figure IV-16. Process Model Simulation.	115
Figure IV-17. Quantity Measurement Procedure Simulation	117
Figure IV-18. Composition Measurement Procedure Simulation	119
Figure IV-19. Comparison Element Simulation	121

Figure IV-20.	Reference Element Simulation.	123
Figure IV-21.	Response Subsystem Simulation	127
Figure IV-22.	Example Control Unit.	129
Figure IV-23.	Monte Carlo Simulation of the Example Detection and Response Subsystem.	133
Figure IV-24.	Response Subsystem Performance.	135
Figure A-1	Relationship of I&C Response Sheets to Bulk Detection Subsystem Statistical Assessment.	A-5

ABSTRACT

Procedures are described for the systematic assessment of a Material Control and Accounting (MC&A) system, in terms of compliance to the proposed MC&A Upgrade Rule. The applicability of these assessment procedures to specific Rule provisions is discussed. Special attention is given to the statistical performance of individual subsystems, and their vulnerability to compromise by insider collusion.

I. INTRODUCTION

This paper proposes a framework for the assessment of a license applicant's Material Control and Accounting (MC&A) Plan, for compliance with the MC&A Upgrade Rule. The applicant's MC&A Plan must follow the format specified in a Standard Format and Content (SF&C) Guide, currently under preparation by the NRC. For the purposes of this paper, we have assumed that the final SF&C Guide will be based upon the inputs provided by LLNL in the following documents:

Part II of Standard Format and Content Guide:

Subsystems and Programs for MC&A Rule Requirements

R. S. Schechter, LLNL, and I. J. Sacks, AIP, February 11, 1981, UCID-18953, Part II.

Part III of Standard Format and Content Guide:

Component Intent and Content Sheets

R. S. Schechter, LLNL, and I. J. Sacks, AIP, February 4, 1981, UCID-18953, Part III.

As pointed out in the forewords to the above documents, we envision the final SF&C Guide structured to:

- a) Elicit successively finer levels of detail concerning the MC&A system.
- b) Facilitate consistency checks between information provided in different portions of the MC&A Plan.
- c) Force the license applicant to rigorously define each aspect of the proposed MC&A system relevant to an evaluation of statistical performance and vulnerability to the design basis threat included in the MC&A Rule.

In preparing this document, we have assumed that the final SF&C Guide prepared by the NRC will consist of the following subdivisions, each of which will instruct the license applicant on how to complete the corresponding portion of the MC&A Plan:

- Part I: MC&A System Overview
- Part II: Subsystems and Programs for MC&A Rule Requirements
- Part III: Component Intent and Content Sheets
- Part IV: Supporting Calculations

Part I of the SF&C Guide is currently under preparation by the NRC staff, and will be based largely upon Part I of the Assessment Questionnaires* Package submitted by LLNL in July of 1980. We assume that Part I will elicit the following overview information**:

1. Facility layout and location designations.
2. Designations, locations and functions of all control units.
3. Description of facility process flow and throughput.
4. Designations, locations, functions and throughputs of all Process and Storage Equipment for SSNM in bulk form.
5. Designations, locations, functions and throughputs of all Secure Storage Compartments for SSNM in itemized form.
6. Designations and descriptions of all material description categories.

* Sacks, I. J., and Schechter, R. S., Material Control and Accounting Upgrade Rule Assessment Questionnaires: Guidance for System Design and Data Collection Format for Compliance Evaluation. June 20, 1980. Submitted to NRC by LLNL as Task 4 deliverable for the "Development of Guidance for the Material Control and Accounting System Design" Project.

** Component types for which Intent and Content Sheets have been provided in Part III of the SF&C Guide are capitalized.

7. Designations, descriptions and locations of all "material batches."*
8. Table of Receiving and Shipping Procedures for different material description categories.
9. Table of Internal Transfer Procedures and associated control units.
10. Table of Item Creation Procedures and Item Destruction Procedures.
11. The management hierarchy of the facility, including:
 - a) Designations and definitions of personnel categories for all facility employees and others who will be authorized to enter the protected area of the facility at any time
 - b) The facility locations to which each personnel category has authorized access.
 - c) The limitations on the alternation of personnel categories between employees.
12. Designations and descriptions of stewardship teams for SSNM.
13. Table of Authorization Schedules and the procedures which they support.
14. Table of Signal Transmission Components and the components which they support.
15. Table of Utility Supply Components and the components which they support.

* A material batch is defined as the SSNM of a particular material description category within a specific piece of Process or Storage Equipment, or within a set of items under identical controls.

16. Table of Locks and the components which they protect.
17. Table of sets of Security Seals and the components which they protect.
18. Table of Secure Storage Compartments and the components which they protect.
19. Designations and functions of all MC&A subsystems, as well as page references to their description in Part II of the MC&A Plan.

Part II of the SF&C Guide will elicit descriptions of the subsystems and programs which will be used to comply with specific requirements of the MC&A Rule. A "subsystem" is a collection of inter-related components which will directly assist in fulfilling a specific functional requirement of the MC&A Rule relating to the detection of or response to a discrepancy in the status of SSNM. A "program" is a collection of components which will be used to fulfill one of the following assurance requirements of the MC&A Rule*: S70.86 (b), (c), (d), (e), (f) or (g). Note that the programs for S70.86 (f) and (g) will contain a number of "subsystems" relating to the detection of or response to inventory differences or shipper/receiver differences. Part II of the MC&A Plan will identify specific components to be used in MC&A subsystems and components. To facilitate the license review, the numbering of the subdivisions of Parts I and II of a MC&A Plan must correspond to those of the SF&C Guide.

Part III of the SF&C Guide will elicit detailed descriptions of each specific component identified in the applicant's MC&A Plan. This portion of the guide will consist of roughly 100 Intent and Content (I&C) Sheets, each of which provides the format for the description of a particular component type. The license applicant's description of a specific

*The Rule provisions referenced herein are based upon the version dated December 16, 1980.

component in Part III of the MC&A Plan is referred to as an I&C Response Sheet. A separate I&C Response Sheet must be completed for each specific component identified in Parts I or II of the MC&A Plan, or in another I&C Response Sheet.

Part IV of the SF&C Guide will elicit justification for any performance parameters or equations included in Parts II or III of the MC&A Plan. That is, no specific format will be required for Part IV of the MC&A Plan.

The following conventions are used in the remainder of this paper, to eliminate needless repetition.

1. References to portions of the MC&A Plan will be abbreviated as in the following example:

"Part II, Section 2.1.2.1 of the MC&A Plan" is abbreviated as "Part II-2.1.2.1."

Note that the numbering of the MC&A Plan must correspond to the numbering of the SF&C Guide. Section numbers for Part I are based upon the proposed breakdown on pages 3-6 above, while section numbers for Part II are based upon the LLNL inputs to the SF&C Guide dated February 11, 1981.

2. Following the convention established in the LLNL inputs to the SF&C Guide, names of component types which correspond to I&C Sheets have been capitalized.
3. References to I&C Response Sheets for individual components will be abbreviated as in the following example:

"Check for a reference to an I&C Response Sheet for an Accounting Form" is abbreviated as "Check for a reference to an Accounting Form."

11. TYPES OF ASSESSMENT PROCEDURES

Compliance with each provision of the MC&A Upgrade Rule will be evaluated by the application of one or more of the following assessment procedures:

1. Completeness Checks--These will be used to determine if the information provided in a particular portion of the MC&A Plan is complete. Examples of completeness checks include the determination of whether or not:
 - a) A correspondence table requested by the SF&C Guide has been included.
 - b) A correspondence table includes a subsystem designation for each entry in a more fundamental table.
 - c) A separate subsystem description has been included for each subsystem designated in a correspondence table.
 - d) All items of information requested by the SF&C Guide have been included in a subsystem description.
 - e) An I&C Response Sheet has been provided for each component referenced in a subsystem description.
 - f) An I&C Response Sheet includes all information requested by the corresponding I&C Sheet.
 - g) Part IV includes the appropriate justification for the performance parameters included in a subsystem description.
 - h) Part IV includes the justification for the equations included in an I&C Response Sheet.
2. Compliance Checks--These will be used to determine if the statistical parameters for subsystem performance presented in the MC&A Plan are consistent with the MC&A Rule. For example, the listed probability of detecting a control quantity loss of SSNM from a single control unit would be compared to the performance required by S70.83(a)(4)(ii). If a subsystem were to fail a compliance check, there would be no need to pursue the Part IV adequacy check or the statistical assessment described below.

3. **Component Adequacy Checks**--These will be used to determine if the component descriptions provided in the I&C Response Sheets are consistent with minimal criteria established by the NRC. For example, an I&C Response Sheet for a Training Procedure might be checked for a commitment to the use of written task descriptions. The minimal criteria will be set forth in the I&C Sheets and/or the appropriate Regulatory Guides. Adequacy checks are especially important for those component features which would not be incorporated into the vulnerability or statistical assessments described below.
4. **Part IV Adequacy Checks**--These will be used to check the justifications provided for performance parameters claimed in Part II of the MC&A Plan, as well as for equations included in the I&C Response Sheets. The basic purpose of such adequacy checks is to discover any gross errors which would obviate the need for the statistical assessment described below. Because the statistical assessment will be used for the final determination of compliance, the Part IV adequacy checks need not include a sophisticated analysis of any simplifications used by the applicant.
5. **Vulnerability Assessment**--This will be used to determine the vulnerability of a detection subsystem to the design basis threat specified in the MC&A Rule. The input to this assessment procedure will consist of information which relates individual components to their safeguards environment, as described in the I&C Response Sheets. The output of this assessment procedure will be a list of combinations of insiders who are capable of preventing the detection of a diversion of SSNM. Because a vulnerability assessment constitutes a complex network problem, a computerized methodology will generally be required. A framework for a vulnerability assessment is described in Section III below.

6. Statistical Assessment--This will be used to determine compliance with the statistical parameters in the MC&A Rule, for detection subsystems, inventory subsystems, and shipper/receiver subsystems. The inputs to this assessment procedure will include error distributions for measurement components, as well as the data processing equations used by the licence applicant. The outputs of this assessment will include the probabilities of detection and false alarm for both a control quantity loss and a 5 FKG loss. An additional output will be the total false alarm rate for all detection subsystems. Because of the complex nature of a statistical assessment, a computerized methodology will generally be required. A framework for a statistical assessment is described in Section IV below.

The applicability of assessment procedures 1) through 6) to specific portions of an MC&A Plan is described in Section V below.

III. FRAMEWORK FOR VULNERABILITY ASSESSMENT

1.0. OBJECTIVES*

This section describes the basic concepts involved in assessing the vulnerabilities of an MC&A subsystem to the design basis threat specified in S70.81 of the MC&A Upgrade Rule. This assessment will be used to evaluate compliance with S70.87, "Protection Against Falsification of MC&A Records or Other Compromise of the MC&A System by the Design Basis Threat."

A vulnerability assessment will determine which insiders or combinations of "insiders" have the capability to "cover up" a diversion of SSNM, by defeating the intended function of a detection subsystem.** An "insider" is defined as any person who will be authorized to enter the protected area (PA) of a facility for any reason at any time, with the exception of DOE/NRC inspectors. Thus, private contractors who are not directly employed by the facility are included in this definition.

The MC&A Plan will refer to each insider in terms of a personnel category, which will be defined in terms of the authorization status of its members. These definitions must be included in Part 1-11 of the MC&A Plan. Note that while the design basis threat of S70.81 refers to outsiders as well as insiders, an MC&A subsystem which is sufficiently well protected against insiders will also be sufficiently well protected against outsiders.

* The modeling techniques used in Section III are based upon those presented in: Parziale, A.A., and Sacks, I.J., The Structured Assessment Approach, Version I, Lawrence Livermore National Laboratory, 1980, NUREG/CR-1233.

** A detection subsystem will be designed to detect the loss of SSNM from one or more pieces of Process or Storage Equipment within a particular control unit.

The output of the vulnerability assessment for an MC&A detection subsystem will be the set of persons or combinations of persons who could prevent the detection of a loss by the subsystem. This set is termed the vulnerability set of the subsystem; all personnel in the set are referred to by their personnel categories. An example vulnerability set may be represented as follows:

$$V(DS9) = a + g \cdot k + l \cdot m + n \cdot s \cdot t$$

The "+" sign in the preceding equation represents a Boolean "OR," while the "." sign represents a Boolean "AND." Thus, the preceding equation would be interpreted as follows:

Detection Subsystem #9 can be compromised by:

- Person a acting alone, or
- Persons g and k in collusion, or
- Persons l and m in collusion, or
- Persons n, s, and t in collusion.

The performance measure for a detection subsystem would be the minimum number of insiders in collusion to which the subsystem is vulnerable (i.e., the size of the smallest combination of insiders in the vulnerability set). For the preceding example, the value of this performance measure would be one insider. The acceptable level for this performance measure will depend upon the NRC's interpretation of the design basis threat. Note that the current wording of S70.81 does not specify the maximum conspiracy size against which a subsystem must be protected.

To allow for the meaningful interpretation of the outputs of an MC&A vulnerability assessment, these results should be integrated with the results of a Physical Protection (PP) vulnerability assessment. That is, the determination that certain persons could cover-up a diversion of SSNM

is of limited value, unless it is also determined whether or not these persons could divert SSNM.* For example, an MC&A detection subsystem which is vulnerable to a single insider might be deemed acceptable, if this person requires the collusion of five additional insiders to accomplish a diversion in the first place.

Thus, the vulnerability set for an MC&A detection subsystem should be integrated with the vulnerability set for the corresponding PP subsystem (i.e., the subsystem which protects the material covered by the MC&A subsystem). The integrated vulnerability set can be determined by finding the intersection of the individual vulnerability sets, as indicated in Figure III-1. The integrated performance of the corresponding subsystems would be evaluated in terms of the smallest combination of insiders in the integrated vulnerability set (i.e., the minimum number of insiders in collusion who could divert SSNM and cover-up the diversion).

The MC&A assessment methodology will derive the vulnerability set for a detection subsystem from the vulnerabilities of its individual components. A component is a piece of equipment, a procedure or a set of information which will be used by a licensee to assist in meeting the performance requirements of the MC&A Upgrade Rule. Section 2.0 below describes the "scoring rules" which could be used to determine the vulnerabilities of individual components; Section 3.0 describes the "aggregation algorithms" which could be used to determine the vulnerabilities of complete subsystems. The modeling techniques involved in these sections are illustrated in terms of hypothetical examples, and their applicability to MC&A subsystem design is described.

* The converse of this statement is not true, as some adversaries might seek to divert SSNM without regard for a subsequent cover-up.

$V(PPN)$ = Vulnerability set for Physical Protection (PP) Subsystem #N (i.e., the set of persons or combinations of persons who could divert SSNM by compromising PP subsystem #N).

$V(DSN)$ = Vulnerability set for MC&A Detection Subsystem #N (i.e., the set of persons or combinations of persons who could cover-up a diversion by compromising detection subsystem #N).

$V(PPN) \cup V(DSN)$ = Integrated vulnerability set for PP Subsystem #N and MC&A Detection Subsystem #N (i.e., the set of persons or combinations of persons who could divert SSNM and cover-up the diversion).

* The necessity for inputs from the PP Plan in the assessment of an MC&A detection subsystem is discussed below in Section 2.2.

FIGURE III-1. INTEGRATION OF VULNERABILITY SETS FOR PP AND MC&A SUBSYSTEMS

2.0 VULNERABILITIES OF INDIVIDUAL COMPONENTS

This section describes the "scoring rules" which could be used by an assessment methodology to determine the vulnerabilities of individual components. These vulnerabilities can be represented via a graph theoretic device referred to as the unit model. The unit model is used to illustrate the relationship of a component to its safeguards environment in terms of authorized control, component location, relationships to other components, tamper protection, etc. This information allows the determination of which persons or combinations of persons can compromise a component by defeating its intended safeguards purpose. Depending upon the type of component in question, typical means of compromise might include falsification, substitution, theft or destruction. Examples of the compromise of specific components include the following:

- a) Falsification of the output of a Mass Measurement Instrument, by tampering with the calibration control.
- b) Substitution of a Reference Standard used in a Quantity Measurement Procedure.
- c) Theft of a Computerized Data Storage Medium which contains reference data.
- d) Destruction of Accounting Forms used in a Reconciliation Procedure.

To represent the potential effects of persons upon components, the unit model uses two Boolean logic structures: the "OR GATE" and the "AND GATE." These structures and their representation in Boolean algebra are respectively illustrated in Figures III-2A and III-2B. An "OR GATE" is used to represent the situation in which a component can be compromised by any of several persons acting alone. An "AND GATE" is used to represent the situation in which a component can be compromised only by several persons in collusion. An equivalent interpretation of the "AND GATE" in Fig. III-2B is that component N is protected against person x by

Boolean Equation: $V(CN) = x_{CN} + y_{CN}$

Translation: Component N is vulnerable to person x or person y acting alone.

FIGURE 111-2A: "OR GATE"

Boolean Equation: $V(CN) = x_{CN} \cdot y_{CN}$

Translation: Component N is vulnerable to person x in collusion with person y.

FIGURE 111-2B: "AND GATE"

person y, and vice versa. "OR GATES" and "AND GATES" can also be used to represent the vulnerabilities of a component due to related components, as discussed below. The I&C Sheets provided in Part III of the SF&C Guide have been designed to elicit data in a manner consistent with the logic gate construct. The algorithms used in computerized packages for vulnerability assessments are designed to manipulate Boolean equations based upon "OR GATES" and "AND GATES."*

The vulnerabilities of a component which are represented by the unit model can be categorized as follows:

- a) Vulnerabilities due to authorized control
- b) Vulnerabilities due to component location
- c) Vulnerabilities due to related components

These three categories are respectively described in Sections 1, 2, and 3 below, and are summarized in Table III-1.

*Computerized packages for vulnerability assessments include:
F. M. Gilman, M. H. Dittmore, W. J. Orvis, P. S. Wahler, Safeguard Vulnerability Analysis Program (SVAP) Executive Summary, Lawrence Livermore National Laboratory; 1980, NUREG/CR-1169.
A. A. Parziale and I. J. Sacks, The Structured Assessment Approach, Version I, Lawrence Livermore National Laboratory, 1980, NUREG/CR-1233.

TABLE III-1. CATEGORIES OF COMPONENT VULNERABILITIES.

SOURCE OF VULNERABILITY	REPRESENTATION	EXAMPLE	DATA SOURCE
1. Authorized Control	<p>(Component N can be compromised through authorized control by person x.)</p>	Falsification of an Accounting Form by person authorized to enter data.	Personnel categories identified in I&C Response Sheets.
2. Component Location (via authorized or unauthorized access)	<p>(Component N can be compromised through access to location I by person x.)</p>	Falsification of an Accounting Form by a key custodian who could gain unauthorized access to its storage room.	a) Component locations identified in I&C Response Sheets b) List of personnel access authorizations in Part I-11 of MC&A Plan. c) Info. in Physical Protection Plan on access controls, personnel monitors, etc.
3. Related Component	<p>(Component N can be compromised through component L.)</p>	Falsification of an Accounting Form through compromise of the procedure which it documents.	Cross references between I&C Response Sheets.

2.1 Vulnerabilities Due to Authorized Control

The first category of component vulnerabilities arises from the authorization of certain personnel to handle or otherwise influence the component. For example, personnel functions which involve authorized control over an Accounting Form would include the entry of data into the form, the transfer of the form, the entry of the form into secure storage, etc. The persons who are assigned to such functions could potentially abuse their authorization, through the falsification, substitution, theft or destruction of the Accounting Form.

To allow for the determination of a component's vulnerabilities, the license applicant is required to identify the personnel categories of all persons who will be authorized to control a component under any circumstances. This information must be stated in the I&C Response Sheet for the component. The handling of an Accounting Form by persons other than those identified on the I&C Response Sheet would be considered a license violation if discovered by an NRC inspection team or an independent audit team.

The assessment will consider a component to be vulnerable to each person identified as having authorized control over the component, unless the MC&A Plan indicates otherwise. That is, the I&C Response Sheet for a component must specify each safeguards measure which would prevent or detect tampering with a component. Recommendations on such measures for specific component types are included in the I&C Sheets of Part III of the SF&C Guide.

A frequently recommended measure for preventing the abuse of authorized control is the multiple-man rule. This is defined as a requirement that a function be performed so that each of at least two participants can attest to its performance as authorized. For example, a multiple-man rule for the entry of data into an

Accounting Form would require that each of several persons responsible for this function be capable of detecting an attempt to compromise the form by any other participant. Such attempts might involve:

- a) Entry of false data into the form,
- b) Modification of data on the form,
- c) Removal of data from the form,
- d) Substitution of the form with a counterfeit copy,
- e) Theft of the form, or
- f) Destruction of the form.

Each participant would be required to attest through signature to the integrity of the form at the time it leaves his responsibility. This would generally be the time at which the form is:

- a) Deposited in a Secure Storage Compartment,
- b) Entered into a Pneumatic Transport System, or
- c) Handed to a courier.

The application of a multiple-man rule is modeled through the use of an "AND GATE," as illustrated in Figure III-2B above.

The assessment will grant no credit for a multiple-man rule unless it is specifically claimed by the license applicant. To claim credit for a multiple-man rule, the Authorization Schedule for the procedure in which it is used must specifically include this requirement. If the license applicant claims credit for a multiple-man rule, it will be considered a license condition subject to verification by NRC inspection teams and independent audit teams. Note that for some procedures, a multiple-man rule might be impractical, or an undue burden upon personnel. In such cases, redundant independent procedures might be used instead.

2.2 Vulnerabilities Due to Component Location

The second category of component vulnerabilities involves those persons who do not have authorized control over a component, but who could gain authorized or unauthorized access to the location of a component. This type of vulnerability would apply only to components which are physical objects, such as Accounting Forms, Reference Standards, Measurement Instruments, etc. For example, a janitor who is not authorized to handle an Accounting Form might still manage to compromise the form if he could gain access to the room in which the form is stored. The assessment will consider a component to be vulnerable to all persons who could gain access to its location, unless the I&C Response Sheet specifies some means of protection against such compromise.

Facility locations must be defined in Part I-2 of the MC&A Plan, in terms of physical barriers and fields of view for personnel monitors (e.g., closed-circuit television). The set of persons or combinations of persons who could gain access to a particular location can be divided into two subsets: those who could gain authorized access and those who could gain unauthorized access. A list of persons or combinations of persons* having authorized access to each facility location must be provided in Part I-11 of the MC&A Plan.

The assessment methodology would incorporate a formal analysis to determine which persons or combinations of persons could bypass those portions of the physical protection system (if any) which would prevent them from gaining unauthorized access to a facility location. This analysis would require inputs from the Physical

*In some cases, persons may be authorized to enter a location only when accompanied by a partner.

Protection Plan concerning guard force disposition, access controls, personnel monitors (e.g., closed-circuit television), etc. Failure to incorporate this analysis in the assessment methodology might result in the omission of some of the most critical vulnerabilities of an MC&A component.

For example, consider a key custodian who controls the key to a room for records retention, which he is not authorized to enter. If the custodian also controls the key to a Secure Storage Compartment for Accounting Forms which are stored in this room, he might be capable of compromising the forms by himself. If this vulnerability were overlooked, the assessment methodology might erroneously conclude that the forms were vulnerable only to combinations of two persons having authorized control over these components. Thus, failure to consider unauthorized access to component locations could lead to serious underestimates of component vulnerabilities. This failure could in turn lead to highly deceptive outputs at the subsystem level.

Figures III-3, III-4, and III-5 illustrate techniques for modeling the vulnerabilities of an MC&A component to compromise through its location. Figure III-3 illustrates the unit model for an Accounting Form which is unprotected against such compromise; this situation would arise if the form were left unattended on a table. Note the introduction of conventions in this figure which are used throughout the remainder of Section III.

Figure III-4 illustrates the protection of an Accounting Form by a Secure Storage Compartment and a Lock. (A separate I&C Response Sheet would be required for each of these components.) This figure introduces the concept of a "unit model chain," which represents the vulnerabilities of inter-related components. Figure III-4 also illustrates the general method for determining the personnel vulnerabilities of a component belonging to such a chain: First

$$V(AF7A) = P_{AF7A} + P_{L4}$$

Conventions:

$V(AF7A)$ = set of persons or combinations of persons who could compromise Accounting form #7, copy A.

P_{AF7} = set of persons or combinations of persons having authorized control over Accounting Form #7, copy A.

P_{L4} = set of persons or combinations of persons who could gain access to location #4.

FIGURE III-3. UNIT MODEL FOR AN UNPROTECTED ACCOUNTING FORM.

$$\begin{aligned}
 V(AF7A) &= P_{AF7A} + V(SSCB) \\
 V(SSCB) &= P_{SSCB} + (P_{L4} + V_{LKR}) \\
 V(LKR) &= P_{LKB} \\
 \hline
 V(AF7A) &= P_{AF7A} + P_{SSCB} + (P_{L4} + P_{LKB})
 \end{aligned}$$

FIGURE III-4: PROTECTION OF A COMPONENT FROM COMPROMISE THROUGH ITS LOCATION

ABBREVIATIONS: AF7A = Accounting Form #7, copy A
 SSCB = Secure Storage Compartment #8
 LK8 = Lock #8

* Contains spare keys for Lock #6
 **Contains spare keys for Lock #8

FIGURE 111-5: SELF CLOSURE OF UNIT MODEL CHAIN

generate a vulnerability equation for each component in terms of its immediate inputs, and then solve the set of equations for the component of interest.

The "AND GATE" in Figure III-4 indicates that the Secure Storage Compartment can be compromised by persons who can gain access to its location and who also have authorized control over its Lock. For the example illustrated, all keys and masterkeys for the Lock are in the possession of persons having authorized control over the Lock, with no spare keys maintained in storage.

Figure III-5 illustrates an example in which spare keys for the compartment which contains the Accounting Form are maintained in a second compartment, thus introducing an additional source of vulnerability to the previous example. Note that the spare keys for the second compartment are in turn stored in the first compartment. This example is an interesting case of a unit model chain which "closes upon itself" by forming a loop.

2.3 Vulnerabilities Due to Related Components

The third category of component vulnerabilities arises from the fact that a component might be indirectly compromised by persons who could compromise a related component, through either authorized or unauthorized means. For this reason, the I&C Sheets have been designed to elicit the identities of all components from which a particular component might be indirectly compromised, as well as all components which might prevent such compromise. Each component so identified must be described on a separate I&C Response Sheet, which will in turn reference another set of components. Thus, the I&C Response Sheets of an MC&A Plan constitute a highly interconnected network of component descriptions.

Examples of potential vulnerabilities of one component to another include:

- a) Vulnerability of a Composition Measurement Procedure to tampering with its Utility Supply Components, such as chemical reagents.
- b) Vulnerability of a Computerized or Non-Computerized Account to tampering with the Accounting Forms from which data is derived.
- c) Vulnerability of an Annunciator to tampering with the Signal Transmission Components which connect it to a Portal Switch.

Figure III-6 illustrates the vulnerability of an Accounting Form to the Quantity Measurement Procedure which it documents. That is, persons who have authorized control over the procedure might falsify the data which is entered into the form, even if they never handle the form. Similarly, the Quantity Measurement Procedure might be falsified through tampering with a Mass Measurement Instrument used in the procedure. Thus, the Accounting Form might be compromised by persons who could influence the instrument, the procedure, or the

$$V(AF7A) = P_{AF7A} + P_{L4} + V(QMP7)$$

$$V(QMP7) = P_{QMP7} + V(MMI3)$$

$$V(MMI3) = P_{MMI3} + P_{L3}$$

$$V(AF7A) = P_{AF7A} + P_{L4} + P_{QMP7} + P_{MMI3} + P_{L3}$$

FIGURE III-6: COMPROMISE OF A COMPONENT THROUGH A RELATED COMPONENT

form itself. An assessment methodology would determine the vulnerability set of the form by simultaneously solving the Boolean equations for each individual component, as indicated in Figure III-6. Note that to simplify the example, the Accounting Form and the Mass Measurement Instrument were assumed to be unprotected from their locations.

The configuration of MC&A components in Figure III-6 could be compared to an electrical circuit having three components wired in series, with a single component failure sufficient for circuit failure. The vulnerability of the Accounting Form could be limited by restricting authorized control over the three components to the same set of persons. This is an example of "consolidation of function," a powerful design tool which is generally appropriate for the allocation of personnel responsibilities to components "wired in series." Note that the separation of function for components "wired in series" may actually increase subsystem vulnerability.

In other instances, the configuration of MC&A components can be compared to an electrical circuit wired in parallel, with multiple component failures necessary for circuit failure. An example would be a Secure Storage Compartment protected by two independent Locks, each of which requires a separate key. This situation is modeled using an "AND GATE" between the two Locks, as illustrated in Figure III-7. Redundant components which are so related should be maintained under separate personnel control, so as to prevent the compromise of both components by the same person. Thus, consolidation of function is appropriate for components "wired in series," while separation of function is appropriate for components "wired in parallel." Note that guidelines for maintaining separation of function between different Locks are provided in the I&C Sheet for this component type.

$$V(SSC9) = P_{SSC9} + (P_{LK3} + V(LK1) + V(LK2))$$

$$V(LK1) = P_{LK1}$$

$$V(LK2) = P_{LK2}$$

$$V(SSC9) = P_{SSC9} + (P_{LK3} + P_{LK1} + P_{LK2})$$

FIGURE III-7 COMPONENTS "WIRED IN PARALLEL"

3.0 VULNERABILITIES OF DETECTION SUBSYSTEMS

The preceding section described the scoring rules by which an assessment methodology would determine the vulnerabilities of individual components. The present section describes the aggregation algorithms by which an assessment methodology would determine the vulnerabilities of a subsystem, as derived from the vulnerabilities of its components.

The vulnerability assessment of a detection subsystem will be based upon the general format provided in Part II-1.1.2B of the SF&C Guide. This format has been designed to facilitate the evaluation of a detection subsystem with respect to both the vulnerability and statistical parameters of the MC&A Rule. The general format decomposes a subsystem into the six basic elements illustrated in Figure III-8, each of which consists of one or more components. Note that the same modeling conventions described in the preceding section are also applicable to this figure. For example, the comparison element could be compromised through the measurement element or the reference element.

A general discussion of each element and its associated component types is provided below:

- a) The Measurement Element - This element will include the components used to determine the total measured quantity of SSNM within a control unit at the end of a detection interval. In a subsystem designed to detect the loss of SSNM in bulk form, this element may consist of a set of Measurement Procedures and Material Sampling Procedures (if applicable), as well as the Data Combination Procedure which will consolidate the results. In a subsystem designed to detect the loss of SSNM in itemized form, this element may consist of a Security Seal Inspection Procedure. Note that if no bulk measurements or item inspections are performed at the end of a detection interval, the output of the measurement element will be zero.

* Element need be described only for subsystems involving measurement of SSNM in bulk form. For other subsystems, the threshold will consist of any discrepancy between the Measurement Element and Reference Element.

FIGURE III-8: GENERAL FORMAT FOR DETECTION SUBSYSTEM DESCRIPTION.

- b) The Reference Element - This element includes the components used to determine the basis of comparison for the output of the measurement element. These components will generally include one or more Computerized or Non-Computerized Accounts containing data for a detection interval on estimated beginning inventory, transfers in, and transfers out of the control unit. The former term may incorporate the output of the measurement element from the preceding detection interval. The reference element may also include one or more Holdup Estimation Procedures to approximate the quantity of unmeasured SSNM within process or storage equipment at the end of a detection interval. A Data Combination Procedure will be used to consolidate all data associated with this element, so as to arrive at a reference quantity of SSNM or a reference list of item serial numbers.
- c) The Comparison Element - This element will consist of a Comparison Procedure used to determine the difference between the outputs of the measurement element and the reference element. In a bulk loss detection subsystem, this procedure may be a simple differencing operation between the measured quantity and reference quantity of SSNM, which will provide an estimate of inventory difference (ID). In an item loss detection subsystem, this procedure may be a simple check for discrepancies between item serial numbers and a reference list. If any such discrepancy is detected, a state of alarm is said to exist.
- d) The Threshold Determination Element - This element will include a Threshold Determination Procedure to arrive at a decision criterion for the output of the comparison element. The inputs to this procedure will include the desired probabilities of detection and false alarm, the control quantity, and the results of a formal Measurement Error Analysis and Material Sampling

Error Analysis (if applicable). Note that the threshold determination element need not be described for a detection subsystem based upon a Security Seal Inspection Procedure, as the action threshold will be any discrepancy between the results of this procedure and the reference. This action threshold is implicitly contained within the comparison element of such subsystems.

- e) The Threshold Test Element - This element will consist of a Threshold Test Procedure to determine whether or not the output of the Comparison Procedure exceeds the output of the Threshold Determination Procedure. If the action threshold is found to have been exceeded, a state of alarm is said to exist. Note that this element need not be described for a detection subsystem based upon a Security Seal Inspection Procedure, for the same reason mentioned under d) above.
- f) The Response Initiation Element - This element will include an Alarm Review Procedure to be performed directly by the persons who detect an alarm. This procedure will involve a check for errors in the data and calculations which led to the alarm. The response initiation element will also include an Alarm Notification Procedure, by which the appropriate authorities will be notified of an alarm which cannot be resolved via an Alarm Review Procedure. These authorities must include facility MC&A and physical protection officials, as well as the NRC regional headquarters. This element represents the interface between a detection subsystem and its corresponding response subsystem.

A detection subsystem can be compromised through the compromise of any one of the elements described above. That is, the compromise of a single element will prevent the initiation of a response to a material loss. (This fact is reflected by Figure III-8 above, which includes no "AND

GATES" between elements.) Thus, the vulnerability set of a detection subsystem can be determined by a separate assessment of each element, followed by the combination of the resulting vulnerability sets. This principle can be symbolically stated as follows:

$$V(DS) = V(ME) + V(RE) + V(CE) + V(TDE) + V(TTE) + V(RIE)$$

A subsystem description provided in Part II-1.1.2 must reference the I&C Response Sheets for components which are directly related to each of the six elements. These sheets will in turn reference other I&C Response Sheets for components which are indirectly related to one or more of the elements. The resulting network of I&C Response Sheets for each element will constitute a unit model chain. Each such chain can be represented through a set of Boolean equations, the solution of which will yield the vulnerabilities of a subsystem element. Thus, the vulnerabilities of a subsystem element are determined in the same manner as those of individual components.

A detection subsystem will undergo two assessments, to determine:

- a) Persons or combinations of persons who could cover-up a loss of SSNM for at least 24 hours for Type A material, or at least three working days for Type B material.
- b) Persons or combinations of persons who could cover-up a loss of SSNM for at least eight weeks.

Assessments a) and b) are respectively referred to as first and second order assessments, and will each provide a separate vulnerability set as output. A first order assessment of a subsystem will generally incorporate only those components related to the detection of a loss between the beginning of a detection interval and the scheduled time of

completion for the Threshold Test Procedure.* A second order assessment will incorporate all components considered by the first order assessment, and will also incorporate any Reconciliation Procedures which might serve to detect a loss after the scheduled completion time of the Threshold Test Procedure, within 8 weeks of the beginning of a detection interval. A Reconciliation Procedure involves a periodic check for discrepancies between redundant data sources, which might reveal the falsification of data. Such procedures might serve to uncover a diversion scenario in which an adversary manages to falsify only one of several redundant data sources used in a detection subsystem. Thus, certain adversaries who could prevent the detection of a diversion by the Threshold Test Procedure might later be detected by a Reconciliation Procedure.**

* In the case of a subsystem designed to detect the loss of SSNM in itemized form, a first order assessment will incorporate only those components related to the detection of a loss between the beginning of a detection interval and the scheduled time of completion for the Comparison Procedure.

** Some detection subsystems may also include Reconciliation Procedures which would detect a diversion before the performance of a Threshold Test Procedure. Such procedures would be incorporated in both the first and second order assessments.

3.1 First Order Assessment

The first order assessment of a detection subsystem can best be described in terms of a unit model chain for each element of a hypothetical subsystem. These chains are illustrated in Figures III-9 through III-17. Note that these figures have been simplified through the omission of the personnel symbols used in previous figures. Each component identified in these figures would be described in an I&C Response Sheet of the license applicant's MC&A Plan. A discussion of each component type identified in these figures can be found in an I&C Sheet in Part III of the SF&C Guide. The following comments on the depiction of the measurement element in the first three figures should assist in the comprehension of a first order assessment:

- a) Because of the difficulty involved in illustrating the entire measurement element in a single figure, various portions or "modules" have been separated from the main diagram in Figure III-9, and illustrated in subsequent figures.
- b) Accounting Report #2 in Figure III-9 is the set of information which describes the execution of Quantity Measurement Procedure #2. Accounting Form #2, copy A is the physical medium by which this information is transmitted for use in Data Combination Procedure #1. Note that the unit model of the form used in the first order assessment would include only those vulnerabilities by which the form could be compromised prior to its use in the Data Combination Procedure (e.g., vulnerability to a courier who delivers the form). Vulnerabilities by which the form could be compromised after this time are incorporated into the second order assessment described below. (To simplify the figures, the protection of Accounting Forms by Secure Storage Compartments and Locks has not been illustrated.)

ABBREVIATIONS: ACCTG. = Accounting
 COMB. = Combination
 MSMT. = Measurement
 P. = Procedure

FIGURE III-9: MEASUREMENT ELEMENT OF A HYPOTHETICAL DETECTION SUBSYSTEM

NEW ABBREVIATIONS:

CALIB. = Calibration
 COMP. = Compartment
 INST. = Instrument
 REF. = Reference
 STD. = Standard

FIGURE III-10: MODULE A FOR MEASUREMENT ELEMENT

FIGURE 111-11: MODULE B FOR MEASUREMENT ELEMENT

NFW ABBREVIATION: NON-CPTZD. = Non-Computerized

- * This node refers to the unit model chain for the measurement element of the preceding detection interval.
- ** The results of the Holdup Estimation Procedure for both the current and preceding detection interval will be used in the reference element.

FIGURE 111-12: REFERENCE ELEMENT OF A HYPOTHETICAL DETECTION SUBSYSTEM.

FIGURE III-13: MODULE D FOR REFERENCE ELEMENT

FIGURE 111-14: COMPARISON ELEMENT OF A HYPOTHETICAL DETECTION SUBSYSTEM

NEW ABBREVIATION: DET. = Determination

FIGURE III-15: THRESHOLD DETERMINATION ELEMENT OF A HYPOTHETICAL DETECTION SUBSYSTEM

FIGURE 111-16: THRESHOLD TEST ELEMENT OF A HYPOTHETICAL DETECTION SUBSYSTEM

FIGURE III-17: RESPONSE INITIATION ELEMENT OF A HYPOTHETICAL DETECTION SUBSYSTEM

- c) Redundant Composition Measurement Procedures in Figure III-9 are used in the hypothetical subsystem to protect the Data Combination Procedure from falsification. Such redundancy can be a useful alternative to a multiple man rule, especially for procedures in which a multiple man rule would be difficult to implement. Because a Composition Measurement Procedure involves a large number of minute details, it would be very difficult for several persons to monitor one another throughout.
- d) Because the two Composition Measurement Procedures in Figure III-9 are "wired in parallel," the components involved in the respective unit model chains should be maintained under separate controls. For example, the two procedures should utilize separate Reference Standards stored in separate Secure Storage Compartments, with no persons having keys to both compartments. A person who could gain access to both Reference Standards could compromise both Measurement Procedures, thus defeating the value of redundancy. Note that failure to carry the assessment to the level of detail indicated in Figure III-11 would exclude such vulnerabilities from the output of the assessments, and could therefore produce highly misleading results.

3.2 Second Order Assessment

The second order assessment of a detection subsystem will incorporate all components included in the first order assessment, and will also incorporate the Reconciliation Procedures which might detect a diversion after the time frame associated with the first order assessment. Thus, the unit model chains used in the first order assessment will be augmented with unit models for the Reconciliation Procedures described in the MC&A Plan.

The I&C Sheet for Reconciliation Procedures describes various types of cross-checks between redundant data sources. One type of Reconciliation Procedure would be a check for discrepancies between redundant copies of an Accounting Form. Figure III-18 illustrates the application of a Reconciliation Procedure to Accounting Form #2, copy A, from Figure III-9. Figure III-18 is explained in terms of its applicability to the hypothetical cover-up scenario described below:

A courier responsible for the delivery of copy A to the persons who perform Data Combination Procedure #1 has diverted SSNM. To cover-up this diversion, he substitutes a bogus copy A for the original copy A. This act results in a subsystem failure to detect the diversion within the time frame associated with the first order assessment. As reflected by the "AND GATE" in Figure III-18, the continuation of the cover-up through the time frame associated with the second order assessment would also require the compromise of Reconciliation Procedure #1. This procedure involves a check for discrepancies between copy A and copy B. Figure III-18 suggests two possible methods for an adversary to prevent the detection of a discrepancy by the Reconciliation Procedure:

- a) Resubstitute the original copy A for the bogus copy A, or
- b) Substitute a bogus copy B for the original copy B, such that bogus copy B matches bogus copy A.

- * This node represents vulnerabilities of Copy A prior to its use in Data Combination Procedure #1.
- ** This node represents vulnerabilities of Copy A between its use in Data Combination Procedure #1 and Reconciliation Procedure #1.

FIGURE III-18: RECONCILIATION PROCEDURE

As indicated in Figure III-18, the second order assessment requires the dichotomy of the unit model for copy A, on the basis of which persons could compromise the form at different times. The figure suggests that to the extent possible, control over copy A prior to its use in the Data Combination Procedure should be separated from:

- 1) Control over copy A after its use in the Data Combination Procedure, and
- 2) Control over copy B.

Another important consideration illustrated in Figure III-18 is the common vulnerability of both copy A and copy B to compromise through the procedure which they document. That is, the persons who perform Quantity Measurement Procedure #8 could compromise all copies of the Accounting form for this procedure, in which case a Reconciliation Procedure between redundant copies would not detect a discrepancy. Thus, the origination of measurement data is a critical function which should be protected through the use of a multiple-man rule or the use of redundant measurement procedures.

IV. FRAMEWORK FOR STATISTICAL ASSESSMENT

1.0 OBJECTIVES

The statistical assessment package is a set of simulations which can be used by a license applicant or an NRC license reviewer to verify the statistical performance of detection, response and assurance subsystems. The statistical assessment package is designed to:

- a) Determine the performance of each MC&A subsystem as specified by the license applicant in the MC&A Plan.
- b) Use only data provided by the license applicant in the MC&A Plan.
- c) Simulate the MC&A subsystems at the level of basic physical property measurements.
- d) Consider diversion scenarios as will be specified for the design basis threat.

As license applicants respond to the prompt detection requirements of the MC&A Upgrade Rule, they will implement subsystems which are more complex than the simple inventory difference types which have been implemented to date. These newer types of detection subsystems may rely on process models, complex data smoothing algorithms, complex threshold determination procedures, etc. The predictions which arise from the performance analyses used for a simple inventory difference model will predict the performance of these complex techniques if the techniques have been correctly implemented. The purpose of an assessment tool, however, is not to assess how good a system might be, but to predict how good it is.

Wherever possible, the MC&A subsystems are simulated at the level of basic physical property measurements. No use is made of derived quantities such as short or long term systematic errors. The effectiveness of replicate measurements and/or replicate samples in reducing "overall" subsystem error is accounted for by processing simulated replicate data using the procedures specified by the license applicant. For example, if 10 measurements are to be made on a single

sample, the simulation will produce 10 separate "measured" values. Each of these "measured" values would correspond to the result of one single measurement and would be determined by random draw from the distribution for a single measurement.* Each of the 10 measured values will be passed to the next stage in the simulation as a separate measured value. This data is then processed using the methods specified in the applicant's MC&A Plan.

Several objectives are achieved by simulation at the basic measurement level. These are:

- a) The fidelity of the simulation to the design and operation of the subsystem is assured.
- b) The simulation user does not need to possess a high degree of statistical analysis abilities.
- c) The simulation provides outputs corresponding to each stage of the applicant's data processing methods, which can be used to verify the applicant's analyses provided in Part IV of the MC&A Plan.
- d) Correlations between measurements are automatically accounted for.

This type of statistical assessment produces two types of outputs; component performance and subsystem performance. Components are the procedures and equipment which comprise the MC&A subsystem. Typical components include Volume Measurement Instruments, Composition Measurement Procedures, Data Combination Procedures, and Threshold

*This type of simulation should be contrasted to ones in which the means and variances of the instrument distributions are used to compute procedure means and variances which are then used to compute measurement subsystem performance, etc.

Determination Procedures.* The determination of the performance of these components constitutes a "component scoring rule."

The determination of subsystem performance through the use of the statistical assessment package is an aggregation of the performance of the individual components. By using the simulations described below, this aggregation is performed so as to capture the effect of common measurement data.

The remainder of this section describes the statistical assessment packages for bulk and item subsystems, as well as for the combined performance of the two. These simulations would be used for the assessment of both abrupt and cumulative detection performance. All of the data required by the assessments will be contained in the license applicant's MC&A Plan.

*A complete list of the components for MC&A subsystems can be found in Part III of Standard Format and Content Guide: Component Intent and Content Sheets, R. S. Schechter, LLNL and I. J. Sacks, AIP, 11 February 1981, UCID-18953, Pt. III.

2.0 OUTPUTS OF STATISTICAL ASSESSMENT PACKAGE

The statistical assessment package will be used to validate the performance of the MC&A detection, response and assurance subsystems. The performance requirements of the MC&A Upgrade Rule are shown in Table IV-1. As can be seen from the table, there are two general detection intervals for bulk material, abrupt and cumulative. There are also two types of detection subsystems specified by the rule. These are subsystems for material in bulk form and subsystems for material packaged in itemized form.

Table IV-1. Statistical Performance Requirements of MC&A Rule
(December 16, 1980 Version)

<u>RULE SECTION</u>	<u>STATISTICAL PERFORMANCE REQUIREMENT</u>	<u>TIME PERIOD</u>	<u>COVERAGE</u>
<u>70.83 (Detection)</u>			
(a)(4)(i)	$P_d = .99$ for 5 FKG Loss	Type A Material: 24 hours	Each Control Unit
(a)(4)(ii)	$P_d = .90$ for Control Quantity		Each Control Unit
(a)(4)(iii)	P_{fa} = sufficiently low to allow for adequate resolution		Each Control Unit
(c)(1)(i)	$P_d = .90$ for 5 FKG	Type B Material: 3 working days	Plantwide
(d)(1)(i)	$P_d = .90$ for 5 FKG	Cumulative over 1 year	Each Control Unit
<u>70.86 (Assurance)</u>			
(f)(5)(i)	$2\sigma_{ID} \leq 0.5\%$ Throughput	Inventory Period	Plantwide
(f)(5)(ii)	$2\sigma_{ID} \leq .200$ FKG	Single Shipment or Receipt	Each Shipment or Receipt
(f)(5)(iii)	$2\sigma_{ID} \leq 2.0$ FKG	Cumulative over 1 year	Sum of Shipments and Receipts

The simulations will produce performance outputs at both the component level and the detection subsystem level. The output at the component level will be performance of a Measurement Procedure (e.g., accuracy of a Volume Measurement Procedure) which arises from the basic physical property measurement accuracies (e.g., measurement of differential pressure). At the detection subsystem level, the simulations will produce aggregate measures of performance such as the probability of detection for a given loss quantity.

Two types of simulations must be provided to determine compliance with the rule. The first of these will determine the performance of bulk loss detection subsystems over periods corresponding to the abrupt and cumulative requirements, whereas the second will determine the performance of item loss detection subsystems. The outputs of each of these simulations are described below. Also described is a method for determining the combined detection capability for material contained in both bulk and itemized form within the same control unit and within the same material description category.

The simulation methods described below are sufficiently general to assess compliance with the relevant provisions of both S70.83 (detection) and S70.86 (assurance), although the examples used will be referenced to the former. Note that compliance with S70.83 (c)(1) will not require a separate simulation, but will be assessed as described under Section V-2.0 below.

2.1 Outputs for Bulk Loss Detection Subsystems

The bulk loss subsystem simulation* will provide the following outputs:

- a) Histograms of the performance of each Measurement Procedure.
- b) A histogram of the subsystem loss indicator for various process conditions.
- c) Histograms of the loss indicator for various levels of abrupt or protracted diversion (depending on subsystem to be analyzed for various process conditions).
- d) The action (detection) threshold as specified by the license applicant for various process conditions.
- e) The detection probabilities for various process conditions and diversion levels.
- f) The false alarm probabilities.**

These simulation outputs are shown schematically in Figures IV-1 through IV-5. The probability distributions shown in these figures would result from the simulation of the effects of measurement (random and bias) errors, measurement procedures, number of samples, data processing, etc. Since a simulation is a finite set of experiments, the actual results achieved are not the continuous curves as shown in Figures IV-1 through IV-5. Figure IV-6a is the actual histogram of volume estimates which results from 300 runs of a Monte-Carlo simulation of differential pressure volume measurement.*** (This corresponds to the schematic representation shown in Figure IV-1.) The ragged shape of this distribution is due to the non-infinite number of samples taken. Figure IV-6b is the cumulative distribution of the same estimates.

* The structure of the bulk loss subsystem simulation will be described in Section 3.1.

** False alarm rate is false alarm probability times the number of detection intervals per unit time.

***Described in more detail in subsection 3.1 below.

FIGURE IV-1 - COMPONENT PERFORMANCE

FIGURE IV-2 - SUBSYSTEM PERFORMANCE (NO LOSS)

FIGURE IV-3 - SUBSYSTEM PERFORMANCE

FIGURE IV-4 - ACTION THRESHOLD

FIGURE IV-5 - DETECTION AND FALSE ALARM PROBABILITY

(a) HISTOGRAM OF VOLUME ESTIMATES

(b) CUMULATIVE DISTRIBUTION FOR VOLUME ESTIMATES

FIGURE IV-6 - RESULTS OF VOLUME MEASUREMENT PROCEDURE SIMULATION

The confidence in the parameters computed by the simulation will depend on the number of simulation experiments (or runs) which are used to generate the histograms. The statistics of the computed parameters are generally assumed to be Gaussian. Hence, standard tests such as Student t and Chi-Square can be used to determine the confidence in these parameters.

The sample variance, σ_s^2 , of the mean of a distribution determined by a Monte-Carlo Simulation can be shown to be:

$$\sigma_s^2 \propto \frac{1}{N}$$

where: σ_s^2 is the sample variance, and
N is the number of experiments (or runs).

Figure IV-7 shows the standard deviation of the mean of the volume estimates as a function of the number of runs. This graph clearly shows the $1/\sqrt{N}$ reduction of the standard deviation.

The number of runs, N, which are required for achieving a specified relative error in the detection and false alarm probabilities can be determined by the equation.*

$$N \approx \frac{9(1-p)}{pd^2}$$

Where p is the value of the probability we wish to determine and d is the relative error.

* Yu. A. Shreider, Ed., the Monte Carlo Method, No. 5 in The Series Spravo Matematicheskaya Biblioteka, Fizmatgiz, Moscow, 1962, (Translation: G. J. Tee, Pergamon Press, 1966).

FIGURE IV-7 - VARIANCE REDUCTION

False alarm probabilities are generally quite small (e.g., 0.001). Thus, it is impractical to perform enough tests to determine them with high confidence. For example, in order to estimate a p of 0.001 within a confidence interval of 0.0005 to 0.002, a total of 4000 runs must be made. The Gaussian assumption which underlies the preceding equation requires that $pN \gg 1$.

Since it is not practical to simulate subsystem performance to the accuracy necessary to determine false alarm probability, another approach is necessary. This approach is based on the use of the intermediate results of the simulation. These results can be compared to the values specified by the license applicant in the supporting analysis described in Part IV of the MC&A Plan. For example, the action threshold calculated by the applicant should be compared to the action threshold based on the measurement distributions determined by the simulation.

There is only one way, however, to be absolutely sure of the claimed detection performance. That is to run the subsystem simulation for a sufficient number of times to verify the claimed performance. The number of runs necessary for P_d is reasonable; this parameter should, therefore, be verified by the simulation.

2.2 Outputs for Item Loss Detection Subsystems

A Monte Carlo simulation is not necessary for item loss detection subsystems since their performance can be predicted on the basis of a set of equations. These equations will determine the probability of detecting the loss of at least one item, given the number of items covered by the subsystem, the number of items inspected, and the presumed loss quantity. Thus, the assessment of a Statistical Sampling Plan corresponds to a reanalysis of the applicant's procedure for determining an item loss. Figure IV-8 shows typical detection performance which might result from the analysis of an item loss detection subsystem. (If an item loss detection subsystem involves the sampling and analysis of bulk material taken from items, the performance of the material measurements would be made using the bulk loss simulations described in this report.)

A subsystem based upon a Statistical Sampling Plan for items is not subject to the statistical "noise" in measurements which produces false alarms in bulk loss detection subsystems. However, it is possible that a miscount of items could be made or that a serial number might be misread. This type of alarm is difficult to simulate since it relies on a model of the performance of the human operator. If such a model can be provided, an estimate of the false alarm probability can be made using the type of probability algebra incorporated in Level 2 of the Structured Assessment Analysis.*

*The Structured Assessment Approach, Version I, U.S. Nuclear Regulatory Commission, NUREG/CR-1233, Lawrence Livermore National Laboratory, UCRL-52735, October 1979.

FIGURE IV-8 - TYPICAL ITEM LOSS DETECTION SUBSYSTEM PERFORMANCE

2.3 Outputs for Joint Performance of Bulk and Item Detection Subsystems

The joint performance of bulk and item detection subsystems must be determined for any CU in which a single material description category is contained in both bulk and itemized form. Statistical assessments can be used to individually determine bulk and item detection performance parameters, as described in the previous subsections. Using this information for each detection subsystem, an assessment module will calculate the overall detection probability for a diversion which involves the "optimal" adversary strategy for apportioning the diversion between SSNM in bulk and itemized form. That is, the assessment will determine the probability of a theft being detected by either detection subsystem, given that the adversary has chosen the best possible strategy to minimize his detection probability.

The optimal strategy for a combined theft of material in bulk and itemized form can be determined using the detection probability curves for the individual subsystems for bulk and items. Figures IV-9a and IV-9b schematically show probability of detection (P_d) versus amount diverted for the bulk and item loss detection subsystems, respectively. Figure IV-9c shows the overall probability of detection for a combined loss of 5 FKG against the amount taken in itemized form. That is, Figure IV-9c indicates the probability of a diversion being detected by either subsystem when the adversary has taken X FKG in item form and 5-X FKG in bulk form. The licensee is in compliance with the rule only if $P_d > .99$ at the lowest point of this curve, which corresponds to the "optimal" adversary strategy.

Figure IV-9c can easily be derived from the information contained in Figures IV-9a and IV-9b, and the use of the following formula:

$$P_C (5 \text{ FKG}) = 1 - (1 - P_B (X \text{ FKG})) (1 - P_I (5 - X \text{ FKG}))$$

FIGURE IV-9 - OVERALL DETECTION PERFORMANCE FOR COMBINED ITEM AND BULK DIVERSION OF 5 FKG

in which

P_C (5 FKG) = probability of detecting a combined loss of 5 FKG of SSNM,

P_B (X FKG) = probability of detecting the loss of X FKG of SSNM in bulk form.

P_I (5-X FKG) = probability of detecting the loss of 5-X FKG of SSNM in itemized form.

The above equation can be explained as follows: The probability of detecting a combined loss of 5 FKG of SSNM is equal to one minus the probability of not detecting the loss by either subsystem.

The detection performance data for a bulk loss detection subsystem as shown in Figure IV-9a will be determined by simulating losses in increments up to 5 FKG. The curve labeled "bulk" in Figure IV-10 shows the simulated performance of a hypothetical bulk loss detection subsystem. This subsystem is designed to detect the loss of 5 FKG with a probability of 0.99. To achieve this detection probability, an inventory is performed once every eight hours. The false alarm probability was set equal to 0.01 for this example.

In addition, the CU represented in Figure IV-10 contains 50 FKG of material stored in 100 tamper-sealed containers. The item loss detection subsystem for this material is designed to detect the loss of at least one container with probability 0.99, given a loss of 5 FKG (i.e., a loss of 10 canisters). To achieve this detection capability, the license applicant will select 36 containers at random and check their security seals and containment integrity. The performance of this item loss detection subsystem is labeled "item" in Figure IV-10. (This performance was determined using the equation in Section 3.2 below.)

FIGURE IV-10 - COMPOSITE DETECTION PERFORMANCE

The combined detection probability which arises from various losses apportioned between items and bulk material is also shown in Figure IV-10. The dashed curve shows that an adversary could steal between 4 FKG of items and 1 FKG of bulk to 1 FKG of items and 4 FKG of bulk and still be detected with less than a 0.99 probability. The minimum detection probability of 0.968 occurs for a theft of 2 FKG of items and 3 FKG of bulk.

2.4 Overall Facility False Alarm Rate

Alarms from a detection subsystem can be thought of as belonging to one of three major categories. These categories are shown in Table IV-2 along with typical causes.

Table IV-2. Alarm Categories

<u>ALARM CATEGORY</u>	<u>TYPICAL CAUSES</u>
GENUINE ALARM	MATERIAL LOSS
FALSE ALARM	STATISTICAL VARIATIONS IN MEASUREMENTS, EXCESSIVE HOLDUP
NUISANCE ALARM	TRANSCRIPTION ERRORS, PROCESS UPSET, ARITHMETIC ERRORS, ETC.

False alarms are traditionally defined to arise from statistical fluctuations, whereas nuisance alarms arise from procedural errors. It is important to realize that an alarm provides no information as to whether its cause is genuine, false, or nuisance. The high detection probabilities specified in the MC&A Rule coupled with the short (1 to 3 days) detection intervals will force relatively high rates of alarm even in the absence of diversion. The subdivision of the plant into control units will also create a high overall false alarm rate.

Alarms from individual subsystems will be cumulative on a facility-wide basis. That is, if a facility includes N subsystems, and the false alarm rate* of subsystem i is denoted FAR_i, then the overall (collective) facility false alarm rate will be:

$$FAR = \sum_{i=1}^N FAR_i$$

The rate of nuisance alarms depends upon human factors considerations which would be difficult to evaluate in an objective manner. This source of alarms is not considered by the statistical assessment package. However, the license applicant will be assessed in terms of his ability to resolve each source of nuisance alarms, as described in Section V-3.0 below.

*The false alarm rate for an individual subsystem is equal to the false alarm probability times number of detection intervals per unit time.

3.0 DETAILS OF STATISTICAL ASSESSMENT

This section discusses the packages for the statistical assessment of the various subsystems which will be described in a license applicant's MC&A Plan. Three types of simulation are discussed. These simulations are designed to assess:

- 1) Bulk Loss Detection Subsystems
- 2) Item Loss Detection Subsystems
- 3) Response Subsystems

The inputs and simulation structure will be described for each of the packages listed above.

Note that the discussion of 1 and 2 above will apply to subsystems used to detect inventory differences or shipper/receiver differences (as required by S70.86 (f)), in addition to detection subsystems used to comply with S70.83. The discussion of 3 above will apply to subsystems used to investigate inventory differences or shipper/receiver differences (as required by S70.86 (g)), in addition to response subsystems used to comply with S70.85.

3.1 Assessment of Bulk Loss Detection Subsystems

The statistical assessment package used to verify the performance claimed by an applicant for detection subsystems designed to meet the bulk loss detection provisions of the MC&A Rule is described in this subsection. This package is based on a Monte Carlo simulation which uses as inputs the data specified by the license applicant in his MC&A Plan. The statistical assessment package produces two types of output. The first of these is the performance of each MC&A *measurement component in the subsystem*. *This component performance* will be determined from the uncertainties in the basic physical property measurement processes. Thus, this portion of the analysis is a component scoring rule and can be used to check the performance claimed for a measurement procedure using the measurement instrument data as input. The second output will be a histogram of the applicant's loss indicator for a variety of process conditions and diversion scenarios. These scenarios will be under the control of the assessor. The purpose of the statistical assessment package is to verify that the performance claims made by an applicant are valid. The package will allow the verification of the statistical performance beginning with the results of basic Measurement Procedures, through Data Combination Procedures, up to the detection and false alarm probabilities. The assessment will not rely on statistical analysis models for calculation of variances but will instead simulate the actual operation of the detection subsystem. This subsection will briefly describe the inputs, their relationship to the SF&C Guide,* and the internal structure of the simulation package.

* The assumption is made that the SF&C Guide will follow the basic design described in Section I above.

The source of all of the data used in the statistical assessment is the license applicant's Material Control and Accounting Plan. The data provided in the plan is of four type :*

- 1) MC&A System Overview (Part I)
- 2) Subsystem and Program Descriptions (Part II)
- 3) I&C Response Sheets (Part III)
- 4) Supporting Analyses (Part IV)

The analysis of any one of the detection subsystems identified in Part II of the MC&A Plan is based on a simulation of the details of the detection subsystem provided in Part III for the processing conditions provided in Part I.

The basic detection subsystem format specified in Part II of the SF&C Guide provides the framework around which the input data is configured. This format is shown in Figure IV-11.

Each of the six elements can be expanded into a set of components, using the I&C Response Sheets provided by the license applicant. For example, Figure IV-12 shows the expansion of the measurement element into the components relevant to the statistical analysis.**

The output of the measurement element is the result of a Data Combination Procedure. This procedure will generally process the results of a Quantity Measurement Procedure and a Composition Measurement Procedure to yield the specific SSNM isotope quantity

* The contents of these parts of the MC&A Plan are described in Section I of this paper.

** The detailed decomposition of each element into its component is given in Appendix I.

FIGURE IV-11 - GENERAL FORMAT FOR DETECTION SUBSYSTEM DESCRIPTION

FIGURE IV-12 - EXPANSION OF MEASUREMENT ELEMENT

values used in the detection subsystem. In some cases, the quantity and composition measurement data will not be processed by the Data Combination Procedure, but will be simply passed through the data combination algorithms which are part of the comparison element.

The components which comprise the measurement element will be described by the applicant on a set of I&C Response Sheets.*

Typical components of this element include:

- Quantity Measurement Procedures
- Composition Measurement Procedures
- Volume Measurement Instruments
- Mass Measurement Instruments

By using the I&C Response Sheets, errors for Quantity Measurement Procedures can be derived from the basic error sources in directly measured physical parameters. The basic error sources for a Quantity Measurement Procedure arise from the thermal noise and calibration errors associated with Measurement Instruments. That is, simulated values will be drawn from a distribution defined by the accuracy parameters specified on the I&C Response Sheets for the Measurement Instruments. For example, volume "measurements" might be determined from simulated differential pressure measurements, using information from an I&C Response Sheet for a Volume Measurement Instrument.

In contrast to quantity measurements, composition measurements will not be simulated at the basic physical parameter level, but will be simulated at the Composition Measurement Procedure level. That is,

*Examples of partially completed I&C Response Sheets are included in Appendix II below.

simulated values for a composition measurement will be drawn directly from a distribution defined by the accuracy parameters specified on the I&C Response Sheet for a Composition Measurement Procedure. The reasons for this will be explained below.

The statistical assessment package is designed to duplicate the actual measurements and actual data processing which will take place at a facility. In order to maintain a faithful simulation of the operation of the detection subsystems at the facility, the measurements are simulated at the basic physical property level, if possible.* The results of these simulated measurements are then propagated through a duplication of the actual data processing operations as specified by the license applicant. This is shown schematically in Figure IV-13. Thus, the only "simulated" portion of the applicant's detection subsystem is measurement data.

There are two basic types of measurements in a bulk loss detection subsystem: quantity measurement and composition measurement. Quantity Measurement Procedures generally involve the use of a small number of Measurement Instruments, which can be well characterized. The measured values which arise from these procedures can be determined by propagating the measured physical values through the relatively simple steps in the procedure. Composition Measurement Procedures, however, generally involve a series of complex steps including dilution, titration, measurement, interference removal, etc. The measured values which result from this type of procedure are more difficult to determine through the use of a simple simulation. Also, the multi-dimensionality of the measurement procedure requires that a simulation which starts with basic measurements be exercised an excessive number of times to achieve

*Composition measurements are simulated at the procedure level.

FIGURE IV-13 - SIMULATION CONCEPT

reasonable accuracy for the composition "measurement." The large number of noise sources also tends to cause the result of a Composition Measurement Procedure to be normally distributed.

For these reasons, we have chosen to generate the measurements from a Quantity Measurement Procedure at the physical property level of the Quantity Measurement Instrument and the "measurements" from a Composition Measurement Procedure at the level of the isotopic or chemical variable measured. The two types of simulation are shown schematically in Figure IV-14. As can be seen from this figure, the values of the measurements used in the statistical assessment package will be drawn from random number distributions for basic instrument accuracy for quantity measurements, and for procedure accuracy for composition measurements. By simulating at these levels, it is possible to provide distributions for Measurement Procedures independent of the use that will be made of the data. Each of the simulated measurements is then stored and used in all following data processing operations. In this way, correlations produced by use of common measurement data are inherently captured. This technique removes the requirement for complex mathematical error propagation equations which generally require approximations or distributional assumptions in order to be solved.

The complete set of simulated measurement data is processed through duplicated data processing operations for a complete detection interval. The result of the detection test for this interval is then one sample of what might happen at a facility using this detection subsystem for the specific process at any given time. In order to generate a statistically meaningful result, the entire simulation/duplication is repeated many times. On each replication new measurement values are drawn from the random number distributions which simulate the measured values.

(a) QUANTITY MEASUREMENT PROCEDURE SIMULATION

(b) COMPOSITION MEASUREMENT PROCEDURE SIMULATION

FIGURE IV-14 - MEASUREMENT PROCEDURE SIMULATION

The only statistical analysis required for this type of simulation is a set of subroutines to generate histograms and compute the moments of these histograms.

More detail will now be provided to further explain the operation and structure of the front end of the statistical assessment package. An example will be used to illustrate the simulation structure.

Process Model

The process model of Figure IV-13 above is derived from the description of the Measurement Instrument and Procedure on their respective I&C Response Sheets. The process model must give the physical parameters which will be measured in terms of the basic process variables. In the example, the basic process variables are the volume and density of the solution in the tank. These two parameters must be mapped into the physical properties, i.e., differential pressures ΔP_a and ΔP_b , which are sensed by the "bubbler" system (Figure IV-15):

$$\Delta P_a = g \rho l_0''$$

$$\Delta P_b = g \rho h$$

where g = acceleration due to gravity and ρ = density of the solution.

As can be seen from the above equation, the values of the differential pressure depend on the density of the solution and the height of the solution in the tank. The height of the solution is determined by the tank cross sectional area and the tank heel as follows:

$$h = \frac{V}{B} - a$$

FIGURE IV-15 - PNEUMATIC DENSITY/HEIGHT MEASUREMENT SYSTEM

where

h = the height of solution

a = the tank heel*

b = the tank cross section area**

V = volume

The volume of solution is a basic input to the Monte Carlo simulation and is not treated as a random variable. The constants a and b, however, are determined by the license applicant through the use of a Calibration Procedure. Thus, a and b are random variables whose value is fixed for any single simulation run, but vary from run to run. The density of the solution is an input to the simulation.

Process losses or diversions, V_D , are input into the simulation by the subtraction of a volume of solution from the volume before computation of the solution height:

$$V = V_T - V_D$$

The simulation of the process model portion of the simulation is shown in Figure IV-16.

Measurement Element Simulation

The measurement simulation shown in Figure IV-17 adds measurement noise to the parameters computed by the process model. The value of this noise is determined by the descriptions provided on the appropriate I&C Response Sheets. The Quantity Measurement Procedure

*The heel is the volume of solution below the lowest of the pressure tubes.
**For simplicity in this example, a constant cross section has been used.

NOTES:

*Allows for Substitution Scenarios

**1 Value for each Simulation Run

+Normal Distribution is assumed, unless Licensee specifies otherwise.

$\tilde{a}$ indicates simulated value of a

FIGURE IV-16 - PROCESS MODEL SIMULATION

FIGURE IV-17 - QUANTITY MEASUREMENT PROCEDURE SIMULATION

I&C Response Sheet states that 10 measurements are made of differential pressure. Thus, the simulation will generate 10 simulated "measured" values of ΔP_a and ΔP_b . The value of the bias used is held constant in the generation of these 10 values, and is drawn from a distribution which represents the results of the Calibration Procedure for the Volume Measurement Instrument.

The composition of the solution in the tank is determined by a Composition Measurement Procedure described on the appropriate I&C Response Sheet. The block diagram of the simulation for the set of measured values which are generated by this procedure is shown in Figure IV-18. Notice that the simulation does not simulate the Composition Measurement Procedure at the basic physical property level.

Comparison Element Simulation

The Comparison Procedure as specified by the license applicant is duplicated in this part of the simulation. This procedure will be described in terms of a set of equations provided by the applicant on an I&C Response Sheet for a Comparison Procedure. The simulation of this procedure is shown in Figure IV-19. The data processing equations use the results of the measurement simulation described above along with data to compute a loss indicator. This portion of the simulation is exercised once per simulation run and hence produces one value of the loss indicator and an updated process state estimate for each run.

Reference Element Simulation

The reference data used by the Comparison Procedure is contained in the reference element. The source of this data is contained in an I&C Response Sheet for a Computerized Account. This sheet will

FIGURE IV-18 - COMPOSITION MEASUREMENT PROCEDURE SIMULATION

*AN ESTIMATION FILTER PRODUCES A STATE ESTIMATE AND A COVARIANCE OF THE STATE ESTIMATE. THE COVARIANCE WOULD BE USED IN THE THRESHOLD DETERMINATION PROCEDURE.

FIGURE IV-19 - COMPARISON ELEMENT SIMULATION

specify the exact data used as the reference data. In the example, the Estimation Filter uses the prior estimate of the process state. Thus, the reference element is loaded with the results from the Comparison Procedure from the previous update time. The simulation of the reference element is shown in Figure IV-20.

Threshold Determination Element Simulation

The Threshold Determination Procedure specified by the applicant would be duplicated in the simulation. In the example, the inputs include the covariance matrix from the Estimation Filter (via the Comparison Procedure).

Threshold Test Element Simulation

The Threshold Test Procedure specified by the applicant is duplicated in the simulation.

COMPARISON PROCEDURE

FIGURE IV-20 - REFERENCE ELEMENT SIMULATION

3.2 Assessment of Item Loss Detection Subsystems

The analysis used to determine the performance of an item loss detection subsystem depends on the implementation of the detection subsystem as described in Part II of the MC&A Plan. If the applicant has chosen to implement an item inspection plan, the analysis will be based on an equation which relates detection probability to the number of items sampled, the number of items covered by the subsystem, and the number of items which must be compromised to yield a 5 FKG loss. If the applicant has chosen to use real time item inventory, the analysis will be based on the use of a detection probability analysis code such as the Structured Assessment Analysis.* The analyses for both types of subsystems will be based on the detailed data provided by the applicant in his I&C Response Sheets.

Various equations will be provided for determining the effectiveness of an item inspection plan. For example, an equation which might be used to determine the probability of detecting the loss of at least one item is:**

$$P_D = \frac{\binom{N-D}{n}}{\binom{N}{n}}$$

N = population size

D = number of missing or compromised items

n = number of items to be inspected or sampled

$$\binom{a}{b} = a! / b! (a-b)!$$

*Level 2 of the SAA determines the probability of detection for MC&A subsystems not based on accounting type measurements.

**A.L. Harkness, G.H. Winslow, "A Weighted Hypergeometric Sampling Plan," Nuclear Materials Management, Spring 1980.

This equation assumes that the detection of a single missing item or compromised tamper seal is cause for an alarm. The outputs of an item loss detection subsystem, as derived from the preceding equation, are presented in Section 2.2 above.

3.3 Assessment of Response Subsystems

The license applicant will provide response subsystems to resolve alarms which arise from detection subsystems. These response subsystems will attempt to classify the cause of an alarm as:

- 1) Operator Error,
- 2) Measurement Error, or
- 3) Actual Loss.

The resolution will be performed in two separate steps. The first of these is intended to detect an operator error and involves checking back through the procedures within the detection subsystem to locate transcription errors, recording errors, etc. This process will be composed of a series of procedures which are described on the appropriate I&C Sheets. The assessment of the performance of this set of resolution procedures is discussed in Section V-3.0 below. The second step is designed to determine whether an alarm is due to measurement "noise" or a material loss. This step will utilize additional measurements. Since the response subsystem may also incorporate some or all of the measurements used in the detection subsystem which generated the alarm, the two subsystems must be assessed simultaneously.

The assessment of a response subsystem which is used to verify an alarm is similar to the assessment of a detection subsystem, and hence depends upon the same principles described in Section 3.1 above. A schematic of the modifications needed for response subsystem assessment is shown in Figure IV-21.

The use of common measurements between a detection and response subsystem will introduce correlations between the two subsystems. To capture these correlations, the assessments of the two subsystems must use the same simulation data for components which they share in

FIGURE IV-21 - RESPONSE SUBSYSTEM SIMULATION

common. The result of the response subsystem assessment is the probability of an unresolved alarm in the absence of a loss.

Response subsystem assessment will be demonstrated using a portion of an example provided by NRC.*

Example of Response Subsystem Assessment

The licensee has implemented a detection subsystem using the prediction of the output of a control unit (CU) based on a process yield factor and the CU input. Figure IV-22 shows the CU and defines the variables.

The loss indicator for the detection subsystem is:

$$I_{23} = K \cdot \tilde{X}_2 - \tilde{X}_3$$

where $\tilde{X}_2$ and $\tilde{X}_3$ are measured values.

If yield, K, were known exactly and there were no measurement errors, the loss indicator, I_{23} , would be zero in the absence of a loss.

However, the yield is not known exactly and the input and output measurements are noisy, resulting in the calculated inventory differences. In order to decide whether the computed loss indicator has arisen from a loss or from process and measurement uncertainty, it is compared against an action threshold. The calculation of this threshold, which would be described on an I&C Response Sheet for a Threshold Determination Procedure, involves the calculation of the variance of the loss indicator:

*Private Communication, Barry Mendelsohn, U.S. NRC, February 27, 1981.

FIGURE IV-22 - EXAMPLE CONTROL UNIT

$$\text{Var}(I_{23}) = K^2 \cdot \text{Var}(X_2) + X_2^2 \cdot \text{Var}(K) + \text{Var}(X_3)$$

This variance is then used to determine an action threshold based on a specified quantity for detection. A value of the loss indicator which exceeds this threshold is called an alarm. A alarm may be due to an actual loss or to "noise."

In order to resolve alarms from this detection subsystem, the licensee implements a response subsystem which involves a Cleanout Procedure to recover the fraction of input trapped as holdup. The loss indicator for this subsystem is based on the following equation:

$$I'_{23} = \tilde{X}_2 - \tilde{X}_3 - \tilde{H}$$

where

$\tilde{X}_2, \tilde{X}_3$ are the set of measured values determined for the detection subsystem,

and

$\tilde{H}$ is a measured value of holdup made for the response subsystem.

The licensee then tests this second loss indicator against the appropriate action threshold. If this loss indicator exceeds the threshold, the alarm from the detection subsystem is said to be a loss alarm.

The probability of a false verification of a false alarm is:

$$P(A_2, A_1 | \text{No loss}) = P(A_2 | A_1, \text{No loss}) \cdot P(A_1 | \text{No loss})$$

where:

A1 is the occurrence of an alarm from the detection subsystem.

A2 is the occurrence of an alarm from the response subsystem.

$P(A2, A1 | \text{No loss})$ is the probability of an alarm from both subsystems, given no loss.

$P(A2 | A1, \text{No loss})$ is the probability of an alarm from the response subsystem, given that the detection subsystem alarmed on no loss.

$P(A1 | \text{No loss})$ is the probability of the detection subsystem alarming on no loss.

Since the two subsystems use some common measurements,

$$P(A2 | A1, \text{No loss}) \neq P(A2 | \text{No loss}) P(A1 | \text{No loss})$$

The operation and performance of the above response subsystem has been simulated with the Monte Carlo code listed in Figure IV-23. An unpredicted holdup was input into the code and the probability of an alarm from the detection subsystem was calculated along with the probability of an alarm from the response subsystem. These results are shown in Figure IV-24. As can be seen from this figure, the alarm probability for a zero loss is approximately 0.01, which is consistent with the threshold set by the 0.01 false alarm criterion. As the holdup fraction rises, the detection subsystem alarm probability increases. The response subsystem is able to resolve most false alarms for high holdup fractions. At low rates of excess holdup, the response subsystem is unable to resolve the alarms. For example, at an excess holdup fraction of zero, the detection subsystem alarms with a probability of 0.0097, and the response subsystem falsely verifies 0.856 of these alarms as true losses. This poor resolution is due to the correlation in the data used by the two subsystems. The "incorrect" measurement causing the

FIGURE IV-23 - MONTE CARLO SIMULATION OF THE EXAMPLE DETECTION AND RESPONSE SUBSYSTEM

FIGURE IV-24 - RESPONSE SUBSYSTEM PERFORMANCE

alarm in the detection subsystem also causes an alarm in the response subsystem. The results shown here emphasize the need for simultaneous simulation of subsystems which use common measurement data.

This section describes the application of the assessment procedures described in Sections I, II, and III above to specific portions of a license applicant's MC&A Plan.

1.0 PRELIMINARY ASSESSMENT PROCEDURES*

The procedures which follow should precede the assessment of individual Rule provisions:

1. Check Part I for the inclusion of all sections requested by the SF&C Guide.
2. Check Part II for the inclusion of all sections requested by the SF&C Guide.
3. Check Index to Part III to ensure the listing of each I&C Response Sheet included in Part III.
4. Check contents of Part III to ensure the inclusion of an I&C Response Sheet for each component listed in the Index to Part III.
5. Check index to Part III for inclusion of each I&C Response Sheet referenced in Parts I, II, and III**.
6. For each I&C Response Sheet in Part III, perform the following:
 - a) Check for inclusion of all information requested by corresponding I&C Sheet.

* Editorial conventions used in Section V are described in Section I below.

** An I&C Response Sheet will generally include references to other I&C Response Sheets.

- b) Check for consistency with minimal criteria established for individual component types by NRC.
- c) Check for inclusion and adequacy of justification provided in Part IV for any equations stated in an I&C Response Sheet.

2.0 ASSESSMENT FOR S70.83: DETECTION CAPABILITY

1. S70.83(a)

- a) Check Part I-2 for inclusion of control unit descriptions.
- b) Check Part I-6 for inclusion of material description categories.
- c) Check Parts I-4, I-5, I-7, I-8, I-9, and I-10 to ensure that all process segments, storage areas, or movements of SSNM between segments and/or storage areas have been assigned to a control unit.
- d) Check table(s) in Part II-1.1.1 to ensure that a detection subsystem has been designated for each material description category within each control unit, as specified in Part I-6.
- e) Check Part II-1.1.2 to ensure the inclusion of a separate description for each subsystem designated in Part II-1.1.1.
- f) For each subsystem description in Part II-1.1.2, perform the following:
 - i) Check description for inclusion of all information requested by the SF&C Guide.
 - ii) Check items A.11) and A.13) of subsystem description for consistency with S70.83(a)(5).*
 - iii) If subsystem is used to detect the loss of tamper-sealed items, check the I&C Response Sheet for the related Item Creation Procedure(s), to verify that at least 3 persons will attest to the contents of each item.
 - iv) Check Part IV for inclusion and adequacy of the justification of each performance parameter included in item A.17) of subsystem description.
 - v) Perform statistical assessment of subsystem, following framework provided in Section IV above.

*These items are described on page 7 of Part II of the SF&C Guide.

2. 70.83(b)

- a) Check table(s) in Part II-1.2.1 to ensure the inclusion of a detection subsystem for each Internal Transfer Procedure identified in Part I-9.
- b) Check each subsystem description in table(s) of Part II-1.2.1 for inclusion of all information called for in the SF&C Guide.
- c) Check Part II-1.2.2 for affirmation statement called for in the SF&C Guide.
- d) Check I&C Response Sheets on Internal Transfer Procedures for compliance with S70.83(b).

3. S70.83(c)(1)

- a) Check table(s) in Part II-1.3.1 for completeness, to ensure that each control unit identified in Part I-2 has been assigned to category (i), (ii), or (iii) of S70.83(c)(1).
- b) Check Part II-1.3.2 to ensure that the sum of control quantities over all control units in category (i) does not exceed 5 FKG.
- c) Check Part II-1.3.3 to ensure that the sum of control quantities for each combination of control units within category (ii) does not exceed 5 FKG.
- d) Check Part II-1.3.3 to ensure the inclusion of the affirmation statement requested in the SF&C Guide. Check this statement for consistency with information on management hierarchy in Part I-11.
- e) Check Part II-1.3.4 to ensure that the sum of control quantities for each individual control unit in category (iii) does not exceed 5 FKG.
- f) Check Part II-1.3.4 to ensure inclusion of the affirmation statement requested in the SF&C Guide.
- g) Check Part II-1.3.4 to ensure references to appropriate portions of the MC&A Plan and/or the Physical Protection Plan which justify the claimed isolation of each control unit in category (iii). Check these portions for adequacy.

- h) Check each sum of control quantities provided in Parts II-1.3.2, II-1.3.3, and II-1.3.4 for consistency with individual control quantities listed in Part II-1.1.1.
- i) Check Part II-1.3.5 to ensure that the expected total number of false alarms listed therein does not exceed maximum established by the NRC. Check this total for consistency with false alarm rates of individual subsystems, as determined by the statistical assessment procedure.

4. S70.83(c)(2)

- a) Check table(s) in Part II-1.4.1 to ensure that each location identified in I-1 is covered by at least one subsystem for detecting direct indications of the unauthorized presence of SSNM.
- b) Check table(s) in Part II-1.4.2 to ensure that each piece of Process or Storage Equipment identified in Part I-1 is covered by at least one subsystem for detecting indirect indications of the presence of SSNM in unauthorized locations.
- c) Check table(s) in Parts II-1.4.1 and II-1.4.2 for inclusion of all information requested in the SF&C Guide.
- d) Check Part II-1.4.3 for reference to an Awareness Program.
- e) Check Part II-1.4.3 for a reference to a Blind Testing Procedure (SSNM is unauthorized locations) for each control unit identified in I-2.
- f) Check Part II-1.4.4 for inclusion and adequacy of description of health/physics monitoring program.

5. S70.83(d)

- a) Check table(s) in Part II-1.5.1 to ensure the inclusion of a detection subsystem to monitor the cumulative imbalance of each quantitative subsystem identified in Part II-1.1.1.

- b) Check table(s) in Part II-1.5.1 to ensure the inclusion of a detection subsystem involving the time series analysis of the imbalances of each quantitative subsystem identified in II-1.1.1.
- c) Check Part II-1.5.2 and Part II-1.5.3 to ensure the inclusion of a separate description for each subsystem identified in Part II-1.5.1.
- d) For each subsystem description in Parts II-1.5.2 or II-1.5.3, perform the following:
 - i) Check description for inclusion of all information requested by the SF&C Guide.
 - ii) Check item A.9) of subsystem description for consistency with S70.83(d)(2).
 - iii) Check Part IV for inclusion and adequacy of the justification of each performance parameter included in item A.15) of subsystem description.
 - iv) Perform statistical assessment of subsystem, following framework provided in Section IV above.

3.0 ASSESSMENT FOR S70.85: RESPONSE CAPABILITY

1. S70.85(a)

- a) Check Part I-2 for identification of control units for which it would be difficult to resolve an alarm if material processing is allowed to continue after the alarm situation is discovered.
- b) Check Part I-12 to ensure that not more than 12 persons are assigned to each stewardship team for SSNM.
- c) Check table in Part II-2.1 to ensure the inclusion of a response subsystem for each detection subsystem identified in the tables of Parts II-1.1.1, II-1.2.1, II-1.4.1, II-1.4.2, and II-1.5.1.
- d) Check Parts II-2.1.1 and II-2.1.2 to ensure the inclusion of a separate description of each subsystem identified in Part II-2.1.
- e) For each subsystem description in Part II-2.1.1, perform the following:
 - i) Check description for inclusion of all information requested by the SF&C Guide.
 - ii) Check the time parameters provided in items g) and h) of the subsystem descriptions against those specified in S70.85(a)(3).
 - iii) Check the list of potential causes of false alarms in item c) of the subsystem description for consistency with the description of the corresponding detection subsystem in Part II-1.1 or II-1.5.
 - iv) Check the list of resolvable false alarm causes in item g) of the subsystem description for consistency with the content of the I&C Response Sheets referenced in item g).
 - v) Check the list of resolvable false alarm causes in item g) of the subsystem description to ensure the coverage of each potential alarm cause listed in item c) of the subsystem description.
 - vi) Perform statistical assessment of subsystem following framework provided in Section IV above.

- f) Check each subsystem description in Part II-2.1.2.1 for inclusion of all information requested in the SF&C Guide.
- g) Check each subsystem description in Part II-2.1.2.2 for inclusion of all information requested in the SF&C Guide.

2. S70.85(b)

- a) Check Part II-2.2 to ensure the inclusion of a separate subsystem description for each of two strata of response times: 0-12 hours, and 12-48 hours.
- b) For each subsystem description in Part II-2.2, perform the following:
 - i) Check the subsystem description for inclusion of all information requested by the SF&C Guide.
 - ii) Check item e) of subsystem description for inclusion of a reference to a detection subsystem covering each batch of SSNM referred to in item d) of subsystem description.
 - iii) Check performance parameters listed in item f) of subsystem description for consistency with minimum standards established by NRC.
 - iv) Check Part IV for inclusion and adequacy of justification for performance parameters included in item f) of subsystem description.

3. S70.85(c), (d) and (e)

- a) Check I&C Response Sheets for Response to SSNM in Unauthorized Locations for compliance with S70.85(c)(1).
- b) Check following sections of MC&A Plan for appropriate affirmation statements requested by the SF&C Guide:

II-2.1.1(j)
II-2.1.1(k)
II-2.1.2.1(h)
II-2.1.2.2(g)
II-2.2(i)

- c) Check I&C Response Sheets for Alarm Notification Procedures and Alarm Investigation Reports for consistency with the affirmation statements referred to in b) above.
- d) Check affirmation statement in Part II-2.1.1(i) for compliance with S70.85(e).

4.0 ASSESSMENT FOR S70.86: ASSURANCE STRUCTURE

1. S70.86(a): Management Control

- a) Check management hierarchy of Part I-11 for consistency with S70.86(a).
- b) Check stewardship team descriptions of Part I-12 for consistency with S70.86(a)(2)(i).
- c) Check Part I-11 against Part I-12, to ensure independence of plantwide accounting responsibility from custodial responsibility.
- d) Check each Internal Transfer Procedure identified in Part I-9 which involves inter-team transfers, to ensure compliance with S70.86(a)(2)(i).
- e) Check each Authorization Schedule identified in Part I-13, to ensure compliance with S70.86(a)(2)(iii).

2. S70.86(b): Selection and Training Program

- a) Check Part II-3.1.1 for a reference to an Employee Selection Procedure for each personnel position identified in Part I-11.
- b) Check Part II-3.1.2 for a reference to a Training Procedure for each personnel position identified in Part I-11.
- c) Check Part II-3.1.3 for a reference to an Awareness Program.

3. S70.86(c): Independent Audit Program

- a) Check Part II-3.2 for inclusion of all information requested in the SF&C Guide.
- b) Check personnel assignments listed in I&C Response Sheets referenced in Part II-3.2.4, to ensure that these persons are independent of facility management.
- c) Check frequency information in Parts II-3.2.2 and II-3.2.7, to ensure that each audit will be performed at least once per year.

- d) Determine the percentages of procedures, authorization schedules and records which are audited by the procedures referenced in Parts II-3.2.4 and II-3.2.9. Check these percentages against minimum adequacy criteria established by the NRC.
- e) Check Part II-3.2.11 for inclusion of all features recommended in the SF&C Guide. (The statements in Part II-3.2.11 will be verified through the adequacy checks on specific I&C Response Sheets referenced in other portions of the MC&A Plan).

4. S70.86(d): Accountability Monitoring Program

Check each I&C Response Sheet for components of types listed in Part II-3.3.1 for consistency with minimal criteria established by NRC. (A complete listing of specific components of each of these types must be provided by the applicant in the index to Part III of the MC&A Plan).

5. S70.86(e): Licensee Self-Test Program

- a) Check Part II-3.4 for inclusion of all information requested by the SF&C Guide.
- b) Check Part II-3.4.1 for a reference to at least one Blind Testing Procedure for each detection or response subsystem identified in Part II-1 or II-2.
- c) Check Parts II-3.4.1, II-3.4.3, II-3.4.4, and II-3.4.6 for consistency with guidelines stated in corresponding sections of the SF&C Guide.

6. S70.86(f): Accounting and Data Analysis Program

- a) Check Part II-3.5.1 for a reference to an Accounting Report and Accounting Form for each specific procedure of the types listed in the corresponding section of the SF&C Guide (A list of specific procedures of these types must be provided by the license applicant in the index to Part III).

- b) Check Part II-3.5.2 for a reference to a Computerized or Non-Computerized Account and a Data Storage Medium for each control unit identified in Part I-2.
- c) Check Part II-3.5.2 for a reference to at least one Computerized or Non-Computerized Account and at least one Data Storage Medium for the facility level accounting system.
- d) Check Part II-3.5.3 for a reference to at least one Computerized or Non-Computerized Log and at least one Data Storage Medium for items a) through i) in the SF&C Guide.
- e) Check Part II-3.5.4 for a reference to at least one Reconciliation Procedure of type a), b), and d) as described in the SF&C Guide.
- f) Check Part II-3.5.4 for a reference to at least one reconciliation Procedure of type c) and type e) for each control unit identified in Part I-2.
- g) Check Part II-3.5.5 for inclusion of all information requested by the SF&C Guide.
- h) Check the expected standard deviation of ID provided in Part II-3.5.6 for compliance with S70.86(f)(5)(i).
- i) Check Part IV for inclusion and adequacy of justification for expected standard deviation of ID provided in Part II-3.5.6
- j) Perform statistical analysis of the inventory subsystem described in Part II-3.5.5, to verify the expected standard deviation claimed in Part II-3.5.6. This analysis should follow the framework described in Section IV below.
- k) Check Part II-3.5.8 for inclusion of three separate subsystem descriptions for the detection of excessive S/R differences for each of the Receiving Procedures identified under Part II-3.5.7 (i.e., a separate subsystem must be described for each of the three bases listed in Part II-3.5.8 of the SF&C Guide).
- l) Check each subsystem description in Part II-3.5.8 for inclusion of all information requested in the SF&C Guide.

- m) For each Shipping and Receiving Procedure identified in Part II-3.5.7, check Part II-3.5.8 for the inclusion of an expected standard deviation.
- n) Check the consistency of each parameter included in Part II-3.5.8 for compliance with S70.86(f)(5)(ii).
- o) Check Part IV for inclusion and adequacy of justification for each parameter provided in Part II-3.5.9.
- p) Perform statistical assessment to verify each parameter claimed in Part II-3.5.9.
- q) Check the expected standard deviation of the cumulative shipper/receiver difference provided in Part II-3.5.10 for compliance with S70.86(f)(1)(iii).
- r) Check Part IV for inclusion and adequacy of justification for the parameter provided in Part II-3.5.10.
- s) Perform statistical assessment to verify the parameter provided in Part II-3.5.10.
- t) Check Part II-3.5.10 for inclusion of affirmation statement requested by the SF&C Guide.
- u) Check I&C Response Sheets referenced in Part II-3.5.10 for consistency with S70.86(f)(6)(i).
- v) Check Part II-3.5.12 for inclusion of affirmation statements requested by the SF&C Guide.

7. S70.86(g): Accounting Investigation/Resolution Program

- a) Check Part II-3.6.1 for inclusion and completeness of the subsystem description requested by the SF&C Guide.
- b) Check the subsystem description in Part II-3.6.1 for adequacy, following a procedure analogous to that outlined in subsection 3.0-1.e) above.
- c) Check Parts II-3.6.2 and II-3.3.6 for the affirmation statements requested by the SF&C Guide.
- d) Check Part II-3.6.4 for the inclusion of each subsystem description requested by the SF&C Guide.

- e) Check each subsystem description in Part II-3.6.4 for adequacy, following a procedure analogous to that outlined in subsection 3.0-1.e) above.
- f) Check Parts II-3.6.5, 3.6.6, and 3.6.7 for inclusion of the affirmation statements requested by the SF&C Guide.

5.0 ASSESSMENT FOR S70.87: PROTECTION AGAINST THE DESIGN BASIS THREAT*

1. Perform "first order" vulnerability assessment of each detection subsystem identified in Part II-1.1.1,** to determine which persons or combinations of persons could prevent the detection of an abrupt loss of SSNM for up to 24 hours for Type A material, or three working days for Type B material.
2. Perform "second order" vulnerability assessment of each detection subsystem identified in Part II-1.1.1, to determine which persons or combinations of persons could prevent the detection of an abrupt loss of SSNM for up to eight weeks.
3. Compare the results of each first and second order vulnerability assessment with minimum standards established by NRC, to determine compliance with S70.87.

* A framework for the vulnerability assessments referred to in this section is provided in Section III above.

** The framework described in Section III above is also applicable to the assessment of subsystems identified in Part II-1.1.5 for the detection of a cumulative loss, should such an assessment be desired by the NRC.

6.0 ASSESSMENT FOR S70.94: RECORD KEEPING

1. Check Part II-3.2.11 for the appropriate affirmation statements requested by the SF&C Guide.
2. Check the I&C Response Sheets for each component of the following types for compliance with S70.94:
 - Accounting Forms
 - Alarm Investigation Reports
 - Independent Audit Reports
 - Blind Testing Procedures
 - Training Procedures

(A complete listing of each component of the above types must be provided by the applicant in the Index to Part III.)

APPENDIXES

APPENDIX I - RELATIONSHIP OF I&C RESPONSE SHEETS TO THE STATISTICAL SIMULATION

This appendix provides an overview of the relationship between the SF&C Guide and the data which will be used in the statistical assessment package described in Section IV above. The SF&C Guide is designed to collect data about the details of the MC&A detection subsystems through the use of Intent and Content (I&C) Sheets. The general six element detection format described earlier is used as the framework for the I&C Sheets.

There are two general types of detection subsystems: those designed for bulk loss detection and those for item loss detection. The bulk loss detection subsystem will be used to illustrate the relationship of data in the I&C Sheets. Each element of the subsystem is shown in Figure A-1 and will now be discussed.

1. Measurement Element

All data enters the measurement element via a Data Combination Procedure.* The purpose of this procedure is to combine the measurement results from one or more procedures to yield the data such as present material inventory which is used in the detection subsystem. The applicant will describe the exact data processing equations which are used in this procedure in the Data Combination Procedure I&C Response Sheet.

The measurement data is gathered through the use of Measurement Procedures. There are six types of these procedures, including:

*The names of all I&C Response Sheets have been capitalized following the convention of Part III of Standard Format and Content Guide: Component Intent and Content Sheets, R. S. Schechter, LLNL, I. J. Sacks, AIP, 11 February 1981.

FIGURE A-1 - RELATIONSHIP OF I&C RESPONSE SHEETS TO BULK DETECTION SUBSYSTEM STATISTICAL ASSESSMENT

- a) Quantity Measurement
- b) Composition Measurement
- c) Non-Destructive Analysis
- d) Holdup Measurement
- e) Effluent Scrap and Waste Measurement
- f) Stored Scrap and Waste Measurement

The first three of these procedures are "basic measurement procedures" and are used by the latter three procedures. On the I&C Response Sheet for each procedure used, the applicant will provide performance data. That is, the accuracy of each procedure will be specified. In addition, the details of the procedure itself, such as number of measurements made, data reduction equations, and data qualification steps will be described. Measurement Procedure I&C Response Sheets will also identify the Material Sampling Procedures which are used to collect the material which is measured.

Each Measurement Procedure described on an I&C Response Sheet will utilize one or more Measurement Instruments. These include:

- 1) Mass Measurement Instruments
- 2) Flow Measurement Instruments
- 3) Volume Measurement Instruments
- 4) Isotopic Analysis Instruments
- 5) Chemical Assay Instruments

The I&C Response Sheets for these instruments will contain descriptions of their performance. The performance data for these instruments will be described in terms of the physical properties measured. For example, an I&C Response Sheet for a Volume Measurement Instrument would describe the errors associated with the measurement of differential pressure. The I&C Response Sheets for these instruments will also identify any Calibration Procedures used. Any procedures for the determination of random errors will be

described on an I&C Response Sheet for a Random Error Determination Procedure. The description of Calibration and Random Error Determination Procedures will reference I&C Response Sheets for Reference Standards.

2. Reference Element

The data used in the reference element is the "book inventory" against which the measurement is compared. The source of this data is described in a set of I&C Response Sheets for Computerized or Non-Computerized Accounts or Records. These sheets in turn reference an I&C Response Sheet for a Data Combination Procedure which describes the processing of the reference data for comparison to the measurement data. This Data Combination Procedure I&C Response Sheet will reference a set of I&C Response Sheets for Measurement Procedures which created the reference data. These Measurement Procedure I&C Response Sheets will reference I&C Response Sheets which describe the Measurement Instruments. Each of the above I&C Response Sheets will contain information as to the source of the data and the time of its collection. This information will allow the determination of the correlation between the reference and measurement data. These correlations are necessary in order to perform the statistical assessment.

3. Comparison Element

The measurement data must be compared to the reference data. This comparison will be described on an I&C Response Sheet for a Comparison Procedure. The Comparison Procedure is a set of equations which are used to generate a loss indicator. In some cases, this procedure will be a simple differencing operation between the measurement and the reference data. In other cases, the loss estimator may be determined by sets of equations which smooth measurement data and fit it to a model of the process. The latter

type of procedure would also require an I&C Response Sheet for an Estimation Filter.

4. Threshold Determination Element

The loss indicator computed by the Comparison Procedure must be compared to an action threshold in order to detect a significant loss. This threshold calculation is described on an I&C Response Sheet for a Threshold Determination Procedure. Within this procedure, an error analysis is performed which formally considers:

- a) The goal quantity* for detection.
- b) The required detection probability for this goal quantity.
- c) The required false alarm probability.
- d) All correlations within and between the measurement data and the reference data.

The Threshold Determination Procedure I&C Response Sheet contains the equations which describe the error propagation analysis. In order to treat correlations between the measurement and reference data, the Threshold Determination Procedure will reference an I&C Response Sheet for a Measurement Error Analysis and for a Material Sampling Error Analysis. These I&C Response Sheets will in turn reference their respective Measurement and Sampling Procedure I&C Response Sheets.

5. Threshold Test Element

The loss indicator determined by the comparison element is tested against the action threshold computed by the threshold determination element. This test is described on the I&C Response Sheet for the Threshold Test Procedure. The procedure is generally a statistical

*Goal quantity is either 5 FK6 or a control quantity.

hypothesis test. The exact data processing equations used for this test will be described on the I&C Response Sheet.

6. Response Initiation Element

This element does not enter into the Statistical Assessment.

APPENDIX II - EXAMPLE SUBSYSTEM DESCRIPTION

This appendix contains a partial description of the detection subsystem which is used as the example in the body of this report relevant to the statistical assessment.

1.1.2* - Description of Detection Subsystem

A. General Information

- 1) Detection Subsystem
Bulk Loss Detection Subsystem #8
- 2) Control Unit
Control Unit #3
- 3) Material Description Category
Material Description Category #3
- 4) Material Batch
Material Batch #6
- 5) Anomaly Monitored
Quantitative loss of SSNM in bulk forms, with or without substitution.
- 6) Personnel with Custodianship

*Numbers correspond to Part II of Standard Format and Content Guide: Subsystems and Programs for MC&A Rule Requirements, R. S. Schechter, LLNL, I. J. Sacks, AIP, 11 February 1981.

*****This data is not relevant to the statistical assessment, and has not been included in this example.

7) Authorization Schedule

8) Alarm/Non-Alarm Report

9) Execution Frequency

Every 8 hours.

10) Special Execution Circumstances

(i) Response to Communicated Threat

(ii) Resolution of loss from other CW's

11) Maximum Detection Time for 5 FKG

No more than 17 hours could elapse between abrupt 5 FKG loss and alarm. Eight hours between measurements plus 8 hours for analytical laboratory assay, 1 hour for data processing.

12) Control Quantity

The control quantity for this detection subsystem is 2 FKG.

13) Maximum Detection Time for Control Quantity

No more than 17 hours could elapse between abrupt control quantity loss and alarm. Eight hours between measurements plus 8 hours for analytical laboratory assay, 1 hour for data processing.

*****This data is not relevant to the statistical assessment and has not been included in this example.

14) Special Conditions

The only situations which could cause a loss of 5 FKG to go undetected for more time than indicated in 11 above is a major process upset condition.

15) Detection Interval

A loss will be localized to within 8 hours.

16) Time to File Alarm/Non-Alarm Report

The Alarm/Non-Alarm Report will be filed within 9 hours of end of detection intervals.

17) Performance Parameters

a) 5 FKG Loss

$$P_d = 0.99$$

b) Control Quantity

$$P_d = 0.90 \text{ @ } 2 \text{ FKG}$$

c) False Alarm for 5 FKG

$$P_{fa} = .001 \text{ Per Detection Interval}$$

d) False Alarm for Control Quantity

$$P_{fa} = .001 \text{ Per Detection Interval}$$

e) False Alarms/Year

$$FAR = 1.095$$

B. Subsystem Configuration

1) Measurement Element

The following components* are used in the measurement element of Bulk Loss Detection Subsystem #8:

- a) Volume Measurement Instrument #11
- b) Quantity Measurement Procedure #1
- c) Isotopic Assay Instrument #1
- d) Composition Measurement Procedure #1
- e) Chemical Analysis Instrument #1
- f) Composition Measurement Procedure #2
- g) Material Sampling Procedure #12
- h) Data Combination Procedure #3

2) Reference Element

The following components are used in the reference element of Bulk Loss Detection Subsystem #8:

- a) Data Combination Procedure #14
- b) Non-Computerized Account #8
- c) Holdup Estimation Procedure #6
- d) Volume Measurement Instrument #11
- e) Quantity Measurement Procedure #2
- i) Isotopic Assay Instrument #1
- g) Composition Measurement Procedure #10
- h) Chemical Analysis Instrument #1
- i) Composition Measurement Procedure #11
- j) Material Sampling Procedure #13

3) Comparison Element

The following components are used in the comparison element of Bulk Loss Detection Subsystem for Control Unit 3.

*Example I&C Response Sheets for some of these components are presented in Appendix III.

a) Comparison Procedure #13

b) Estimation Filter #1

(This element incorporates a weighted least squares fit of measurement data to a model of the solution dynamics. The model includes terms for evaporation and radiolysis.)

4) Threshold Determination Element

The following components are used in the threshold determination element.

a) Threshold Determination Procedure #6

b) Measurement Error Analysis #3

c) Material Sampling Error Analysis #2

5) Threshold Test Element

The following component is used in the threshold test element.

Threshold Test Procedure #4

6) Response Initiation Element

*****This data is not relevant to the statistical assessment and has not been included in this example.

APPENDIX III - EXAMPLE I&C RESPONSE SHEETS FOR DETECTION SUBSYSTEM
COMPONENTS

This appendix contains partially completed I&C Response Sheets for some of the components of the detection subsystem which is used as the example in the Section IV of this report. The following I&C Response Sheets have been provided in this appendix:

	<u>Abbreviation*</u>
1) Volume Measurement Instrument Number #11 -----	VM111
2) Quantity Measurement Procedure #1 -----	QMP1

The information which has been provided follows the format specified in Part III of Standard Format and Content Guide: Component Intent and Content Sheets, R. S. Schechter, LLNL and I. J. Sacks, AIP, 11 February 1961.

*We have chosen to abbreviate the instrument names for conciseness.

I&C Response Sheet
For
Volume Measurement Instrument #11 --- VMI1

1. Type, Manufacturer, Model Number

Differential Pressure Pneumatic Density/Height
Sensing System, XYZ Comparator, Model 002

2. Quantity Measurement Procedure

Quantity Measurement Procedure #1

3. Material Batches Measured

Material Batch #5

4. Physical Properties Measured

ΔP_a = Differential Pressure between ambient and bubbler tube 1,
 ΔP_b = Differential Pressure between bubbler tube 1 and bubbler tube 2.
Height Difference between tube 1 and 2 = 10 inches

5. Location

6. Utility Components

7. Measurement Communication

8. Signal Transmission Components

*****This information is not relevant to the statistical assessment and has not been included in this example.

9. Equations to convert measured parameters to material properties

$$\Delta P_a = g \rho (10'')$$
$$\Delta P_b = g \rho h$$

where

ΔP_a = Differential Pressure between ambient and bubbler tube 1

ΔP_b = Differential Pressure between bubbler tube 1 and bubbler tube 2

g = Acceleration due to gravity

ρ = Density of Solution

h = Height of Solution above tank

$$\rho = \frac{\Delta P_a}{g(10'')}$$

$$h = \frac{\Delta P_b}{g\rho} = \frac{\Delta P_b 10''}{\Delta P_a}$$

V = Volume of Solution

$$V = a + bh$$

where

a = Tank Heel (See #14 below)

b = Tank cross section (See #14 below)

m = Mass of solution

$$m = \rho V$$

10. Performing Personnel

11. Control Personnel

*****This information is not relevant to the statistical assessment and has not been included in this example.

12. Tamper Detection

13. Expected Accuracy

a) Bias Error

The bias error of the differential pressure sensors will be Gaussian with a mean of 0 and a standard deviation equal to 0.1% of the full scale reading.

b) Random Error

The random errors associated with the differential pressure sensors are Gaussian with a mean of 0 and a standard deviation of 5%.

c) Roundoff Error

Differential pressure is quantized to 12 bits full scale.

14. Calibration and Bias Determination Procedures

Calibration Procedure #2 ----- CPS2

Bias Error Determination Procedure #3 ----- BEDS3

15. Error Determination Procedure

Determined by multiple measurements; see Quantity Measurement Procedure #1.

16. Maintenance Policy

17. Reliability

*****This information is not relevant to the statistical assessment and has not been included in this example.

I&C Response Sheet
for
Quantity Measurement Procedure #1 --- QMP1

1. Description
 - a) Volume Measurement
 - b) Determination of volume and density of solution in the storage tank in CU3.
2. Detection Subsystem
Bulk Loss Detection Subsystem #8
3. Batch Measured
Material Batch #5
4. Communication of Measurement

5. Accounting Report
Accounting Report #10
6. Initial Information Output

7. Hard Copy of Accounting Report

8. Data Combination Procedure
 - a) The volume and density measurements are combined into solution mass using the procedure described on I&C Response Sheet for Data Combination Procedure #1.

*****This information is not relevant to the statistical assessment and has not been included in this example.

- b) Mass and composition are combined into SSNM mass via Data Combination Procedure #1.

9. Stages of Measurement Procedure

Volume and density of the solution in the storage tank is measured by querying the differential pressure transducers of Volume Measurement Instrument #11.

10. Equipment Used

Volume Measurement Instrument #11---VM11

11. Number of Replicate Measurements

There are 10 measurements made of the differential pressures which are used to compute volume and density. These are designated ΔP_{ai} and ΔP_{bi} where i ranges from 1 to 10.

12. Procedure Personnel

13. Tamper Detection

14. Verification Procedures

The differential pressure is checked for normality using the W Test specified in ANSI Standard N15.15-1974*.

15. Outlier Tests

The differential pressure is checked for normality using the W Test specified in ANSI Standard N15.15-1974*.

*In an actual I&C Response Sheet, this test would be described in detail.
*****This information is not relevant to the statistical assessment and has not been included in this example.

APPENDIX IV - RESPONSE TO NRC CONCERNS OF 5 FEBRUARY 1981

In a letter to LLNL dated February 5, 1981, Barry Mendelsohn of the NRC recommended that the MC&A assessment methodology reflect the four concerns discussed below:

1. Limit the required content of the MC&A Plan to information essential to assessment of safeguards adequacy in license reviews and inspections.

The Standard Format and Content Guide proposed by LLNL in Task 4 was specifically designed for the above purposes. Section I of the present paper reviews the intent of each part of the SF&C Guide, and Section V reviews the relevance of each portion of the MC&A Plan to the assessment of compliance to specific Rule provisions.

2. Minimize the burden on the license applicant of writing the MC&A Plan.

To achieve this goal, the SF&C Guide proposed by LLNL is structured to elicit successively finer levels of detail concerning an MC&A system, as described in Section I above. This structure will enable the license applicant to prepare his MC&A Plan in a systematic fashion, with each portion after Part I keyed to a previous portion of the Plan.

The burden of completing the Plan is further minimized by the fact that the SF&C Guide provides explicit formats for the information requested by Parts I, II, and III, with each section of the Plan corresponding to a specific section of the Guide. The names of I&C Sheets which provide the formats for individual component descriptions are capitalized throughout the SF&C Guide, to facilitate their recognition. In addition, the requirement that unique designations be provided for each location, component, subsystem and

personnel category will facilitate the traceability of these safeguards entities throughout the MC&A Plan.

The preceding arguments are by no means intended to imply that the preparation of an MC&A Plan will be an easy task. Indeed, the systematic assessment of statistical performance and vulnerability requires the rigorous specification of numerous details, as discussed in Sections III and IV above. Failure to require the documentation of such details leaves critical aspects of an MC&A system undefined, as we have found to be the case with current MC&A Plans.

In general, a vulnerability assessment will not be robust to the omission of the fine level of detail requested by the I&C Sheets. This principle was illustrated in the example of Section III-3.1 above, which indicated how failure to consider key control over storage compartments for reference standards might lead to the omission of a subsystem vulnerability to a single insider. An assessment which failed to incorporate such details could produce highly deceptive outputs, and seriously degrade the integrity of a license review.

The preparation of an MC&A Plan suitable for a meaningful assessment will undoubtedly be a burdensome task. However, the burden will be compensated for by the valuable insights which this task will provide for the license applicant.

3. Minimize the extent to which a change in licensee operations would necessitate modification of the MC&A Plan.

To achieve this goal, the SF&I Guide calls for the creation of the MC&A Plan in modular fashion. That is, each subsystem description and each component description constitutes a distinct segment of the Plan, which references each related segment of the Plan. Thus, the deletion of a single subsystem or component would require only the

deletion of that particular segment, and the modification of the segments referenced therein.

Note that in some instances, the modification of a component would not require any modification of the MC&A Plan. As discussed in the introduction to Part III of the SF&C Guide, no modifications to the Plan would be needed if:

- a) Each performance specification associated with the new component is at least as good as that of the previous component; and
 - b) The relationship of the component to the MC&A system will remain unchanged, in terms of the personnel having control authority, tamper protection, etc.
4. Minimize the extent of the license review activity that requires computer assistance.

Of the six types of assessment procedures described in Section II above, the following would not require computer assistance: completeness checks, compliance checks, component adequacy checks, and Part IV adequacy checks. On the other hand, a computerized methodology is strongly recommended for the vulnerability assessment and the statistical assessment, which involve the analysis of complex networks. While the methods described for these assessments in Sections III and IV above could theoretically be performed without a computer, this approach would, in most instances, be too tedious to warrant serious consideration. In addition, the number of steps involved in a non-computerized approach would result in a high probability of error, and the results would be difficult to verify.