LA-UR -82-2753

Conf-821119--6

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36

LA-UR--82-2753

DE83 000635

MASTER

TITLE: AUTHENTICATION OF NUCLEAR-MATERIAL ASSAYS MADE WITH IN-PLANT INSTRUMENTS

AUTHOR(S): C. R. Hatcher, S. -T. Hsue, and P. A. Russo

SUBMITTED TO: International Symposium on Recent Advances in Nuclear Material Safeguards
Vienna, Austria
November 8-12, 1982

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

FORM NO 836 R4
ST NO 2629 5/81

AUTHENTICATION OF NUCLEAR MATERIAL ASSAYS MADE WITH IN-PLANT INSTRUMENTS*

ABSTRACT

This paper develops a general approach for International Atomic Energy Agency (IAEA) authentication of nuclear material assays made with in-plant instruments under facility operator control. The IAEA is evaluating the use of in-plant instruments as a part of international safeguards at large bulk-handling facilities, such as reprocessing plants, fuel fabrication plants, and enrichment plants. One of the major technical problems associated with IAEA use of data from in-plant instruments is the need to show that there has been no tampering with the measurements. Two fundamentally different methods are discussed that can be used by IAEA inspectors to independently verify (or authenticate) measurements made with in-plant instruments. Method 1, called external authentication, uses a protected IAEA measurement technique to compare in-plant instrument results with IAEA results. Method 2, called internal authentication, uses protected IAEA standards, known physical constants, and special test procedures to determine the performance characteristics of the in-plant instrument. The importance of measurement control

---

*Work performed under the US Program of Technical Support to IAEA Safeguards.

programs to detect normally expected instrument failures and procedural errors is also addressed. The paper concludes with a brief discussion of factors that should be considered by the designers of new in-plant instruments in order to facilitate IAEA authentication procedures.

I. INTRODUCTION

A. Background

In verifying declared nuclear material inventories at facilities under international safeguards, the International Atomic Energy Agency (IAEA) has made significant use of two types of material assays: destructive analysis of samples shipped to the IAEA Safeguards Analytical Laboratory (SAL) near Vienna and nondestructive assay (NDA) at the operating facilities using portable NDA equipment. These two approaches to nuclear material assay (combined with other inspection procedures) have proven adequate for the item-dominant facilities and low-throughput bulk facilities currently under international safeguards. However, for high-throughput bulk facilities (such as large reprocessing plants, fuel fabrication plants, and enrichment plants), additional assay approaches are needed to provide more measurements, quicker results, and in some cases greater accuracy than is practical using either of the previous IAEA approaches. For this reason, the IAEA recently began to study the use of data from in-plant NDA instruments that are operated and maintained by the facility operator.[1,2] This new approach appears to offer several advantages to the IAEA, but it poses

one significant technical problem that is best summarized by the following question. How can an inspector be certain that the assay values and probable measurement errors determined with an in-plant instrument are correct?

B. Structuring the Problem

The overall problem of authenticating nuclear material assays can be divided into three parts:

(1) verification of the sample,

(2) verification of the assay, and

(3) protection of the assay data.

In verifying the sample, the inspector must determine that the sample measured is representative of the material at the key measurement point, that there has been no tampering with the material, and that the sample selected is the one measured.

Verification of the assay involves ascertaining that the assay value and probable measurement error recorded for each sample are correct. Data reduction to convert raw data to assay results is considered part of the measurement because, in many cases, data reduction is performed by the assay instrument.

For small amounts of data, the simplest way of protecting the assay data is for the inspector to keep a copy of the verified assay data in his possession. Encoding of data and transmission of data to a secure memory have been recommended for protecting large amounts of data generated by on-line instruments.

All three of the above steps are important considerations, regardless of whether the IAEA uses an in-plant assay instrument

or an assay method completely under IAEA control. At the time of this study (1981), other investigators[3-5] had dealt with Steps 1 and 3, sample verification and protection of the assay data, but there was essentially nothing in the literature on Step 2, verification of the assay. However, as is often the case in the field of safeguards, a lack of literature does not necessarily mean a lack of previous thought on the subject; and clever ideas for detecting sophisticated tampering (such as the blind samples and add-a-gram techniques discussed below) had been around for a number of years. The purpose of this study was to develop a general approach for authentication of measurements made with in-plant instruments that would tie the previous work into an overall framework and shed new light on what we now call Step 2, verification of the assay.

C. Role of Measurement Control

In authenticating assay results, it is most important to recognize that anomalous assays are more likely to be due to instrument failure or operator error than to instrument tampering.[6] Thus, an important step in planning IAEA use of data from an in-plant instrument is to review the facility operator's measurement control program (for the instrument) to see if it is also suitable for IAEA use. The measurement control program should be designed so that it is capable of establishing with high probability that assay results are free of anomalies resulting from instrument failures and operator (procedural) errors. But as a general rule, measurement control programs cannot be expected to detect sophisticated types of tampering.

Practical measurement control programs always involve a compromise between operator convenience and the ability to detect all possible failures. For example, measurement control programs should make frequent tests for simple failure modes and less frequent tests for more complex (and hence less probable) failure modes.[6] A major advantage of using in-plant instruments is that very effective measurement control programs can be implemented by designing measurement control procedures into the instrument software and by having an instrument operator who is thoroughly familiar with the equipment and measurement procedures.

D. Classification of Tampering Scenarios

Once the measurement control program has established that the assay data are largely free of anomalies caused by instrument and procedural failures, one can concentrate on the subject of tampering. Tampering with an instrument can take any of the following forms:

(1) disabling the instrument, perhaps at a crucial time,

(2) introducing a fixed change in calibration by tampering with geometry, counting efficiency, etc.,

(3) increasing the probable measurement error by introducing noise or instabilities, and

(4) varying instrument performance in real time; for example, by using a "button under the table" that causes the instrument to read correctly when standards are measured and to read incorrectly when process samples are measured.

The fourth type of tampering listed above is frequently referred to as "sophisticated tampering," suggesting a basic difference between it and the first three (simpler) tampering scenarios.

II. TWO METHODS FOR MEASUREMENT AUTHENTICATION

A. External Authentication*

Two fundamentally different methods have been identified for authenticating nuclear material assays made with in-plant instruments, as illustrated in Figs. 1 and 2. External authentication (Fig. 1) is accomplished by comparing in-plant instrument assays with independent assays made using a method completely under IAEA control. Boxes at the top of Fig. 1 show the three basic steps that are followed by an inspector when planning to use assay data from an in-plant instrument: (1) verification of the samples, (2) measurement of N samples with the in-plant instrument, and (3) protection of the assay data. As discussed in Sec. I.C, the inspector can use the operator's measurement control program (perhaps with modifications) to ensure that the assay data are largely free of anomalies caused by instrument failures and procedural errors (box 2' in Fig. 1).

External authentication of the assay is made by following the steps shown in boxes 4 through 7 in Fig. 1. After the IAEA

---

*The terms "external authentication" and "internal authentication" (for what had previously been called Methods 1 and 2) were suggested by members of the IAEA Advisory Group on "Authentication Techniques for In-Plant NDA Equipment Applied to IAEA Safeguards" held in Vienna, November 10-13, 1981.

inspector has received a copy of the assay data (or after the data has entered protected storage), n samples are randomly selected from the complete set of N samples for remeasurement. Samples must be protected by the IAEA during the random selection process and during any subsequent sample preparation, shipment, or storage. Next, the n samples are reassayed, using a well-characterized measurement technique under IAEA control, such as a portable NDA instrument or destructive analysis at SAL. A comparison of assays made on the n samples by the two techniques allows the IAEA to establish the calibration and probable measurement errors associated with the in-plant instrument during the measurement of the N samples, including any effects that possible tampering with the instrument may have had on calibration or measurement errors.

External authentication is the standard approach used in scientific research by an investigator who wishes to confirm a previous investigator's results; and for this reason, it is well understood and widely accepted. The approach is also similar in many respects to the practice of customs officials, who first request that travelers declare goods in their possession and then perform an independent verification on a random subset of travelers. It will be impractical to implement external authentication if samples cannot be shipped for IAEA analysis and there is no suitable NDA instrument for reassaying the samples. In this case, one must rely on internal authentication.

B. Internal Authentication

Figure 2 shows that internal authentication is similar to external authentication in that the same three basic steps (boxes 1-3) are followed by the inspector and the same kind of measurement control program is used to keep the assay results largely free of anomalies caused by instrument failures and procedural errors. However, in internal authentication, no samples are reassayed using a measurement technique under IAEA control. Instead, protected IAEA standards, known physical constants, and special test procedures and equipment are used to determine the performance characteristics of the in-plant instrument, as indicated in Fig. 2.

To be comparable in performance to external authentication, internal authentication must

(a) establish calibration of the in-plant instrument relative to known physical constants or to standards under IAEA control,

(b) verify that the probable measurement errors quoted for the in-plant instrument are valid, and

(c) show that there has been no tampering with instrument performance in real time.

Steps (a) and (b) cannot be performed independently of Step (c) because it is impossible (using internal authentication techniques) to establish calibration and verify probable measurement errors if there is cleverly designed real-time instrument tampering. Thus, the key to internal authentication is Step (c).

A number of approaches (other than external authentication) have been evaluated for detecting tampering with instrument performance in real time, including use of:

- protected standards,
- blind samples,
- blind standards,
- add-a-gram,
- parallel instruments,
- internal consistency of data,
- containment and surveillance,
- visual inspection, and
- substitution of key components.

Each of these techniques is discussed below.

Protected standards can be used to detect simple forms of tampering, but cannot detect real-time tampering in which the instrument is made to give correct assays for standards and incorrect assays for process samples.

Blind samples involves concealing the identity of process samples during sample measurement and/or remeasurement. This method is useful for determining measurement precision, but cannot detect falsified assays that are internally consistent.

Blind standards involves concealing the identity of all items measured, so that it is not known whether a standard or a process sample is being measured until after the assay is completed. This approach is appealing in concept, but difficult to implement in most practical situations. The chief problem

is in ensuring that some covert method is not being used to determine when a standard is being measured.

Add-a-gram refers to the technique of first assaying an unknown sample, then assaying the sum of the unknown sample and a standard. If tampering causes the assays to be in error by a constant fraction (for example, 10%) this method may detect an inconsistency between the two assays. However, if tampering causes the assays to be in error by a fixed bias (for example, 10 g), there will be no inconsistency between the two assays.

Parallel instruments means that two or more unprotected instruments gather data that can be tested for consistency. One assumes that it is unlikely that all of the instruments will be tampered with and, hence, that tampering will produce detectable inconsistencies. Although this method provides some level of assurance, its usefulness is difficult to quantify.

Internal consistency of data makes use of the fact that some instruments generate several readings that have a logical relationship to each other. Certain forms of tampering would destroy this logical relationship. This method is similar to that of parallel instruments discussed above, except that the data come from a single instrument.

Containment and surveillance in this application is most likely to take the form of seals on part or all of the in-plant instrument, although surveillance could prove useful for protecting large arrays of instruments. This approach is effective, but in some instances it may limit operator access to the instrument for maintenance.

Visual inspection of the instrument by the IAEA inspector is a very effective way to detect tampering, particularly for simpler instruments. Software inspection can be achieved through techniques such as a software bit comparitor.

Substitution of key components of the in-plant instrument with equivalent components that are under the custody of the IAEA will prove simpler and more effective, in some cases, than inspection or containment and surveillance measures. For example, it is generally simpler to replace software than to inspect it or to protect it with seals.

Several of the techniques discussed above can be used for showing that there is no tampering with in-plant instrument performance in real time. The techniques that are most generally applicable to a variety of instruments and tampering scenarios are seals, visual inspection, and substitution of key components. These three methods are somewhat complimentary and can be used in combination. For example, if a part of an instrument is relatively simple and has visual access, it is a candidate for inspection. If a component has poor access and rarely needs maintenance, it may be possible to protect it with seals. If a component is highly complex and requires access, it may be best to substitute an IAEA component for it.

After establishing that there is no real-time tampering with the in-plant instrument, the inspector can proceed to (a) establish calibration of the instrument relative to known physical constants or to standards under IAEA control and (b) verify

the probable measurement errors quoted for the instrument by using ordinary laboratory procedures.

A few types of instruments can be calibrated on the basis of known physical constants, using the so-called intrinsic calibration approach. Gamma-ray instruments that measure ratios of gamma-ray intensities typically fall into this category. They have the advantage that standards are not needed to independently establish their calibration, although proof of their performance is normally based initially on comparisons with chemistry.

The calibration problem is considerably more complicated for other types of in-plant instruments. One approach is to develop a set of nuclear material standards that the IAEA verifies and then keeps under seal at the facility. Another approach (similar to external authentication except that random sampling is not required) is to ship samples measured with the in-plant instrument to SAL (and perhaps other laboratories) for analysis.

III. SUMMARY AND CONCLUSIONS

Considerable progress has been made in developing a framework and general understanding of the subject of authentication, and emphasis has now shifted toward practical implementation for specific in-plant instruments.[2] Separating authentication approaches into the two categories, external and internal, has proved to be a significant aid in evaluating which technique, or combination of techniques, should be used for specific in-

plant instruments.[1] The main advantage of external authentication is that detailed knowledge of the in-plant instrument is not required of the inspector. The main advantage of internal authentication is that shipment of samples and use of portable NDA equipment are not necessary. In practice, a combination of external authentication and internal authentication techniques may often provide the most effective approach. For example, an inspector may choose to supplement external authentication procedures with visual inspection of the instrument.

Designers of new in-plant instruments can assist the IAEA by considering authentication as part of the design process. For example, is the assay most amenable to authentication by an external or internal technique, or by some combination of the two? If internal authentication is to be used, can instrument design facilitate visual inspection, use of seals, or substitution of key components? Does instrument design allow for independent IAEA calibration and error analysis using an intrinsic method, standards, or post-assay destructive analysis? If external authentication is to be used, how are all assayed samples to be protected until a random selection is made for further IAEA study? Can protected samples be shipped to SAL or remeasured using a portable NDA instrument? For both external authentication and internal authentication, the in-plant instrument designer should also be concerned with how the IAEA can verify the samples, protect the assay data, and utilize the instrument's measurement control program.

Advances in technology should lead to in-plant instruments that are more easily authenticated and also to portable instruments that can expedite the authentication process. Meanwhile, recent activities at the IAEA suggest that authentication using currently available technology is practical for several existing in-plant instruments and can be expected to have a growing role in IAEA safeguards at large bulk-processing facilities.[2]

REFERENCES

[1] Advisory Group Paper on Authentication Techniques for In-Plant NDA Equipment Applied to IAEA Safeguards, IAEA Rep. AG-336 (1981).

[2] AUGUSTSON, R. H., et al., IAEA Experience With Authentication of In-Plant NDA Instrumentation, paper presented at International Symposium on Recent Advances in Nuclear Materials Safeguards, Vienna, Austria, IAEA-SM-260/1 (1982).

[3] HAKKILA, E. A., et al., Materials Management in an Internationally Safeguarded Fuels Reprocessing Plant, Los Alamos National Laboratory Rep. LA-8042, Vol. II (1980).

[4] KATZ, H., Independent Verification of Reprocessing Facilities with Installed Instrumentation as Tested in The TASTEX Program, ISPO-107 (1980).

[5] LEDERER, R. A., A Tamper Protected In-Line Liquid UF_6 Enrichment Monitor, Sandia National Laboratories Draft Rep. (1981).

[6] HATCHER, C. R., A Socratic Approach to Independent Verification, J. Nucl. Mater. Management. IX 3 (1980) 61.

FIGURE CAPTIONS

Fig. 1. Procedure for IAEA authentication of measurements made with in-plant instruments, based on remeasurement of some of the samples using a method under IAEA control.

Fig. 2. Procedure for IAEA authentication of measurements made with in-plant instruments, based on independent IAEA tests of in-plant instrument characteristics.

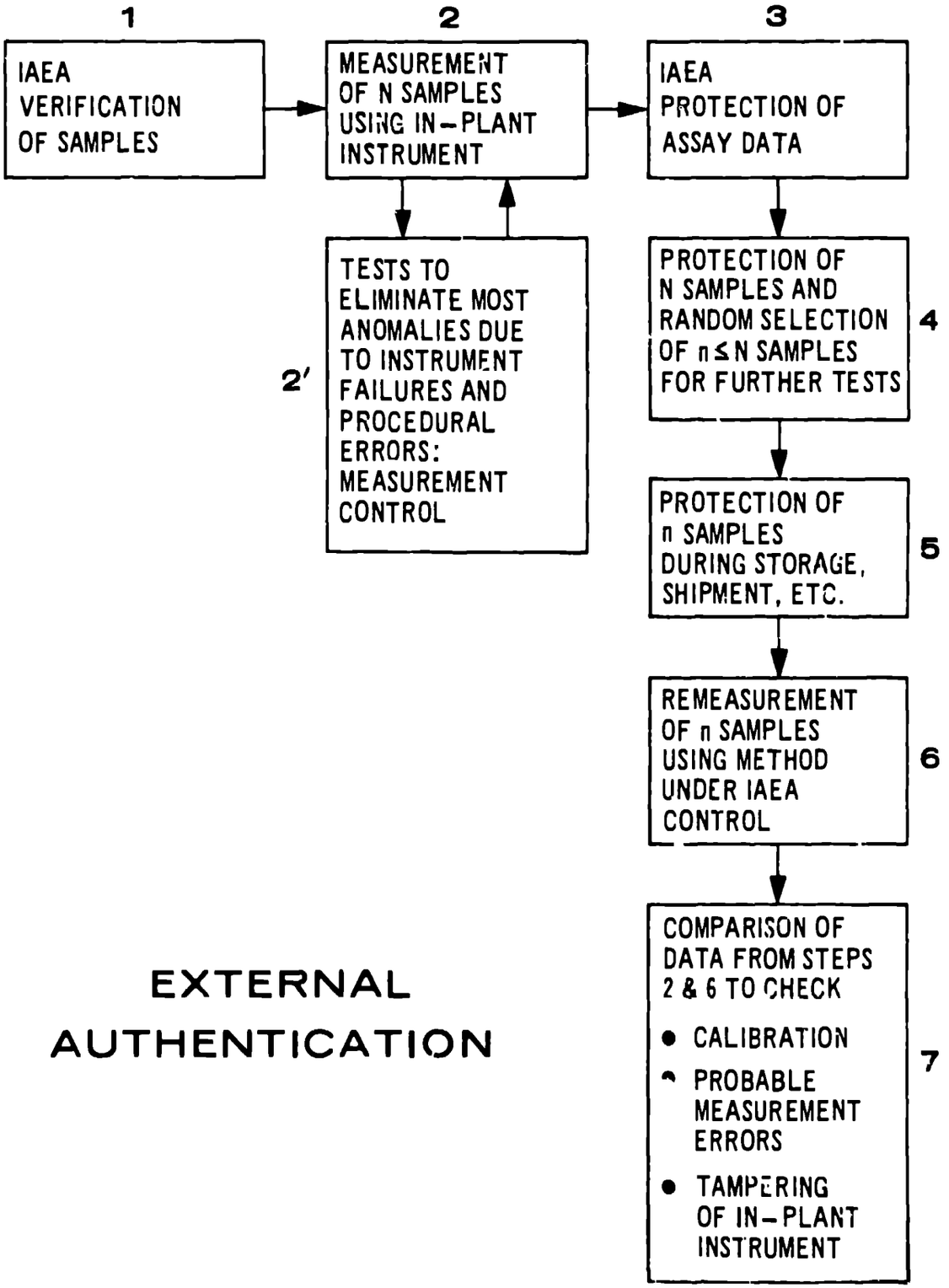

Fig. 1. Procedure for IAEA authentication of measurements made with in-plant instruments, based on remeasurement of some of the samples using a method under IAEA control.

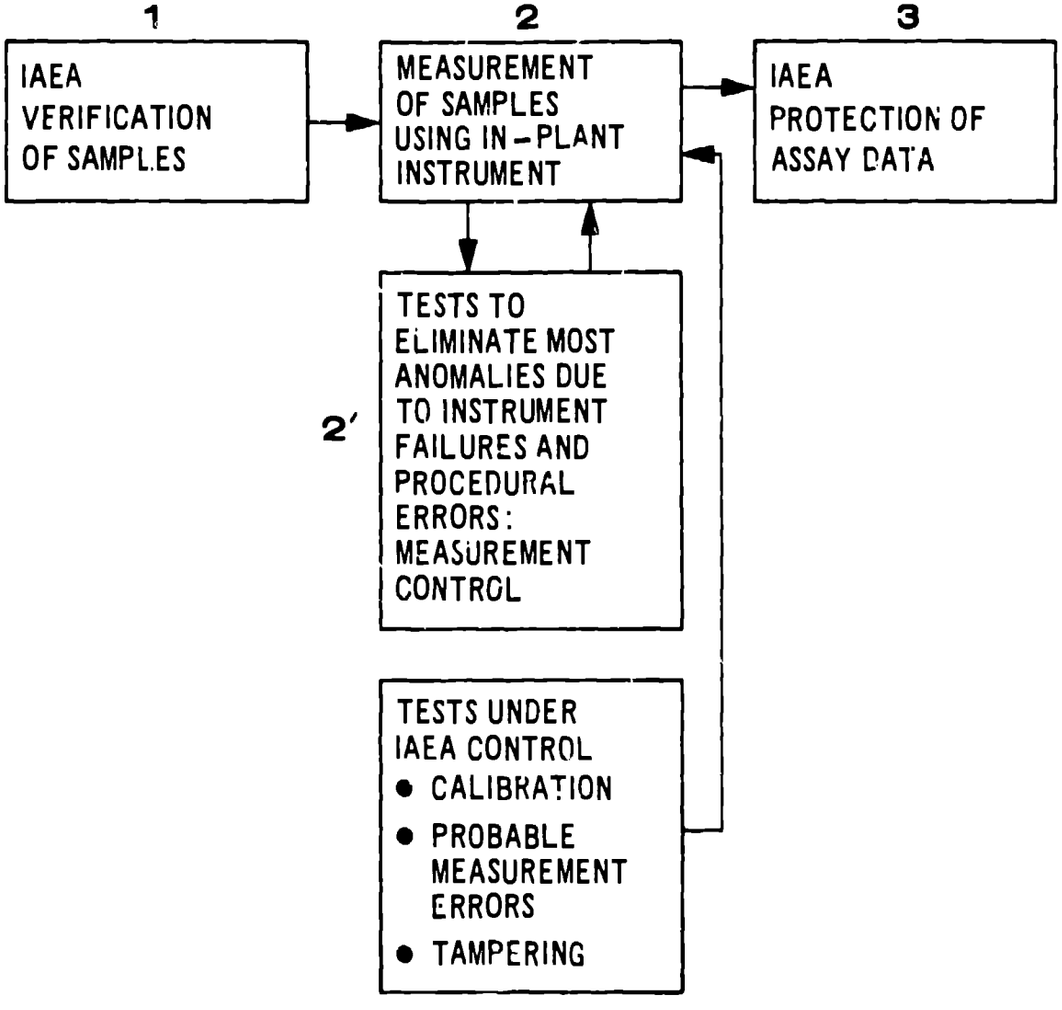

Fig. 2. Procedure for IAEA authentication of measurements made with in-plant instruments, based on independent IAEA tests of in-plant instrument characteristics.