

On-Site Procedures for Authentication of Mayak FMSF Monitoring Equipment

May30, 2001

PNNL Authentication Team

*This report was prepared for the
U.S. Defense Threat Reduction Agency*

On-Site Procedures for Authentication of Mayak FMSF Monitoring Equipment

1.0 Purpose of This Document

The PNNL Authentication Team was asked to provide a document specifying the types of authentication related activities for the Attribute Measurement System (AMS) that would be performed on-site at the Mayak Fissile Material Storage Facility (FMSF) during normal inspection visits. This document is intended to support development of text for a proposed protocol for monitoring party activities. The ground rules are to describe the types of activities that could be accomplished by two members of the monitoring party during one normal working day (about 6 hours).

This document is limited to discussing AMS authentication activity only for normal monitoring party visits and does not consider other periods of the equipment lifecycle.

2.0 Authentication Task Force Guidance

Authentication During Normal Operations – Once a facility becomes operational, Monitoring Party access may be limited. Some systems may only be used intermittently; in this case, periodic re-authentication prior to each use may be required. Other systems may be in continuous use and re-authentication would by necessity be accomplished by means that do not hinder operations. Whether systems operate in inspector attended or unattended mode will also impact what authentication and continuity of knowledge measures are required.

During normal operation of a facility, information will potentially be provided to the Monitoring Party through a combination of Host declaration, unattended measurements, and on-site inspections. Declarations might include information on each item entering and leaving a facility along with declared attributes for each item. Unattended measurements might include video surveillance of equipment and material that could be reviewed during on-site visits to insure continuity of knowledge of measurement equipment. On-site inspections would have as an important goal the measurement of items with authenticated measurement equipment. The measurement equipment would undergo some level of authentication prior to use during such on-site visits. Such authentication procedures could include, but not be limited to, the following activities:

- Checking TIDs on systems, components, and reference sources.
- Establishing characteristics of reference sources through independent measurements.
- Examining facility-monitoring information to provide continuity of knowledge of measurement equipment and reference sources.
- Performing functional testing of the system with randomly selected reference sources.
- Performing random comparisons of physical components to documentation.
- Performing random comparisons of software components to documentation.
- Performing random selection of system components for possible off-site authentication procedures.

Reference materials, sources, spare parts for the system, and components only used during onsite inspections must be stored in a fashion agreed by all parties. This storage should give the Monitoring Party confidence that the Host did not disturb these items during the period of time between inspections.

3.0 Assumptions Regarding Monitoring Party Activities at FMSF

Some assumptions need to be made about activities that will occur during inspection visits. We make the following assumptions with regard to monitoring party visit time constraints:

- Monitoring party will have ten 8-hour workdays on-site at FMSF per inspection period.
- Less intake and checkout time, about 6-hours will be available for AMS activity per day.
- Day 1 of the inspection period will be dedicated to AMS authentication.
- Days 2-last of the inspection period will be used for assaying containers of material.
- The last day will include activities to secure the AMS until the next inspection period.
- The storage cabinet for spare components is in room 358.
- The AMS will incorporate an open mode for display of data during authentication.
- Seals preventing undisclosed AMS access or operation shall be broken and reinstalled only in the presence of both parties.

4.0 Monitoring Party Rights During Routine AMS Authentication

The inspecting team shall be allowed to:

1. Supply, install, and check TIDs on AMS units, components, and reference sources.¹
2. Establish characteristics of reference sources² through independent measurements with monitoring party supplied equipment, and to retain the data from these measurements.
3. Examine containment and surveillance information to provide continuity of knowledge for AMS equipment and reference sources.
4. Perform functional testing of the AMS with Monitor selected reference sources.
5. Specify either open-mode or closed-mode operation during the collection of background or reference-source data.
6. Establish that software matches the standard copy, through hash function or other mechanisms.
7. Select and direct replacement of system components from spares.
8. Select system components for off-site authentication procedures.
9. Ascertain that previously approved procedures are used for storing, protecting and retrieving
 - Reference sources
 - Spare components
 - Complete spare systems
 - Monitoring-party-owned equipment and supplies to be left on site between visits

¹ If these Monitor prerogatives are yielded to the Russian party, confidence will be reduced, but some may be regained by adding to the time and completeness of the testing.

² The reference sources will be made by the Russian party to monitoring party specifications.

5.0 AMS Authentication Steps During On-Site Inspections

This section lays out possible monitoring party activities related to authentication of hardware and software, and functional testing. It is extracted from a comprehensive document being prepared by the Authentication Team entitled *Procedures For Authentication Of Mayak FMSF Monitoring Equipment* (first draft to be delivered June 1) that will discuss authentication procedures for all equipment lifecycle periods.

5.1 First Day Monitoring Party Authentication Activities – *Software Examination*

1. For higher confidence: The Russian party provides to the monitoring party several identical copies of *each* software-bearing component in the system (e.g., PROMs, once-programmable FPGAs, component subsystems, or entire systems). Each of the offered choices is identified by a permanent, unique mark acceptable to the monitoring party. The monitoring party shall be allowed to select a copy of each component to be installed for use and another copy to be immediately sent to a monitoring party facility in the U.S. All the items to be collected by the monitoring party shall leave immediately following the selection process by monitoring party's diplomatic courier. All non-selected items will be returned to the spares collection in controlled storage. All components offered for random selection will be identified as indicated above. At the start of each day's operation, identification marks will be recorded for each of the components in service. Without the type of identification specified above, some other adequate means of sealing/observing these components throughout the measurement campaign must be provided. If no permanent visible marking differentiates the components, other protection from sleight-of-hand swaps must be provided.
2. For somewhat less confidence: A *single* software-bearing component (not one of each type) can be selected for replacement. The balance of activities as described above.
3. For less confidence yet: If the software-bearing component is not removed to the U.S. immediately, a comparison of the software with a hash function in the field provides a slightly lower level of confidence than examination in the U.S. The hash function scheme (a secure enhanced checksum concept) is robust against tampering. The comparison could be performed in the AMS or on a monitoring-party-supplied computer in the field if adequate AMS I/O access is not negotiated. Hash function comparison requires implementation of the algorithm, a keyboard for input of a monitoring party provided key, and an output to display the hash function result for comparison to a value only known to the monitoring party.
4. Least desirable: The software-bearing component could be byte-for-byte compared on a monitoring-party-supplied field computer if continuity of knowledge of that computer is maintained. Use of a field computer for a byte-for-byte compare is less useful than the hash-function compare because the field computer could be compromised. The output of a byte-for-byte comparison is generally a YES/NO answer that could be erroneously output by corrupted comparison software.

5.2 First Day Monitoring Party Authentication Activities – *Hardware Examination*

1. For higher confidence: All the hardware components within the system shall be photographed in the presence of the monitoring party with a camera supplied by the monitoring party. This camera shall be either a high-resolution digital model or a high-quality self-developing film camera to allow the monitoring party to insure the quality of each picture and the Russian party to insure that no security measures are included in the pictures. An electronic record or high quality print of the photographs shall leave Russian party's control immediately by monitoring party's diplomatic courier. The monitoring party shall be allowed to select a hardware subsystem for replacement. The selected subsystem will be the analysis CPU or one of the sensor electronics modules. As with the software-bearing components, these components will be immediately removed by monitoring party's diplomatic courier.
2. For somewhat less confidence: A Russian-party-supplied camera meeting specifications of the monitoring party would be used instead. The balance of activities as described above.
3. For less confidence yet: Visual comparison performed by monitoring party against a monitoring-party-held photographic set.
4. Other measures: The monitoring party and Russian party can together identify a joint inspection team to make electrical measurements on the operational system to verify correct operations. Test points will be monitored with a battery-operated portable oscilloscope for correct voltage levels and waveforms. This joint measurement process will be limited to one hour. The team will have previously selected the test points to be used from the provided documentation.

5.3 First Day Monitoring Party Authentication Activities – *Calibration Source Examination*

The monitoring party will authenticate all the calibration sources using monitoring-party supplied, separate and totally unclassified measurement equipment. A 16-k channel HPGe spectrum of each of these calibration sources will be collected. A singles neutron count will be collected.

1. For higher confidence: The monitoring party will be allowed to carry back to the U.S. electronic copies of the gamma and neutron spectra and counts. In addition, an expert will be allowed to analyze each spectrum and make notes of the features observed.
2. For less confidence: A monitoring party expert will be allowed to analyze each spectrum and count while making notes of the features observed.

5.4 First Day Monitoring Party Authentication Activities – *Functional Testing*

The monitoring party will select calibration sources to be measured in open mode to verify that the system is properly functioning.

1. For most confidence: All the channel-by-channel data collected during open mode operation will be displayed in detail. This information will be printed on paper and recorded on electronic media for examination in the U.S.
2. For less confidence: All the channel-by-channel data collected during open mode operation will be displayed in detail. This information will be printed on paper for the monitoring party.
3. For less confidence yet: The data will be displayed for at least ten minutes.

5.5 First Day Monitoring Party Authentication Activities – *Maintain Continuity of Knowledge*

Maintaining continuity of knowledge of the AMS and its associated spares and functional testing sources between monitoring party visits is crucial in order to avoid extensive re-authentication activities during each visit.

1. For most confidence: Monitoring party will examine *all* TIDs placed onto the AMS and associated spares and functional testing sources. Facility Monitoring System video records of the AMS and its associated spares and functional testing sources will be reviewed to establish that no inappropriate access to the system, associated spares, or functional testing sources has occurred.
2. For less confidence: Monitoring party will examine *selected* TIDs placed onto the AMS and its associated spares and functional testing sources. Facility Monitoring System video records of the AMS and its associated spares and functional testing sources will be reviewed to establish that no inappropriate access to the system or its associated spares and functional testing sources has occurred.
3. For less confidence yet: Monitoring party will examine selected TIDs placed onto the AMS and its associated spares and functional testing sources.

5.6 Normal Assay Day Monitoring Party Activities – *Canister Measurements*

The normal assay measurements are conducted. A background measurement and energy calibration is made at the start of each day, as required for the routine measurement process. If the measurements require a 1-hour measurement period, 2-hours are allowed for each canister to provide time to retrieve and swap in the next canister. (Note: It is assumed the Russian party will begin the retrieval process during the previous measurement time and stage the canister near the absolute control room door. The time programmed to measure each canister requires specification.)

If delays occur that are beyond the monitoring party's control, the monitoring party shall be allowed additional equipment examination time or time for additional open-mode calibration measurements.

5.7 Any Inspection Day – Challenge Assay Testing

The monitoring party reserves the right to conduct challenge measurements with calibration sources selected from the pool of sources during each assay day. The monitoring party reserves the right during each assay day for photographing the hardware and/or verification of the software.

6.0 Example of a Monitoring Party Timeline for AMS Authentication

This section outlines *one possible* monitoring party authentication-day scenario timeline using the above descriptions. This example does not exercise all monitoring party rights, and different such scenarios will be expected to apply during different visits. It is assumed that two members of the monitoring party will be involved in these activities, and that each member has technical knowledge of AMS operation and authentication.³ Any TIDs removed will become monitoring party property and be returned to the U.S. via diplomatic courier.

- 0800 Arrive FMSF
Facility entry processing
- 0900 Enter room 358
Examine TIDs on systems, spare storage, and sources
Examine Facility Monitoring System video records to establish CoK
- 1000 Seal on AMS is broken, and AMS is opened
Monitoring party selects AMS subsystem is to be examined and notifies Russian party
Physical examination of open system, noting integrity of TIDs
Photographic record is made of hardware components
Russian party provides three identical copies of one monitoring party selected software-bearing component
Monitoring party marks each component provided
Monitoring party selects component to be installed and component to return to the U.S.
- 1100 AMS is turned on in open mode
Monitoring party observes correct startup diagnostics results
Hash function algorithm is run to validate AMS software
System is observed to operate normally with a check source
- 1200 A californium source is used for “measurement control” (testing) of the NMC
Energy calibration of HPGe is performed with sources and results observed
- 1300 Background HPGe measurement is started
Lunch break

³ Two members of the monitoring party are needed to ensure CoK for equipment or sources temporarily deprived of protection by TIDs.

- 1400 Background measurement result is observed
 - AMS placed in secure mode
 - Unclassified 4kg plutonium standard is placed in AMS
 - Data collected with unclassified 4kg plutonium standard with correct output
 - Unclassified 4kg plutonium standard is removed from AMS

- 1500 Low mass isotopic plutonium source is placed in AMS
 - Low mass isotopic plutonium source is measured by AMS with correct output
 - Low mass isotopic plutonium source is removed from AMS
 - System is left on in secure mode at end of testing

- 1600 Exit and jointly seal room 358
 - Facility exit processing

- 1700 Depart FMSF