LA-UR-99-5611

Proposed Attribute Measurement System (AMS) with Information Barrier For the Mayak/PPIA Demonstration: System Overview

Duncan W. MacArthur

EXECUTIVE SUMMARY

There are two major objectives for the Mayak/PPIA demonstration. The first is to demonstrate to the Russian delegation that an attribute measurement system (AMS) can be built with sufficient protection to allow measurement of classified components without revealing classified information. The second, to construct this AMS in such a manner as to convince the Russian delegation that it would be possible for an inspecting party to fully authenticate operation of the system.

Six attributes will be measured in the demonstration AMS. These are:

1) presence of plutonium,
2) plutonium isotopic ratio,
3) plutonium mass,
4) plutonium age,
5) presence of oxide, and
6) symmetry of the plutonium.

In order to measure these attributes the demonstration AMS will use three detection systems connected to four analyzing computers. The three detectors are:

1) a medium sized (50%) germanium detector-based high resolution gamma spectroscopy (HRGS) system,
2) a large (100%) germanium detector-based HRGS system, and
3) a neutron multiplicity well counter (NMC) with the ability to individually read out each bank of tubes.

The medium sized HRGS detector and associated analyzer will be used to measure Pu presence, isotopic ratio, and Pu age. The larger HRGS detector and associated analyzer will be used to (1) measure oxygen content and (2) identify the presence of oxides. The neutron multiplicity detector and NMC analyzer will be used to compute Pu mass and identify the presence of oxides. Only if an oxide signature is detected in both the HRGS and the NMC will an object to be classed as “oxide”. Finally, the signals from eight segments of the multiplicity counter will be used to measure the symmetry of the object being monitored.

Measurement of any of these attributes requires use of a detection system that generates classified data. Thus, an information barrier hides all of the “raw” data and only unclassified yes/no threshold evaluations are shown on the unclassified display.

The demonstration AMS can operate with the access doors open or closed. When the access door is closed, a red and green LED display is the only output from the system. In this configuration, either classified items or unclassified reference materials can be measured, but only the simple unclassified display is possible. When the access door is opened, all power is immediately removed from the system. Since no data is stored in non-volatile memory, this power removal, in combination with an active purge procedure, will ensure that no classified information can remain in the AMS after the door is opened. If, and only if, no classified material is present in the AMS, the security

watchdog will restore power to the AMS following a delay of approximately 20 seconds. This will allow authentication measurements to take place using unclassified reference materials only. If a classified object is placed in the system while the door is open, all power to the system will be immediately cut off and will remain off until the classified item is removed or the access door is closed.

Raw data generated in any of the three detectors passes into the shielded enclosure and to the one of the four data acquisition systems and analyzers. Both the raw data from the detectors and the analyzed data from the analyzers will be classified if a classified item is being measured. The analyzed results pass into the computational block where the attribute threshold values are stored and threshold comparisons are performed. The outputs from the computational block, in the form of yes/no data, leave the shielded enclosure through the data barrier and are sent to the unclassified display. Although the outputs from the computational block are unclassified, these signals are inside the shielded enclosure and are treated as classified until they pass out of the enclosure through the data barrier.

There are several additional important elements of the AMS that are not in the direct data processing path described above. All power for the AMS enters the security watchdog through an AC line filter. The only function of the security watchdog is to monitor the security status of the entire system and to remove all power from all other AMS elements if the access doors are opened or if classified material is introduced into the system incorrectly. The security mode of the security watchdog (and hence the entire AMS) is set by the security switch that is controlled by the security container itself without human intervention. In addition, several data switches are used to start a background run, start calibration runs, and start measurement runs.

The AMS for the Mayak/PPIA demonstration will use 5 computers; one each for the two HRGS systems, two for the neutron multiplicity detector (one for mass & oxides and one for symmetry) and one for the computational block. All five will be implemented with simple hardware such as the PC-104 specification and use simple software. Most importantly, all of these CPUs are located within the shielded enclosure. All communications with the unclassified area are either simple hardware switch controls (the data switches) or filtered through the (hardware) data barrier. There is at least one “hardware only” element between each of these CPUs and the outside world. Thus, the programming in the CPUs cannot affect the hardware components of the information barrier. In particular, it is physically impossible for one of the CPUs can reprogram either the data barrier or the display to reveal classified information. In addition, all data flow within the AMS is unidirectional. No information can be passed from the display back to the remainder of the system.

Another important feature of the demonstration AMS is the separation between the security and data switches. The security switch controls the security watchdog directly. The security watchdog, in turn, controls the power to all of the other elements of the AMS, **but** there is no other connection from the security watchdog to the CPUs. Thus, the CPUs do not know the position of the security switch and have no way of knowing whether they are processing classified or unclassified data. This adds some assurance that the analyzers are operating similarly whether or not a classified item is being measured.

INTRODUCTION

The objectives of the Mayak/PPIA demonstration are:

1) to demonstrate to the Russian delegation that an attribute measurement system (AMS) can be built with sufficient protection to allow measurement of classified components without revealing classified information, and
2) to construct this AMS in such a manner as to convince the Russian delegation that it would be possible for an inspecting party to fully authenticate operation of the system.

The AMS illustrated in Fig. 1 was designed to meet both of these goals. More details of this design are included in Ref. 1.

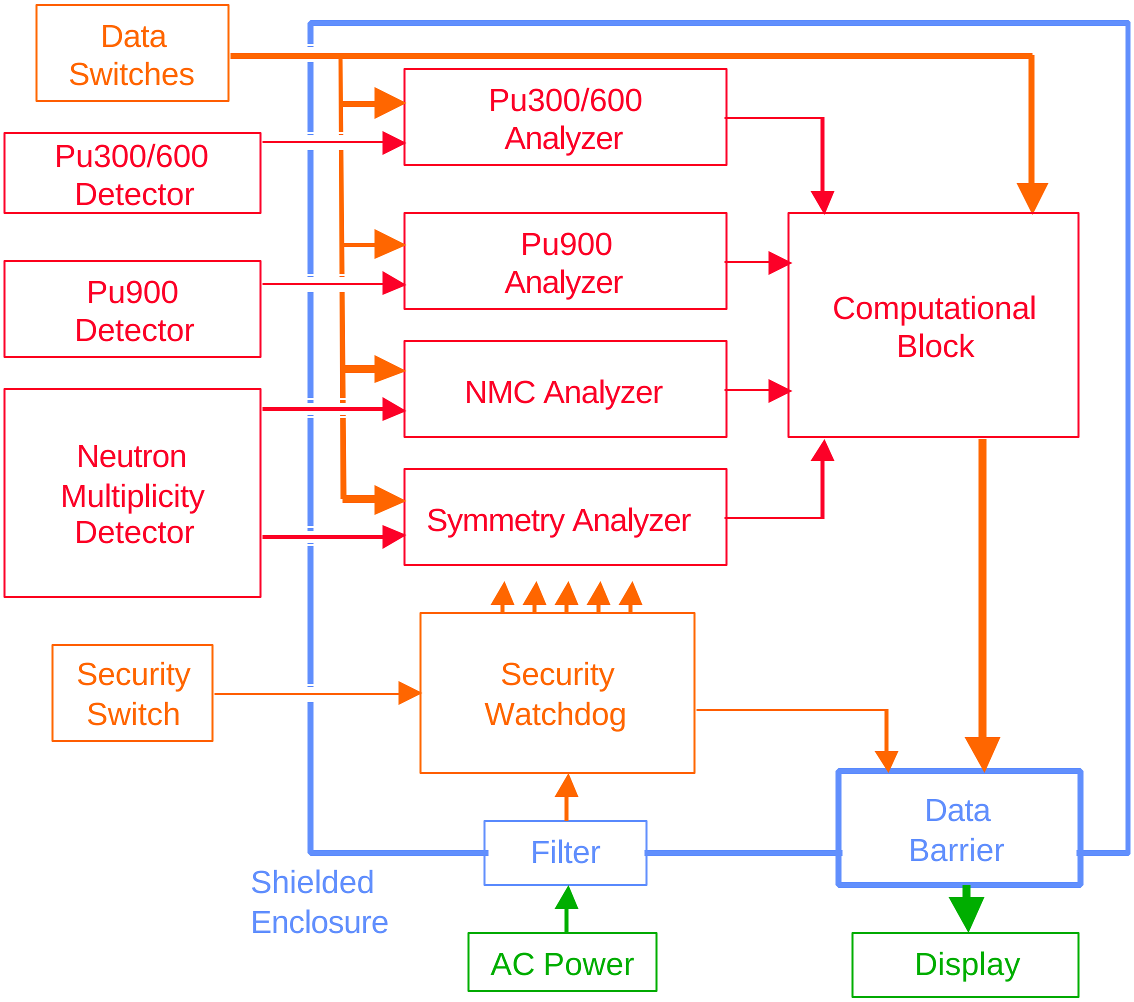

Fig. 1. Block diagram of attribute measurement system (AMS) for Mayak/PPIA. Elements that may contain classified information are shown in red. Elements that are themselves unclassified but must be treated as classified because of their location or function are shown in orange. Unclassified elements are shown in green. The protective enclosure and associated elements are in blue.

Six attributes will be measured in the demonstration AMS. These are:

1) Presence of plutonium,
2) plutonium isotopic ratio,
3) plutonium mass,
4) plutonium age,
5) presence of oxide, and
6) symmetry of plutonium.

Measurement of any of these attributes requires use of a detection system that generates classified data. Thus, an information barrier hides all of the “raw” data and only unclassified yes/no threshold evaluations are shown on the unclassified display.

As shown in Fig. 1, the raw data generated in the **detection systems** (described in sections 1.x) passes into the **shielded enclosure** (section 8.1) to the specific data acquisition systems and **analyzers** (section 2.0). Both the raw data from the detectors and the analyzed data from the **analyzers** will be classified if a classified item is being measured. The analyzed results pass into the **computational block** (section 3.0) where the threshold values are stored and threshold comparisons are performed. The outputs from the **computational block**, in the form of yes/no data are passed through the **data barrier** (section 4.0) and finally to the unclassified **display** (section 5.0). Although the outputs from the **computational block** are unclassified, these signals are inside the **shielded enclosure** and are treated as classified until they pass out of the enclosure through the **data barrier**.

Several additional important elements of the AMS are also illustrated in Fig.1. All power for the AMS enters the **security watchdog** (section 6.0) through an **ac line filter** (section 8.2). The only function of the security watchdog is to monitor the security status of the entire system and to remove all power from all other AMS elements if the access doors are opened or if classified material is introduced into the system incorrectly. The security mode of the **security watchdog** (and hence the entire AMS) is set by the **security switch** (section 7.2). In addition, several **data switches** (section 7.1) are used to start a background run, start calibration runs, and start measurement runs. Other important features of the **physical barrier and emanation reduction** are discussed in section 8.x.

1.0 DETECTION SYSTEMS

As discussed above, this AMS will employ of 3 detector systems, a large HRGS, a medium-sized HRGS, and a neutron multiplicity counter (NMC) modified to provide access to the signals coming from individual banks of ^{3}He tubes. All three detector systems will be co-located around a single measurement position. The most likely way to accomplish this will be to arrange both HRGS detectors to “look” through the walls of the NMC at the source position.

All connections for all detectors will run to the shielded enclosure. All power for the detectors will be derived from the shielded enclosure and controlled by the security watchdog.

1.1 Pu300/600 - The aforementioned medium sized germanium detector (50%) will be used to supply the raw data for both the Pu300 and Pu600 analysis programs. These analysis programs will run sequentially in a single computer so that, although Pu300 and Pu600 are separate analysis programs, they will both be running in a single HRGS system.

The Pu300 analysis uses the data from a region around 300-keVin the plutonium gamma-ray spectrum. As plutonium ages, more and more ^{241}Am is created (in the plutonium) through β-decay of ^{241}Pu. Thus, the amount of ^{241}Am present in the object being measured is indicative of the age of the object. The region around 300 keV includes spectral lines from ^{241}Am that can be used to determine the amount of americium present in the object and infer the age of the plutonium in the object.

The spectral region around 600 keV is analyzed by the Pu600 code to provide both an isotopic ratio (^{240}Pu /^{239}Pu) for the object being measured and an indicator of the presence of plutonium. The spectral region around 600 keV includes lines of both ^{240}Pu and ^{239}Pu. A comparison of the strengths of these lines provides a measure of the isotopic ratio of the object. The existence of the lines is indicative of the presence of plutonium.

The germanium detector for the Pu300/600 system will be located in an interlocked solid enclosure that will provide shielding and physical protection for the detector itself. The MCA and analysis computer for this sub-system will be located within the large shielded enclosure along with all the other AMS electronics. The detector enclosure will be connected to the main shielded enclosure by a set of shielded cables specific to the HRGS system. This bundle of shielded cables will be located within another shield, probably a braided tube.

1.2 Pu900 – The larger (100%) germanium detector supplies raw data for the Pu900 analysis. This analysis utilizes data from the region around 900-keV in the plutonium gamma-ray spectrum. This region includes lines indicative of oxygen content in the plutonium being measured. Thus, the Pu900 measurement is one test that may indicate the presence of oxides in the plutonium being measured.

The germanium detector for the Pu900 system will also be located in an interlocked solid enclosure that will provide shielding and physical protection for the detector itself. The MCA and analysis computer for this sub-system will be located within the large shielded enclosure along with all the other AMS electronics. The detector enclosure will be connected to the main shielded enclosure by a set of shielded cables specific to the HRGS system. This bundle of shielded cables will be located within another shield, probably a braided tube.

1.3 Multiplicity Counter – The NMC used in this demonstration consists of thirty-six ^{3}He tubes mounted within the four walls of a rectangular polyethylene enclosure. During normal operation, the count rates for non-coincident, doubly coincident, and triply coincident events (singles, doubles, and triples) are measured in the NMC detector. If the efficiency of this detector has been measured, then the singles, doubles, and triples can be used to calculate the ^{240}Pu effective mass, the fraction of (α,n) reactions (or α), and the multiplication in the sample. With the isotopic ratio, the ^{240}Pu effective mass is used to calculate to Pu mass and α is used as an indicator of oxide presence.

The neutron detectors and polyethylene of the NMC are located in a solid metal enclosure that will provide shielding and physical protection for the detector itself. The shift register and analysis computer for this sub-system will be located within the large shielded enclosure along with all the other AMS electronics. The detector enclosure will be connected to the main shielded enclosure by a set of shielded cables specific to the NMC system. This bundle of shielded cables will be located within another shield, probably a braided tube.

1.4 Symmetry Detector – As well as being combined for the multiplicity measurement described in section 1.3, signals from the eight octants of the neutron detector will be counted individually to provide an indication of the symmetry (in 2 dimensions) of the object under test.

As described above, the neutron detectors will be located in a solid metal enclosure. The analysis computer and any associated hardware will be located in the main shielded enclosure. The detector enclosure will be connected to the main shielded enclosure by a set of shielded cables specific to the symmetry system. This bundle of shielded cables will be located within another shield, probably a braided tube.

2.0 ANALYZERS

All of the CPUs used in the AMS in general (5), and the analyzers in particular (4), will be small, easily inspectable, and with documented functionality. Each of the four measurement systems discussed above will include a separate CPU as its analyzer. These separate CPUs, among other advantages, will allow each measurement system to be tested separately without requiring the remainder of the AMS to be operational.

The analyzer CPUs will all be implementations of the PC-104 standard and will all use DOS operating systems. These CPU boards are commercially available; for this demonstration, the commercial boards will be used with excess functionality disabled but not removed. All of the analyzers will be within the shielded enclosure and all will receive their power from the security watchdog.

3.0 COMPUTATIONAL BLOCK

The attribute threshold values are stored (in read only memory) in the computational block and attribute threshold comparisons are also performed in this element. In addition, any calculations requiring the results from more than one analyzer are performed in the computational block. There is no interconnection between analysis computers aside from the computational block. The inputs to the computational block from the analyzers are potentially classified but the outputs from the computational block to the data barrier are unclassified (yes/no) values.

As implemented in this demonstration, the computational block will use a small, easily inspected computer with limited hardware and software functionality. The demonstrated computational block will be based on an Ampro 3SXI 386 computer with an Emerald digital I/O card. This PC-104 specification CPU will be running a DOS operating system. As with the analysis CPUs, there is no data connection between the security watchdog and the computational block.

4.0 DATA BARRIER

The only function of the data barrier is to pass unclassified information from inside the shielded enclosure to the display. Operationally, this can be separated (somewhat) into 2 requirements.

1) The data barrier will only pass information from the computational block to the display. No information can be passed from the display to the remainder of the system.
2) The data barrier will not pass classified information.

In ordinary operation, no classified information will be presented to the data barrier by the computational block. In any event, the data barrier is implemented in simple hardware so that it cannot be “reprogrammed” to pass other types of information.

As implemented in the demonstration system, the data barrier utilizes fiber optics drivers and fiber optic links to the display to ensure that no data can pass back into the shielded enclosure. The fiber optic links also ensure that no extraneous electrical signal can be picked up or radiated by the links to the display. The fiber optics drivers are driven by either flip-flops or low-pass filters. The flip-flops are clocked once each measurement cycle so that only one change of output state is allowed for each measurement. Ideally, all signals derived from the computational block would pass through flip-flops clocked by the security watchdog. However, in this implementation, all of the threshold data signs do pass through flip flops, but the “measurement complete” and “error” signals pass through low-pass filters. In this demonstration system, the flip-flops are clocked by the computational block. The two security signals are derived directly from the security watchdog. Thus, an additional flip-flop stage is not required and low-pass filters will be used in these signal paths.

5.0 DISPLAY

The unclassified display is another simple hardware circuit with no computer-controlled functions. The optical signals transmitted by the data barrier are received in optical receivers. The optical receivers in turn are connected to LED drivers, which are connected directly to the red and green LEDs. All power for the display is DC that is generated within the shielded enclosure and sent to the display through a shielded cable. Thus, the security watchdog also controls the display power.

The display for the Mayak/PPIA demonstration AMS has 8 red and 8 green LEDs and no other displays. Six pairs of LEDs are used to indicate passing or failing the 6 attribute tests. The remaining four LEDs are for system “housekeeping” functions. One pair indicates the security status of the AMS, i.e. they indicate whether the system is open (red) or secure (green). An additional green LED indicates that a measurement has been completed and the final red LED is indicative of a hardware malfunction within the AMS.

6.0 SECURITY WATCHDOG

The demonstration AMS can operate with the access doors open or closed. When the access door is closed, the red and green display is the only output from the system. In this configuration, either classified items or unclassified reference materials can be measured, but only the simple unclassified display is possible. Whenever the access door is opened, all power is immediately removed from the system. This, in addition to an active purge procedure, will ensure that no classified information can remain in the AMS after the door is opened. If, and only if, no classified material is present in the AMS, the security watchdog will restore power to the AMS following a delay of approximately 20 seconds. This will allow authentication measurements to take place using unclassified reference materials only. If a classified object is placed in the system while the door is open, all power to the system will be immediately cut off and will remain off until the classified item is removed or the access door is closed.

The only function of the security watchdog is to control the AC power to the rest of the AMS as described above. The security watchdog uses simple relay logic with no silicon components or software. There are two power relays in the watchdog. The first, or main, relay turns on AC power to the remainder of the AMS if, and only if, the doors to the shielded enclosure and any auxiliary enclosures are closed. In this case power is applied to the AMS regardless of whether or not classified objects are present (as indicated by the security switch.) If a door is opened, the main relay contacts open, and all power is removed from the remainder of the AMS. Following a delay of approximately 20 seconds, a second relay will close (re-energizing the AMS) **if** no classified material is present (as determined by the security switch).

In addition, the security watchdog incorporates a SCRAM switch that, if pressed, will remove all power from the AMS regardless of whether classified material is present or not.

6.1 Active Purge – Any time the doors are opened, all power is removed from the system. Since no data is written into non-volatile memory during AMS operation, this operation should remove all classified information. (This power-down method is termed a “passive purge”.) However, in cases where a passive purge is not sufficient, the volatile memory must be overwritten before the purge is considered complete. (This overwriting method is termed an “active purge”.)

An active purge of the memory in the demonstration AMS is performed procedurally rather than electronically. The SCRAM button is pressed and manually released prior to opening the access door. The computers are allowed to restart (which overwrites their entire RAM) **before** the door is opened. This procedure can be repeated as many times as required to achieve appropriate sanitation of the system.

7.0 SWITCHES

The demonstration AMS will incorporate two types of switches. (1) Security functions of the security watchdog will be controlled by the SCRAM switch, the door switches, and the security switch itself. All switches performing security functions will be normally closed switches operating in a “fail-safe” configuration, i.e. if any of the cables connecting these switches is not connected fully, then the switch is assumed to be open. (2) The data analysis systems will be controlled by the data switches, a set of mechanical switches separate from the security functions. If the cables to the data switches are not connected correctly, no measurements can be initiated and the system will not function until the connection is fixed.

A key feature of the demonstration AMS is the separation between the security and data switches. The security switches control the security watchdog (and only the security watchdog) directly. The security watchdog, in turn, controls the power to all of the other elements of the AMS. There is **no** other connection between the security watchdog and the CPUs. Thus, the CPUs do not “know” the position of the security switches and have no way of “knowing” whether they are processing classified or unclassified data. This adds some assurance that the analyzers are operating similarly whether or not a classified item is being measured.

Similarly the data switches are demonstrably not connected to the security watchdog. No manipulation of the data switches can change the security status of the system.

7.1 Data Switches – These push-button switches, operated by the material handler (as opposed to an inspector or observer) control the starting of background, calibration, or measurement cycles within the AMS. Once any type of cycle has been started, additional switch closures have no further effect. These switches are simple hardware closures – no further electronics or processing capability is included in this part of the AMS.

Ideally, the source container itself would make the determination as to what type of measurement was required and the handler would push a single “start” switch. However, for this demonstration, the handler will also make a determination as to which switch is appropriate.

7.2 Security Switch – The container that holds a classified item presses against a mechanical security switch when the container is placed in the detector of the AMS. Thus any container is assumed to contain classified material unless that container has been specifically modified so as not to contact the security switch.

In the demonstration AMS, the security switch will consist of 2 switches in series, either one of which is sufficient to indicate a classified container.

7.3 Door Switches – Both doors to the shielded enclosure as well as the doors to the HRGS detectors will be instrumented with interlock switches. Each door of the shielded enclosure will have 2 switches (top and bottom) and each smaller door of the HRGS detector enclosure will have one switch.

All of these switches must be closed (i.e. all doors closed) before classified material can be measured in the AMS.

7.4 SCRAM switch – In addition to the door switches, a SCRAM switch will be mounted on the shielded enclosure. The SCRAM switch is operable from outside the shielded enclosure. If the SCRAM switch is pressed, all power is immediately removed from the AMS (other than the security watchdog) regardless of the position of the other security switches. The AMS cannot be restarted until the SCRAM switch is manually reset.

As detailed in section 6.0, the SCRAM switch also forms part of the active purging operation in the demonstration AMS.

8.0 PHYSICAL BARRIER AND EMANATIONS REDUCTION

Although the AMS will be constructed of tested components using good assembly procedures, the final proof of the effectiveness of the system shielding has to be an actual measurement of the entire AMS after assembly is complete. Following these measurements, a physical exclusion area around the AMS may be defined in order to meet RF power limits.

8.1 Shielded Enclosure – All of the CPUs and high-level signal (as opposed to detector output signal) wiring will be contained within a shielded enclosure. The enclosure for the demonstration AMS will be a Hoffman PROLINE EMI/RFI high performance enclosure. This enclosure includes spring finger contacts around all door openings and welded construction and is rated for 30 dB attenuation at 1 GHz. All door and ventilation openings in this cabinet will be as supplied by the manufacturer. All other penetrations in the enclosure will be made according to manufacturer recommendations.

8.2 Power Filtering - All power for the AMS will enter the shielded enclosure through a Corcom CDSRW-E series filter. This filter is mounted directly on the inner side of the shielded enclosure and the AC socket is enclosed in the shielded volume of the filter. This type of filter is specified to have an insertion loss of > 100 dB from 14 KHz to 10 GHz as per MIL-STD-220A.

8.3 Cable Shielding – As illustrated in Fig. 1, the detectors for this demonstration AMS are not within the shielded enclosure. The detectors will be connected to the shielded enclosure through cable bundles. These cables, as well as the detector enclosures, will be shielded to reduce electronic emanations. In addition, each bundle of shielded cables from a detector will be located within another shield, probably a braided tube. The exterior shield will not be carrying any signal information – i.e., this shield will not be used as a "return" for the signal wiring or to carry any other signal.

8.4 Physical Barrier – Most of the elements (and all of the elements incorporating memory) of the AMS are protected from physical interference by the shielded enclosure. However, the detectors and detector cabling are outside of this enclosure and require other protective measures. For this demonstration system, the HRGS detectors will be enclosed in interlocked shielded enclosures that are interconnected to the security watchdog. The NMC will be enclosed in a shielded enclosure, but interlocking this enclosure was not possible for this demonstration. Thus, physical protection for the NMC detector and all cabling will be provided by procedural limitations on access.

REFERENCES

[1] Duncan MacArthur and Geoffrey Dransfield, "PPIA System Wiring Diagram," Los Alamos Publication LAUR-99-5295, September 1999.