LA-UR-09- 063603

Approved for public release;
distribution is unlimited.

Title:	Third-Generation Attribute Measurement System Conceptual Design Report
Author(s):	Crystal Dale, David DeSimone, Peter Karpius, Duncan MacArthur, Morag Smith, Jonathan Thron, Duc Vo, Richard Williams Los Alamos National Laboratory
Intended for:	Deliverable to NA-241

Los Alamos
NATIONAL LABORATORY
EST. 1943

Third-Generation Attribute Measurement System Conceptual Design Report

September 28, 2009
Los Alamos National Laboratory

Los Alamos National Laboratory
PO Box 1663
Los Alamos, NM 87545

Contents

Executive Summary

An attribute measurement system (AMS) is intended to measure a number of unclassified attributes (e.g., mass above threshold and isotopic composition below threshold) of a sensitive special nuclear material (SNM) item. These attributes can be used to confirm a declaration (made by the "host") concerning the SNM without revealing any sensitive information to the monitor. Although the AMS concept is applicable to all types of SNM, the discussion presented here will concentrate on plutonium measurements.

The design of the third-generation AMS (3G-AMS) will incorporate lessons learned in the minimum functionality AMS project,[1] the authentication working group,[2] the next-generation AMS,[3] the Russian neutron/gamma AMS (AVNG),[4] the United States (US)/United Kingdom (UK) authentication workshop,[5] and the US/UK information barrier workshop.[6] These lessons learned, in turn, draw on lessons learned in the Trilateral Initiative demonstration[7] and the Fissile Material Transparency Technology Demonstration (FMTTD).[8]

Although this conceptual design is intended as a basis for the final design in fiscal year (FY)10, some design details or directions may change as a result of ongoing AMS and minimum functionality research or in response to hardware and software availability issues. We have attempted to specify feasible solutions in this paper; however, some conflicts may not be discovered until the detailed design process occurs. Other compromises may need to be addressed during the construction of the 3G-AMS, which is anticipated to occur in FY11.

As with the Trilateral Initiative, FMTTD, and AVNG designs, we intend the final design and construction of the 3G-AMS to be a joint effort incorporating contributions from several laboratories. In addition, we intend to incorporate the contributions of two separate red teams: one for authentication (representing the monitor's interests) and one for certification (representing the host's interests). Both red teams will be independent of the design groups.

The 3G-AMS will use a high purity germanium (HPGe) detector system to measure the gamma rays from the item and a modular neutron multiplicity counter for the neutrons. These detector components will be separate units connected to an Electronics Box (E-Box) that will contain most of the electronics and the computer to process the detector information, calculate the attributes, and control the operation of the AMS. The E-Box will have display lights to indicate the results of the assay. The system will be modular, small, inexpensive, and have only the minimum functionality required to perform the measurements. These characteristics will aid in the authentication and certification of the system.

For the 3G-AMS, authentication will be achieved primarily by using a random selection of the system/parts to be used in the measurement and validation systems. The validation modules are then brought to the monitor's home facilities and examined in detail to ensure that the modules operate as expected. To have this process make sense, a strict continuity of knowledge (CoK) must be maintained from the time of random selection until the validation modules get home. Equally important is maintaining a CoK on the measurement system from the time of its selection through its use. There must also be the capability of performing a sufficiently detailed examination of the validation modules.

Another level of authentication comes from using reference radiation sources to determine that the measurement system produces the correct results when measuring the sources. The sources are nonsensitive and would be measured in detail to ascertain that they are the sources we expect.

Certifiability in the 3G-AMS is achieved by careful design to avoid potential information leakage paths. Once assembled, the system comprises an enclosing Faraday cage. The integrity and continuity of the Faraday cage connections are monitored by a watchdog circuit that can power off the entire system, thereby flushing all sensitive information if it detects an error.

The interconnections between the system components extend the Faraday cage between them with enclosing, conducting connections. The power into the system would be strongly filtered to eliminate any signaling.

The only accepted path of information in and out of the system would be via the lights and the button on the E-Box; these components would be kept to a minimum. Additionally, the level of sensitivity of the information in the detector modules would be kept low. Calculations that produce sensitive results take place only in the E-Box, and its interior will not be accessible.

1 INTRODUCTION

An attribute measurements system (AMS) could be used in a treaty verification regime, by a monitoring party, to confirm declarations made by the host party about special nuclear material (SNM) items covered by the treaty. These items will typically be stored in containers that cannot be opened during a monitoring visit. The AMS makes nondestructive analysis (NDA) measurements on these containers and calculates values associated with the SNM based on those measurements. If displayed directly, some of these measurements and calculated values might reveal information about the declared items that the host considers sensitive. The AMS is designed so that it displays this information only in a nonsensitive form that has been agreed to by both parties. Potentially sensitive information could be translated into a nonsensitive form by comparing the calculated values to agreed-on threshold values and displaying only whether the calculated values are above or below that threshold. These nonsensitive comparison results are termed "attributes." In addition to carefully controlling the information that is displayed to the monitors, the AMS must prevent unintended releases of the sensitive information. The design of an AMS is such that the measurements and calculations are made inside the system, out of sight of the monitors, and only the carefully controlled attributes are visible on an external display. The subsystem that protects the sensitive information is called an "information barrier" (IB).[9] This barrier includes the physical enclosure of the system, electronics and sensors to monitor the integrity of the enclosure, and also the electronics and software to ensure that only the attributes are displayed. An AMS is considered certified when its IB, and any accompanying operating procedure, is deemed secure enough by the host to allow the SNM items to be measured by the AMS in the presence of the monitors.

If an AMS is used, the task of the monitoring party is to confirm the declaration made by the host concerning the SNM contents of storage containers. The amount of available information may be quite limited because the IB may display only a red light or a green light (i.e., the attribute is above or below the threshold). An AMS is said to be authenticated if the monitoring party has sufficient confidence that the limited information available to it accurately reflects the properties of the item being measured, thus allowing the monitors to confirm the declaration concerning that item.

Although several AMSs have been built that can make the required measurements and calculations, and several have been certified,[10] the problem of authenticating a system has not been previously examined in detail. Many methods have been proposed, and some have been tested. We are developing a conceptual design for an AMS that will be able to be both certified and authenticated—the Third-Generation Attribute Measurement System (3G-AMS). This design is based on previous experience in building such systems, most recently the Next-Generation Attribute Measurement System (NG-AMS) built at Los Alamos National Laboratory.[11,12] The goal of the NG-AMS and of the 3G-AMS is to measure sealed canisters of plutonium. Both systems measure the neutron and gamma-ray emissions from the plutonium to calculate three values: the mass of the plutonium, the $^{240}Pu/^{239}Pu$ ratio, and the date on which the ^{241}Am was last separated from the plutonium. Because these values may be considered sensitive, they are compared with agreed thresholds to generate the unclassified attributes, plutonium mass above threshold, plutonium isotopic ratio below threshold, and plutonium age greater (or possibly less) than a threshold. Different attributes could be calculated if desired, and the

methods of authentication being considered could be applied to AMSs measuring items other than plutonium containers.

For the purposes of this paper, we consider it likely that the hosts would build and assemble the AMS for use in their facility—thus making it easier to certify. We also assume that the monitor will not be allowed to examine the AMS once it had been used to measure sensitive items.

The monitor's main concern in authenticating an AMS is that a mode of operation that is not immediately visible could be activated to produce an incorrect result. Such a mode could cause the AMS to display a green light when actually the canister being measured contained no plutonium. The problem of authenticating an AMS can be thought of as gaining confidence that no such mode exists or that procedures and tests are in place that have a reasonable chance of detecting the existence of such a mode (often referred to as the "hidden switch" problem). The monitoring party must also be confident that the AMS is capable of making the required measurements.

2 AUTHENTICATION DESIGN CONSIDERATIONS

We have considered a number of methods that can be used to increase the monitor's confidence in the AMS. To increase the monitoring party's faith in the AMS, several of these methods would be used. Absolute confidence in an AMS is unachievable, but a combination of methods may make the implementation of a hidden switch too complicated, too costly, or have too high a risk of it being detected to be worth implementing.

2.1 Inspection of the AMS

Carefully examining the AMS with all its subsystems could reveal a hidden switch. Such an examination could range from a cursory overview, which might discover an obvious hidden switch to a detailed, potentially destructive, analysis of all components, which could find all hidden switches. An inspection of the measurement system at the host's facility will likely be limited by the time, people, and equipment available to the monitors. Also, a thorough, destructive analysis would render the system unusable for the intended measurements. Therefore, for the purposes of this report, we assume that an inspection of the AMS at the host facility would not be as thorough as we might desire.

An alternative would be for the monitoring party to be allowed to thoroughly inspect an AMS that is identical to the AMS used for the measurements. In this case, the identical system could be brought back to the monitor's country and be tested by any method desired. Testing could be accomplished without the host country's presence, allowing a much broader spectrum of tests. The threat of unknown tests could be more of a deterrent than the completion of a set of previously negotiated tests on site. A sufficiently thorough inspection would reveal any hidden switches.

The effectiveness of inspection of an identical system depends on the monitoring party's confidence that the two systems were, and would remain, identical. Thus, the effectiveness of this type of inspection depends on the monitor's ability to maintain continuity of knowledge (CoK) of both the measurement system and the identical system.

2.2 Random Selection

A powerful method of obtaining an identical AMS to be inspected is random selection from a pool of AMS modules. At the time of the monitoring visit, a measurement AMS is made up of components randomly chosen from the pool, and other modules are randomly chosen by the monitors for testing in the monitor's country. The host would not know beforehand which AMS modules would be inspected and which would be used for the measurement.

The random selection process could be applied to entire AMSs or to AMS modules that could be assembled into complete systems. Ideally, the random selection would be performed at the beginning of each day, during which measurements would be made. This procedure would allow the monitors to watch the systems and not need to rely on tags and seals to ensure that the selected systems had not been altered. However, such a daily "reauthentication" process would require a very large number of modules to be purchased at the beginning of the planned

measurement campaign. Especially for the more expensive AMS components [e.g., the high-purity germanium (HPGe) gamma detectors], these purchases could be quite expensive. Furthermore, appropriate storage of many modules could present additional difficulties. A more practical solution may be to randomly select modules only at the beginning of each monitoring measurement visit. The systems would be stored in sealed rooms, perhaps with video monitoring, and would be fitted with unique identification tags. An intermediate option would be to make the selection of the measurement and validation systems at the beginning of the visit but have the option to select more components throughout the visit. These components could be used to replace the corresponding one in the measurement system or to be one of those brought back to the monitor's country.

The 3G-AMS will be designed to facilitate random selection. The design is not directly affected by the choice of the random selection procedure.

2.3 Joint System Design

Monitoring party confidence requires a thorough understanding of the AMS. This understanding can be achieved best by having the AMS jointly designed by all parties. The joint work would be not only at the level of the conceptual design, but also at the level of the implementation and layout of the system. The monitoring party would then know what it expects to see and would be more likely to recognize anything that had been added (or removed). An additional benefit would be that the monitoring party would be assured that the system was actually capable of functioning and making the measurements as expected. The joint design would apply to all aspects of the system—both hardware and software. Although this consideration is mostly relevant in actual treaty situations, for the 3G-AMS we intend to make all design information available to both the authentication and certification red teams.

2.4 Use of Open/Secure Modes

An AMS can be designed to have an "open mode," as well as the normal secure mode used to measure the sensitive items. In the open mode, the internal workings of the system can be seen by the monitor. In this open mode, the following could be observed: the raw data acquired from the sensors, the progress of the calculations performed, the results of the calculations, and the attributes shown on the external display. Observing and understanding the operation of the system in open mode allows the monitors to verify that the AMS **can** operate as expected. In a carefully laid out system, an open mode can also provide some confidence that the AMS would work as expected when it was returned to the secure mode (where the internal workings are hidden). Implementing such a system [as was done in the NG-AMS, Fissile Material Transparency Technology Demonstration (FMTTD), Russian neutron/gamma AMS (AVNG), and the Trilateral Initiative demonstration] requires care that the open mode can be entered only when a nonsensitive item (e.g., a reference source) is being measured. Also, transitioning from the secure to the open mode must not leave any residual sensitive information that could be seen. When nonsensitive items are switched in the open mode, care must be taken that the system does not enter the secure mode between the two open states. Another problem is that in the open mode, any results observed could give information about nearby sources (potentially sensitive) or the background radiation field in the facility.

Although observations of the AMS in the open mode could provide confidence that the system was capable of proper operation, the inspection of the system would likely be cursory and not reveal any well hidden switches.

2.5 Functional Testing of the Measurement System

Presenting the AMS with a known, nonsensitive radioactive source and observing the resultant display can help provide assurance that the system is capable of operating properly. These test items could include objects that should produce a negative result, as well as ones that should produce positive results. The test items could be interspersed in the measurement sequence randomly or in an order chosen by the monitor. Test items could be measured in combination with sensitive ones.

More information derived from functional testing is available if an open mode is implemented in the AMS. However, the concept is equally applicable to single (secure)-mode systems.

2.6 Use of Commercial off-the-Shelf Products

An idea that has been explored in AMS design and construction is the use of commercial off-the-shelf (COTS) products. In the case of the NG-AMS, the detectors, signal processing electronics, computer, enclosure, and software were all COTS products. The concept was that these products would be purchased from manufacturers who had no motivation to tamper with their products to subvert an AMS treaty verification system. The manufacturers would be motivated to make profits only by pleasing their customers. If COTS items were used in an AMS, the monitor could have confidence that the items performed the functions that the manufacturer claimed and had no hidden switches. An additional benefit would be that the COTS items could be commonly used, giving the monitors (and the hosts) familiarity with their capabilities and operations. Items that have been produced for the commercial market are usually well tested, and any remaining problem would have been found by the customers and presumably corrected. This process could help make the AMS more reliable.

Several issues were found with this approach. Much of the electronics had more functionality than was needed or wanted for an AMS. The manufacturers added many bells and whistles to satisfy their customers or to make their equipment more flexible or convenient to use. Some of these features went counter to the AMS's security needs and had to be removed (making the item no longer strictly COTS). Although the COTS idea could work for items that were produced in large quantities and sold all over the world, some of the equipment used for radiation measurements is so specialized that the manufacturer does not have any of them "on the shelf" but assembles each item when the order is placed. Thus, the manufacturer knows the customer and might be able to guess as to the use. A major concern is that the COTS item might have to be inspected in detail in any case to ensure its proper operation. In this case, the overly complex and possibly proprietary system would be more difficult to inspect than a simpler, custom-built one.

2.7 Blind-Buy Purchases

A technique that can be used in conjunction with COTS is to purchase the items in such a way that the manufacturer/retailer cannot know who is making the purchase. This technique further

increases the assurance that the manufacturers have had no motivation to tamper with their standard product. Such a blind buy could be accomplished by making the purchase through a third party.

2.8 Use of Minimum Functionality Products

An alternate approach to the COTS-centric design is to build custom components that perform exactly and only the functions needed. These items would be built to be as easy to inspect and understand as possible. Custom design could apply to both software and hardware components of the system. Although these custom items would be easier to authenticate than COTS items if a full inspection were required, these items could lack the flexibility and robustness of a more complex COTS system. A tradeoff of measurement capability and reliability could be made for simplicity, which will have to be carefully evaluated in light of the measurement requirements. Custom-built products have the disadvantage in that they must be tested and documented by the institution producing them and that their reliability in prolonged use may be unknown. Limited support may also be an issue.

Any AMS will be a hybrid custom/COTS system. Some components (e.g., HPGe crystals and microprocessor chips) would be difficult to implement as custom designs. Others (e.g., IB and security components) are unlikely to ever be produced as COTS. However, many other AMS elements can be implemented as either COTS or custom designs. Minimum functionality systems could be implemented, mostly in software[13] or alternatively in hardware.[1] A software-centric system would digitize the signals from the measurement devices as soon as possible and then perform all subsequent operations in software. A hardware-centric system would put as much of the functionality as possible in custom electronics or programmable gate arrays. Benefits and drawbacks of authenticating electronics versus software or custom versus COTS must be considered.

2.9 Minimization and Control of Inputs

Limiting and controlling the inputs to the AMS can help minimize unintended signaling paths that could be used to instruct the system to respond differently to different items being tested. Such input could be used to activate a hidden switch. The AMS should be blind to the item type—performing the same predefined functions for all types. These limitations mean that the AMS's computer must have most of the information needed for making measurements, processing the data, and controlling the sequence stored internally and not rely on external inputs.

The NG-AMS had only two inputs: the alternating current (AC) power, which was heavily filtered to prevent such signaling; and a single button on the control panel to tell the computer to proceed to the next step in its sequence. The circuit receiving inputs from the button could not change states faster than 1 Hz, thus preventing the possibility of rapidly tapping out instructions on the button.

2.10 Maintaining Continuity of Knowledge

CoK for an item (either physical or information) comes when a party is confident that a continuous chain of custody has been maintained during the time period of interest. This chain can be achieved by various methods, including watching or sensing the item (e.g., directly or via cameras), securing the item against outside access (e.g., placing it in a sealed container or encrypting it), or entrusting it with a trusted party or procedure.

Although the methods listed in the sections above can increase the monitoring party's confidence in the performance of an AMS, most of these techniques require maintaining CoK from the time the system is authenticated until the measurement is made or the system is checked in the monitor's home country. This requirement is based on the assumption that the party that has the last sole possession of the system can modify it. This modification could be to add a hidden switch before the AMS is used for a measurement or to remove one before it is examined by the monitor.

One way to maintain CoK of the measurement system would be to have one or more of the monitors (and the host party) continuously watching the system or modules. Although this concept sounds straightforward, the system may have to be moved around the facility and the monitors would have to be allowed continuous access. Even trained observers are fallible; psychologists, as well as stage magicians, have demonstrated that human attention can be diverted, that we will often see what we expect to see, and that we can concentrate only on a limited number of tasks at one time. These natural human tendencies could be exploited to perform a sleight-of-hand trick to exchange one item for another.

During monitoring visits that are longer than one day, the monitors will need some way to ensure that the system is still operating correctly the following day after being "unattended" all night. One approach would be to "reauthenticate" the system to be used for that day's measurements each morning, which could be time consuming and require a large random-selection pool. A more traditional approach would be to have cameras or other sensors monitor the AMS during the night. Additional confidence could be gained by placing tags or seals on the AMS itself and/or on the room or special container where it is stored.

Maintaining CoK on any modules or systems shipped back to the monitor's country for validation presents a related, but different set of challenges. The items would have to be transported in such a way that the host country could not have access to the shipment.

3 3G-AMS CONCEPTUAL DESIGN

Our conceptual design for a 3G-AMS is to build a system with the following characteristics.

- Where possible, custom components with the minimum functionality required will be used. This requirement will aid the certification, as well as the inspections for authentication. The components should be designed to be as simple to inspect and understand as possible. Because AMSs would be used only to make confirmatory measurements, the measurement quality does not have to be the very best possible, although they still have to be adequate for this situation. In a given measurement campaign, many of the parameters will have been defined by the treaty and so the measurement instruments will have to be capable of making measurements only for a limited range of conditions. These instruments need not be for general purpose use.

- The AMS will be assembled out of components that should be as inexpensive as possible within the system requirements. This feature will allow a random selection to be made from a larger pool if random selection is used as an authentication method. The modules should be relatively small in size to make them easier to transport, but not so small as to make them hard to observe for CoK.

- The system will not have an open mode, which simplifies the AMS design and the operating procedures. We will test the system using a series of reference radioactive sources that have been verified before each use.

3.1 Physical Design

The conceptual design is illustrated in Figure 1. It consists of a number of modules: an electronics box (E-Box), an HPGe detector, and several neutron slab detectors. Within this concept, several considerations apply to design of the modules:

- The efficiency requirements of the neutron measurement system will determine the number and placement of the slabs. Slabs could be located on all sides and even the bottom/top of the container.

- The HPGe detector could have a clear view of the plutonium container (allowing a higher count rate and perhaps a smaller crystal) or could measure gamma rays coming through one of the neutron slabs (similar to the NG-AMS), depending on both gamma- and neutron-system requirements.

- The E-Box contains the multichannel analyzer (MCA), the shift register, a computational system to determine the attributes, and the information barrier.

- The E-Box also has external display lights and a single button. These operator interfaces are similar to those located on the NG-AMS control panel.

- All modules, both detectors and electronics, will have integral Faraday cages, which have conducting connections to the E-Box.

- All connections between the E-Box and the neutron and gamma module are shielded. These shields are extensions of the Faraday cage, effectively making a single larger Faraday enclosure. The connections could be cables, or various enclosures could "snap" together. Snapping the modules into a single unit could make the certification easier. Optical fiber connections could be possible, depending on the types of signals being transmitted.

- All of the Faraday cages and shields are attached to the building ground through a single point on the E-Box.

- The E-Box will contain a watchdog circuit to ensure that all modules are properly connected and grounded before operation is allowed. Because there is no open mode, there are no doors to monitor. A system will monitor that the Faraday cage remains intact.

- All of the "smart" electronics is protected in the E-Box; only simple electronics will be used in the detector modules. Information sent from the neutron slabs and the gamma system to the E-Box will be unprocessed (to the extent possible) to reduce the amount of potentially sensitive information in the detector modules, as well as their complexity. The outputs of the neutron slabs will be digital pulse trains, and the gamma module output will be amplified pulses from the HPGe detector.

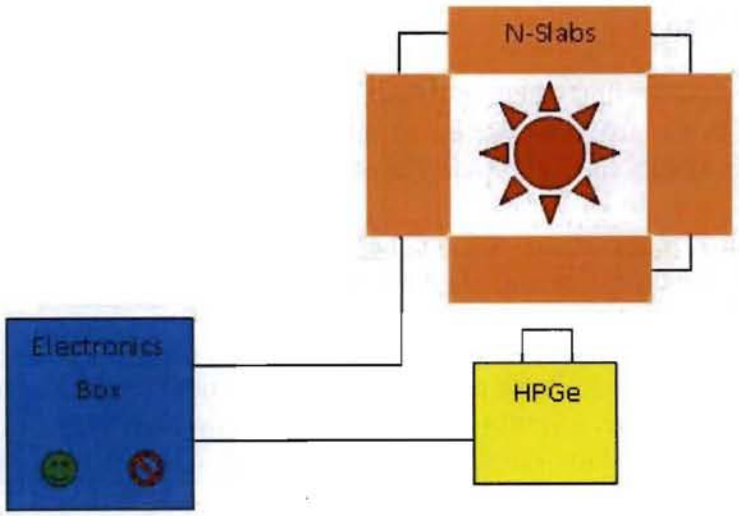

Figure 1 shows a schematic layout of the conceptual design of the 3G-AMS. The item to be measured is surrounded by several modular neutron slab detectors (the exact number and configuration has not yet been determined) to count neutron emissions and an HPGe gamma-ray detector to register the gamma-ray emissions. The detector modules are connected to an E-Box where all the processing is performed. The E-Box also provides the limited display and user input to the system.

3.2 Neutron Measurement System

The purpose of the neutron measurement system is to determine the quantity ^{240}Pu effective. The ^{240}Pu effective is an estimate of the mass of plutonium present calculated as if the neutrons were emitted entirely from ^{240}Pu. Combined with a measurement of the isotopic fractions, as described in the next section, this measurement is the basis for an evaluation of the total mass of plutonium present that, when compared with a threshold value, is one of the assumed attributes.

Past attribute measurement systems have used high-efficiency neutron multiplicity counters (NMCs) for the neutron measurement.[14] If the measurement quality is the only concern, an NMC is the clear solution because the high efficiency generally makes the neutron measurement easy to perform with adequate precision. The essential simplicity of an NMC—^{3}He proportional tubes embedded in polyethylene—makes certification reasonably direct. However, the size and cost of an NMC makes it difficult to work into proposed authentication schemes. If an NMC were subject to random selection, the transportation of the NMC back to a monitoring party's home country would require shipping it as freight—methods for simply taking a piece of equipment back with the monitoring party would not apply. Shipping the NMC as freight would almost certainly require breaking any planned, visual, continuous surveillance by the monitoring party and require the extensive use of tags and seals to maintain CoK. Even if these authentication problems were surmounted, the cost issue would remain. An NMC, as a single piece of equipment, is typically at least a $250k purchase. Maintaining a pool of NMCs ready for monitoring use and withdrawal under random selection would quickly become very expensive.

The 3G-AMS approach makes the neutron measurement system more amenable to authentication while still taking advantage of the relative simplicity of the detector (i.e., ^{3}He tubes embedded in polyethylene). Smaller neutron detector modules or slabs would be assembled to create a composite NMC out of units that individually are much more transportable and much less expensive. Our design would attempt to make the individual blocks as interchangeable as possible so that the selection of one from a pool would adequately represent the entire pool.

Once the neutron detectors have been assembled into an NMC configuration (see Figure 1), the neutron measurement procedures will be very similar to those used in prior AMSs. As a first step, the neutron measurement system will evaluate the neutron background. The background measurement is used to subtract background counts from the neutron measurements. Typically, in (non-AMS) NMC applications, the background is measured periodically throughout a measurement campaign, either daily or whenever a change in background is possible. For an AMS, measuring the background raises some additional issues. Because the background measurement may be greatly (relatively) separated in time from the item measurement, it is possible that changes in the background will occur without the monitors' knowledge and adversely affect the measurement. This problem can be managed by frequently checking the background, administrative controls to require substantial open space around the AMS, and combinations of cadmium and polyethylene shielding around the AMS to minimize the effects of background.

The primary functional check of the neutron measurement system is an evaluation of the detector efficiency. A known neutron emitter (typically a Californium source) is measured, and the neutron count rate is corrected for decay. The calculated efficiency is compared with an efficiency determined in the initial setup of the system. An efficiency that differs from that expected is a sign of either a system malfunction or an unknown, and thus unallowed, change in the system configuration.

After the neutron background and detector efficiency have been verified, no further checks are required of the neutron measurement system. The nature of the neutron measurement does not require calibration. However, it is expected that further functional testing using reference standards will be carried out.

3.3 Gamma-Ray Measurement System

The primary purpose of gamma-ray system of the 3G-AMS is to determine the isotopic composition of the plutonium item. Given the density of gamma-ray lines from plutonium in the relevant regions of the energy spectrum, an HPGe detector will be used because it has the necessary resolution to distinguish the lines. The detector may be measuring the gamma rays penetrating through the neutron detector modules, which means that only the higher-energy (>~200KeV) lines will be available for analysis. This restriction was also the case for the NG-AMS. The HPGe crystal will be sized to allow a data acquisition time that is comparable to the neutron detection system's and will give a sufficiently accurate determination of the plutonium isotopics. The HPGe crystal will be surrounded by a collimator/shield pointing at the plutonium item. This collimator will reduce the effect of potential background radiation.

The isotopic information generated from the gamma measurements also contributes to the determination of total plutonium mass. The ^{240}Pu effective mass is determined by the neutron system, as described above. This effective mass will be combined with the isotopic information to generate the total plutonium mass.

Finally, if it is determined that the 3G-AMS should calculate the "date of last ^{241}Am removal from the plutonium" attribute, the 3G-AMS will need a date determination system similar to that used in the NG-AMS. This measurement would require mounting small ^{210}Pb and ^{241}Am sources on the face of the HPGe detector (on the outside the cryostat). The date measurement system will not place any additional requirements on the gamma-ray system, so the inclusion of, or lack of a date measurement does not affect the conceptual design. Software would need to be included to extract the date from the relative areas of the lead and americium peaks, as well as to determine "time since separation" from the plutonium and americium peaks generated by the SNM.

If the date sources are present, they can be used to determine that the gamma-ray readout chain is working properly. If they are not present, a small source will be needed regardless to perform this function.

The HPGe detector will need to be cooled; either a mechanical cooling system or a liquid-nitrogen (LN_2)-filled dewar could be used. The dewar is a simpler system and can provide faster cooling times. Its downside is that it will need to be regularly filled with LN_2.

3.4 Electronics Systems

The electronics for the 3G-AMS must perform several functions.

- A minimal amount of processing of the raw detector signals will be done at the detector modules themselves. All higher-level processing will take place in the E-Box to concentrate any potentially sensitive information there. Thus, the neutron detector modules will include amplifier/discriminators, probably commercial units, for the ^{3}He tube output. The logic signals generated by these discriminators will be sent to the E-Box. The HPGe module will include a cooled field-effect-transistor preamplifier and possibly an amplifier at room temperature. These units are expected to be commercial and supplied by the HPGe module vendor. The analog pulses will be sent to the E-Box for shaping and digitization.

- The electronics for reading out the neutron and gamma-ray detectors will be located in the E-Box. These electronics are expected to be custom made to minimize their extraneous functionality and designed for easy authentication.

- A processor in the E-Box will perform data analysis and control the system. This processor will be relatively simple, but the computing power requirements will have to be evaluated. The processor will be connected to the neutron and gamma-ray readout electronics and will provide output for the attribute display. The software for the processor will be located on a separate nonvolatile memory chip.

- A watchdog circuit will confirm that the detector modules are correctly connected and that the integrity of the Faraday cage enclosures is maintained. If an error is detected, the watchdog will shut off all the power to the system. All electronics components will be designed/chosen to lose any potentially sensitive information on power loss. (Removing all writeable nonvolatile memory is impractical in modern electronics, but care will be taken not to write sensitive information to this memory.)

- Display lights and an input button will be mounted on the E-Box. These components will need driver circuits and a means to ensure that the state of the display and the button cannot change faster than about 1 Hz. The input/output (I/O) can be controlled either directly from the processor or by a data barrier that receives and sends simple messages to/from the processor. (This approach worked well in the NG-AMS.)

- Low-voltage power supplies for the electronics and high-voltage supplies for the detectors will be contained in the E-Box.

- A filter will be used for the incoming AC power. All power will be supplied to the 3G-AMS through this filter.

For ease of certification and authentication, the electronics will be implemented with the minimum functionality necessary to perform the tasks required for the AMS adequately. AMSs may not need to make highly precise or accurate measurements, and therefore, such capability

should not be implemented in the electronics. The electronics will be mostly custom designed, although commercial components will be used.

The readout for the neutron multiplicity system can be implemented as a shift register. A shift-register-on-a-chip has been designed using a field-programmable gate array (FPGA). Shift registers are well understood technology and would be fairly straightforward to certify and authenticate.

The gamma-ray detector will require an MCA for its readout. This part of the circuit will need an analog front end and a digitizer before the information can be passed to digital logic. Some older designs for MCAs that perform the minimum functions required are available and would be implemented with more modern electronics.[12]

In the 3G-AMS, the digital logic will be implemented in FPGAs, which will significantly increase the ease of prototyping and revising the system. FPGAs are complex devices but can perform many functions in a single chip. They are configured by writing a "program" based on circuit diagrams. This program is then "compiled" to a set of instructions that configures the FPGA. The instructions that configured the FPGA can be downloaded and checked to ascertain that the FPGA has the expected configuration. Authentication of the program, and especially the compiler, may be problematic because the compiler is typically a proprietary product of the FPGA manufacturer. However, given a trusted copy, the configuration of an FPGA can be verified. Alternatively, the logic could be implemented in simple chips, but this would necessitate a large increase in chip count and board size.

3.5 Software

To make the software as easy to authenticate as possible, it will be written in a clear, well-structured fashion. In a treaty-implemented AMS, the parties to the agreement should develop the software jointly; but regardless, well-documented source code should be available so that an expert in the field can fully understand the program flow and the algorithms used. This understanding will ensure that the software is capable of performing the functions required.

Any software that runs on the processor, as well as any software that processed the analysis/control programs, will need an authentication procedure to give the monitoring party confidence that it is performing as intended. Not only must the programs written to perform the tasks needed for the AMS be checked, but also the operating system of the computer and the compilers and linkers of the code. A direct method would be to write all the software needed in the assembly language of the processor used. This would eliminate the need for an operating system and a compiler. Although this solution is possible, writing assembly language is a painstaking, tedious process that few programmers would want to undertake for anything but a very short program. Reading assembly language code is also slow, making the authentication process cumbersome.

For the 3G-AMS, we will move one step away from this extreme solution and write the programs in a fairly low-level procedural (non-object-oriented) language such as C. Given the C source code and the binary output of the compiler, we have tools that can ascertain that the source code did, in fact, produce the binary and that no "hidden" functions have been added. We

will run the processor without an operating system—all I/O and interfaces will be handled as part of the C program. Given that floating point operations will be needed for the analysis of the neutron and gamma-ray data, we will use a processor with a hardware floating-point unit that will remove the need for linking in outside software routines.

Once the software has been written, compiled and tested, it will be burned to a nonvolatile memory chip and attached to the processor board. To verify which software the processor is using, the contents of this memory chip can be examined and easily compared with a known "golden" copy. For this procedure to make sense, we will precisely define the processor type (and lot) and the compiler that are to be used. A different complier could produce slightly different machine-language instructions, and the processor must be the one to match the program and the compiler's output.

The control/sequencing program would be written to match the processor and electronics hardware configuration and to implement the operating procedures described below. The data analysis programs will be kept as simple as possible but could use algorithms from existing programs, such as FRAM (fixed-energy, response function analysis with multiple efficiencies) or MGA (multi-group analysis) for the gamma rays or INCC (International Atomic Energy Agency neutron coincidence counting) for the neutrons. If used, these programs will be stripped of their extraneous features, such as graphical user interfaces, the ability to process input from many detector types, and the ability to change processing parameters.

3.6 Concept of Operations

The assumed mode of operation for the 3G-AMS is to

1. perform a random selection of AMS modules: some to form the measurement system to be used in the host's facility and some to be returned to the monitor's facility for further validation,

2. verify the characteristics of the reference sources,

3. make the measurements with these sources and the potentially sensitive items in an order specified by the monitor, and

4. bring the selected AMS validation modules back to the monitor's facility to be examined in detail.

It is assumed that both parties will maintain continuous visual contact with the measurement AMS and the selected validation modules. Following the random selection process, we will place the selected AMS validation modules in a diplomatic pouch for transport back to the monitor's home facility. This procedure will ensure that the monitoring party maintains CoK during the entire transportation process.

Although the procedures for a specific treaty would have to be negotiated, we assumed an operating procedure to be used for the 3G-AMS. A large part of authentication comes from the

procedures of operation which are used. Some of the design criteria of the 3G-AMS were to facilitate these operations. The procedure is outlined in more detail in the list below.

1. Operations 2–8 (listed below) would be performed at the beginning of the monitoring measurement visit (a duration of perhaps 1 week) and would be repeated for the next visit.

2. Modules would be randomly chosen from a stockpile: one complete set to construct a measurement AMS and other modules to return to the monitor's facility for validation. The HPGe detectors should be precooled so that they are ready to operate.

3. The monitors would maintain CoK on each module during and after assembly into complete systems.

4. Measurements of the reference materials (RMs) and other standard sources would be made with standard equipment. All spectra, counting rates, and other information would be available. These measurements possibly could be done with the detector components of the actual measurement system (but probably not its E-Box).

5. Having gained confidence that the characteristics of the RM are as expected, the monitors would maintain CoK on the RMs throughout the monitoring visit. The HPGe detector will have to be kept cold throughout the measurement visit.

6. Measurements of the RMs and the sensitive items would be made with the measurement system. Because there is no open mode, only red/green lights would be visible. The RMs could be measured multiple times throughout this measurement cycle, and the order of measurements would be chosen at the last minute.

7. At the end of the day of measurements, the measurement system and the validation modules would each be fitted with a unique identification tag and placed in a sealed container or room ready for use the next day.

8. At some time after random selection, the validation modules would be placed in a diplomatic pouch for return to the monitoring party's facility. Possibly only pieces of the system would be taken home. This procedure would minimize the risk associated with storing them in the host's facility during the visit. The modules would be carefully packaged to avoid damage during transport.

9. The validation modules would be analyzed in detail at home. A credible (both in terms of cost and technical feasibility) method must be available for examining the validation modules in complete detail.

10. In addition, the stockpile of modules would be stored in a tamper-indicating enclosure at the host facility between measurement visits and the parts would have unique identifications that would be checked as they are randomly chosen and throughout the process.

4 APPLICATION OF SYSTEM ENGINEERING TO 3G-AMS DESIGN

The Institute of Electrical and Electronics Engineers (IEEE) standard definition for a "man-made system" is a "collection of hardware, software, people, facilities, procedures, and other factors organized to accomplish a common objective." This statement encapsulates the complexity of developing an operational system, which beyond the "device" includes the full context of the device's implementation, over its entire life cycle, under all states or modes of operation.

The purpose of system engineering as applied to system design and integration is to reduce the risk associated with system development. System development progresses necessarily, although not equally, along four parallel paths or domains. These four domains are the derivation and prioritization of requirements, decomposition of system functions, evaluation of solution alternatives (usually termed the physical description), and design verification. The communication between the various stakeholders (the customers, the software and hardware designers, the requirements managers, the systems integrator, etc.) is the most critical component of development risk.

System engineering provides a structured formal language for communicating among the various stakeholders. The further application of model-based systems engineering (MBSE) provides a common repository for all four domains of the system development. Having that common language and common repository of record, allows the design development to proceed along all four domains in an integrated fashion, reducing or eliminating costly, sometimes unrecoverable, design errors.

The linking of the four domains via the common database allows changes in one domain to be reflected in all other domains, with little time lag. Further, the documentation of design decisions is integrated with the requirements derivation, creating an auditable trail for design decision bases.

As an extension of the system engineering effort, the database could feed into a "critical nodes" analysis. A "critical nodes" analysis is a risk-based analysis of the pathways by which the system could fail to perform as desired. Identification of these "critical nodes" helps to prioritize allocation of resources during the design development.

4.1 Functional Description

System engineering provides a formal tool to simplify the design thought process: functional decomposition. Functional decomposition concentrates on what the system must do, not on how well it must perform or on what the physical instantiation of that function may look like. The simplifying power of this approach lies in that there may be numerous ways to perform a given function, but at its most granular level, only one function must be performed. In later design stages, each function must have a performance metric by which a given solution is judged. These performance metrics will become the functional and performance requirements for the system.

The diagrams provided over the next several pages provide the functional decomposition of the 3G-AMS. In the structured semantics of MBSE, functions are verbs because a function describes

what the system must "do." Figure 2 presents the top-level functional decomposition of the 3G-AMS with the top-level function to verify a treaty item. The immediate next-level functions that must be accomplished to achieve that function are to assess the item using a system that has been certified, producing results that are authenticated. Even this level of functional decomposition opens up immediately to the discussion of performance metrics/requirements. How accurately does the item need to be assessed? How confident does the host need to be in the certification of the system to allow entry into their facility? How confident does the monitor need to be in the authentication of the system to believe the results? We believe we have answers to some of these based on earlier prototyping; however, the confidence level for authentication, which is the focus of this effort, has been identified as a need.

To break the decomposition down further, for the device to assess an item, that device must have some means to control the operation of the measurements being made, make those measurements, determine the calculated results from the given data, and provide results. Again, it does not matter at this point how these functions get performed, but that all necessary functions are identified. For the system to be certified, the system must provide both physical and information security to preclude the inadvertent or purposeful transmission of sensitive information. For the results to be authenticatable, protection against tampering must be provided for the system, along with provision for providing CoK throughout the time of interest. Again, metrics associated with these "soft" parameters will need to be rolled up into the confidence of authentication at a later stage of design.

The following series of functional diagrams continues to break down the higher-level functions into manageable chunks for discussion purposes. Figure 3 provides the basic functions solely for control of the measurement system operation.

Figure 4 provides the measurement functions needed to be able to quantify the assumed attributes of age, isotopic ratio, and mass. The current depiction does not include other potential measurement methods, such as thermal measurements, because it is assumed that thermal measurements will not be made. Should that decision change, the function to collect thermal data would be entered as a subfunction to function 1.2.

Figure 5 provides a more complicated structure, which describes the functions that need to be performed to transform the raw data into the calculated results of age, isotopic ratio, and mass. It can be seen in the diagram that the gamma spectra play a role in both the age and isotopic ratio determinations, which further impacts the mass determination via the isotopic ratio. Processing the gamma spectra is identified as a "critical node" in that vulnerability in that area could impact all of the calculated results.

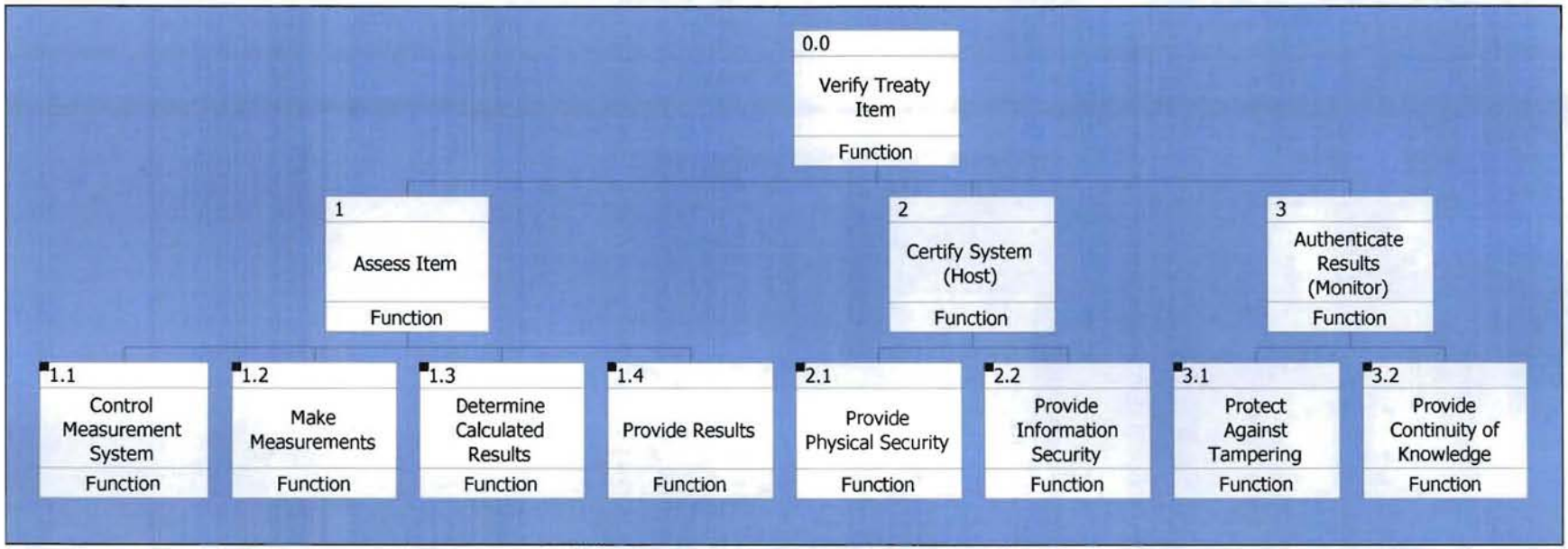

Figure 2. Top-level functional decomposition of the 3G-AMS.

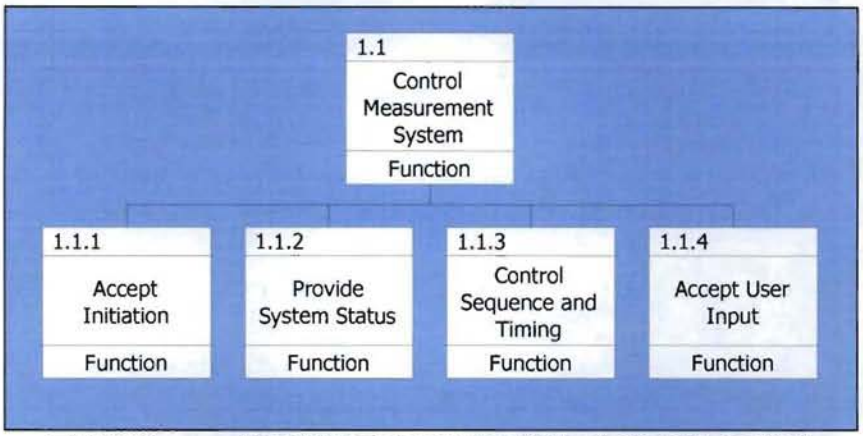

Figure 3. Functional decomposition of system control.

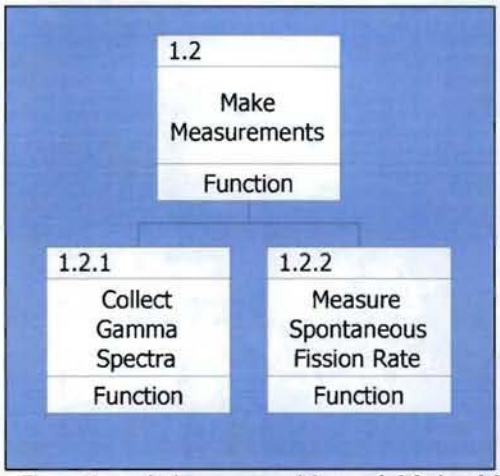

Figure 4. Functional decomposition of *Make Measurements*.

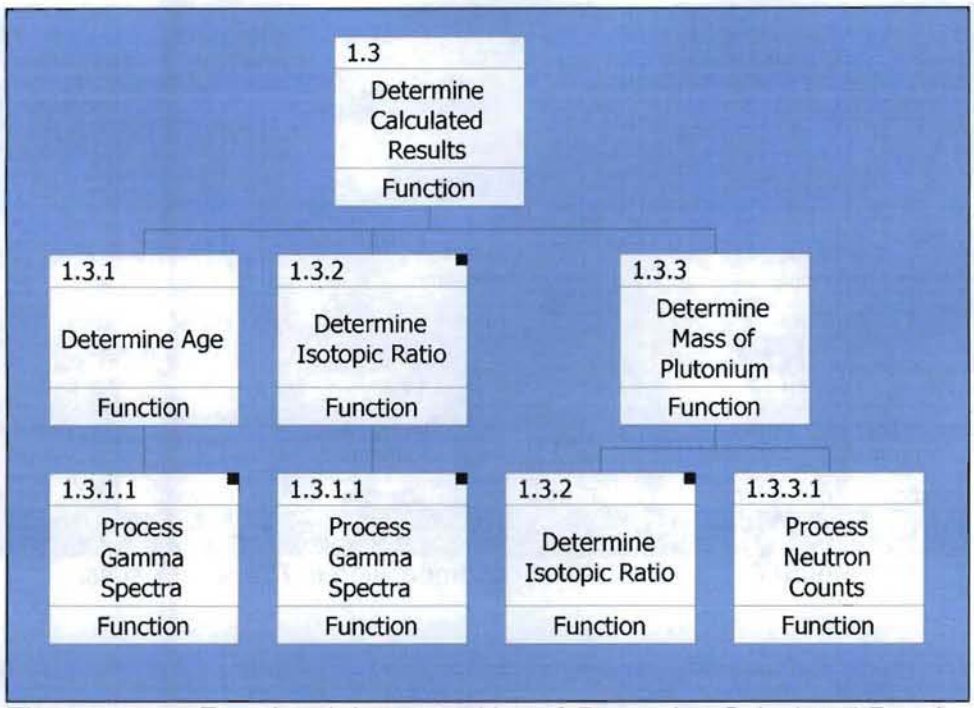

Figure 5. Functional decomposition of *Determine Calculated Results*.

Figure 6 provides the functional decomposition for the *provide results* function. At their lowest level, the functions are to compare each of the calculated results against an agreed-on threshold, with some as-yet undetermined tolerance. The other side of the *provide results* function is to display confirmation (or rejection) of each of the calculated results. This decomposition is an example of how this approach simplifies the complex. Looking at the age metric as an example, when the age comparison is made to the threshold, the data used in that comparison may be sensitive; when the age confirmation is displayed, that display is not. The reason and the mechanism for that difference lies in Figure 7, which shows the functional decomposition for certifying the system. The provision for information security will accept the sensitive data, protect that data, cleanse/desensitize the data, and then transmit the unclassified data for display.

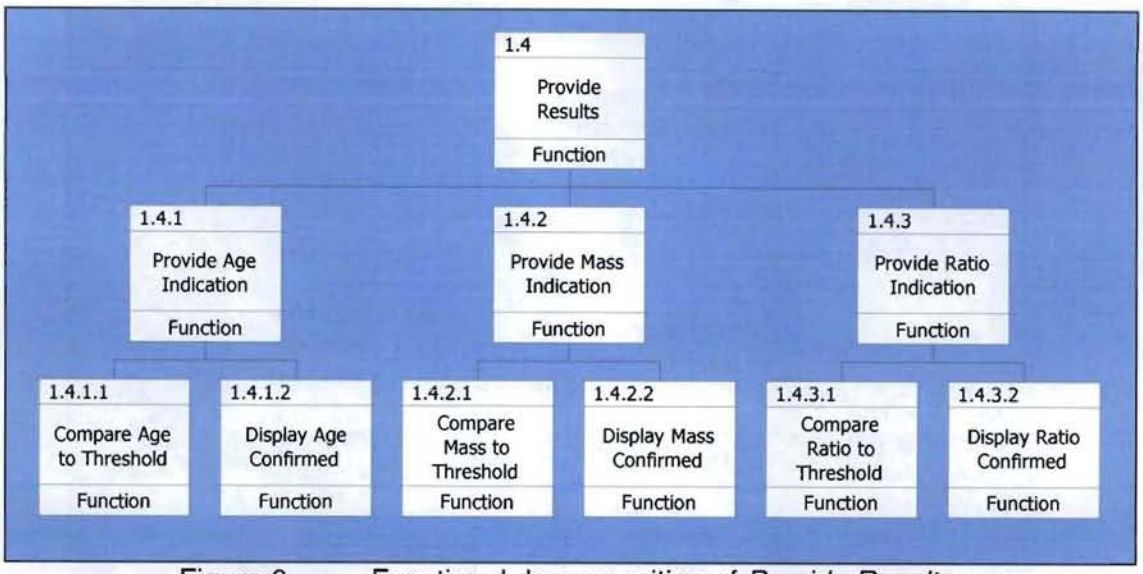

Figure 6. Functional decomposition of *Provide Results*.

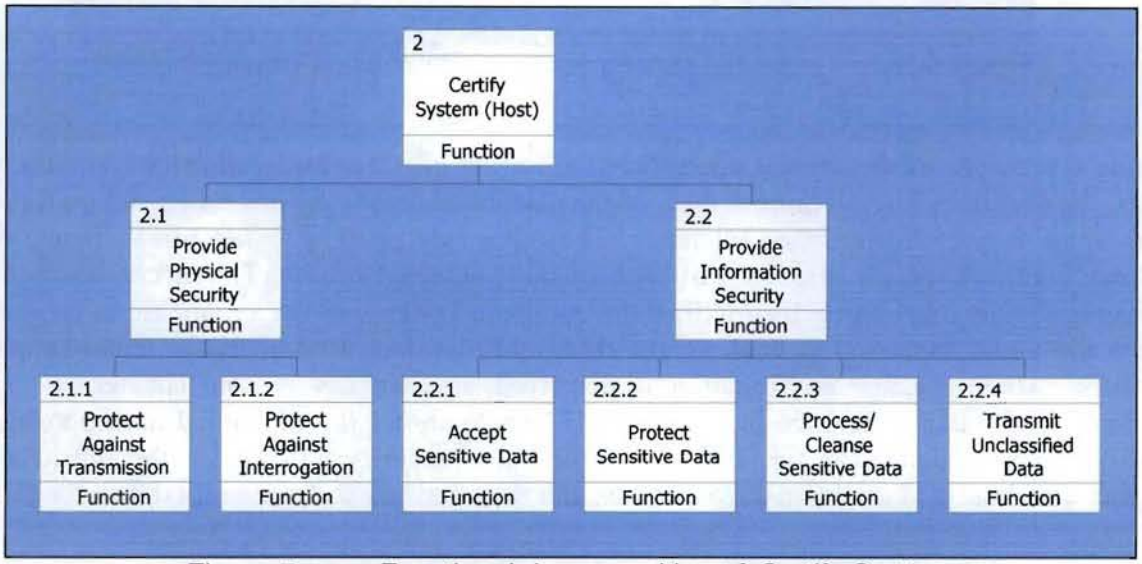

Figure 7. Functional decomposition of *Certify System*.

Figure 8 provides the functional decomposition for the *authenticate results* function. As discussed in previous sections of the text, numerous solutions or combinations of solutions have been proposed to support authentication. However, those solutions fundamentally address one of two functions: *protect against tampering* or *provide CoK*. The function to *protect against tampering* encompasses the ideas of prevent, deter, and detect. It is recognized that absolute confidence in the AMS may not be possible. The objective in authentication is therefore to make tampering with the AMS (i.e., implementing a hidden switch) too complicated, too costly, and/or too likely to be detected to be worth doing. Options for protection against tampering are essentially only two: inspect and test. Inspection has been broken down into pre- and post-measurement because derived requirements differ for the different monitoring regimes. The

cornerstone of authentication by inspection and testing in the absence of an open mode is maintaining CoK by controlling the chain of custody for both the measurement and validation systems.

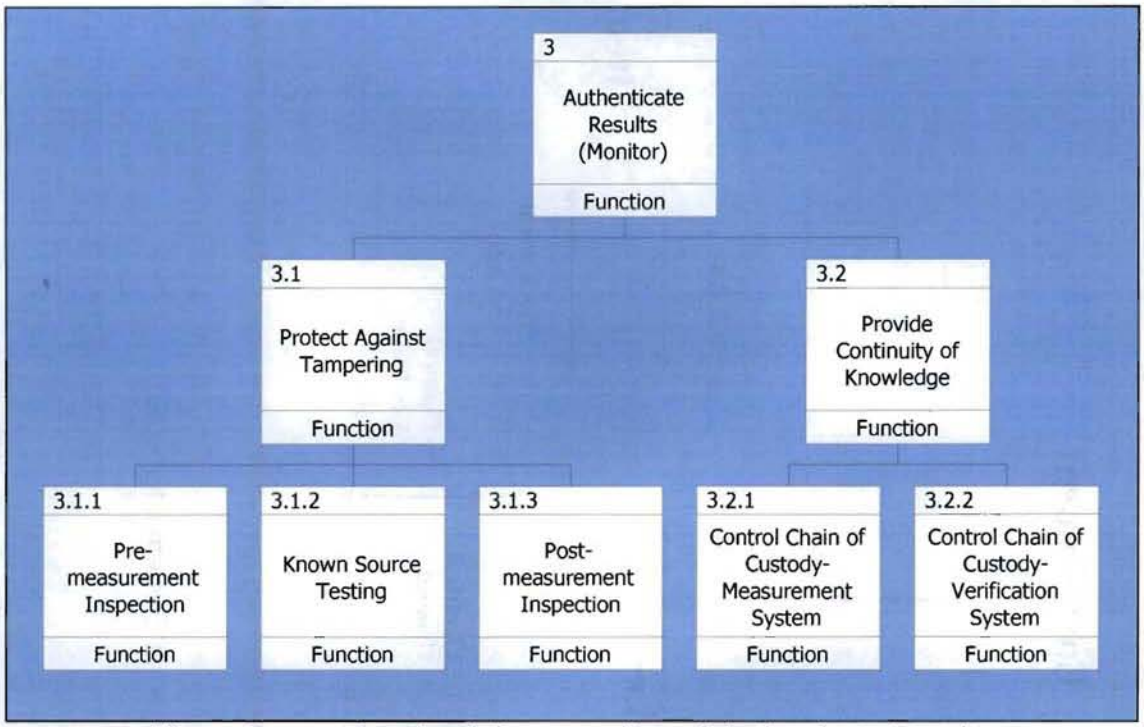

Figure 8. Functional decomposition of *Authenticate Results*.

4.2 Physical Representation

The physical representation of the system begins with defining the system boundary and its interfaces. Figure 9 presents the operational system interfaces of the 3G-AMS. For the system in question, all of the identified interfaces must be carefully controlled for the purposes of either certification or authentication. For the same reasons, pathways that are not required for communication must be strictly precluded. Examples are hidden switches, radiofrequency, and thermal.

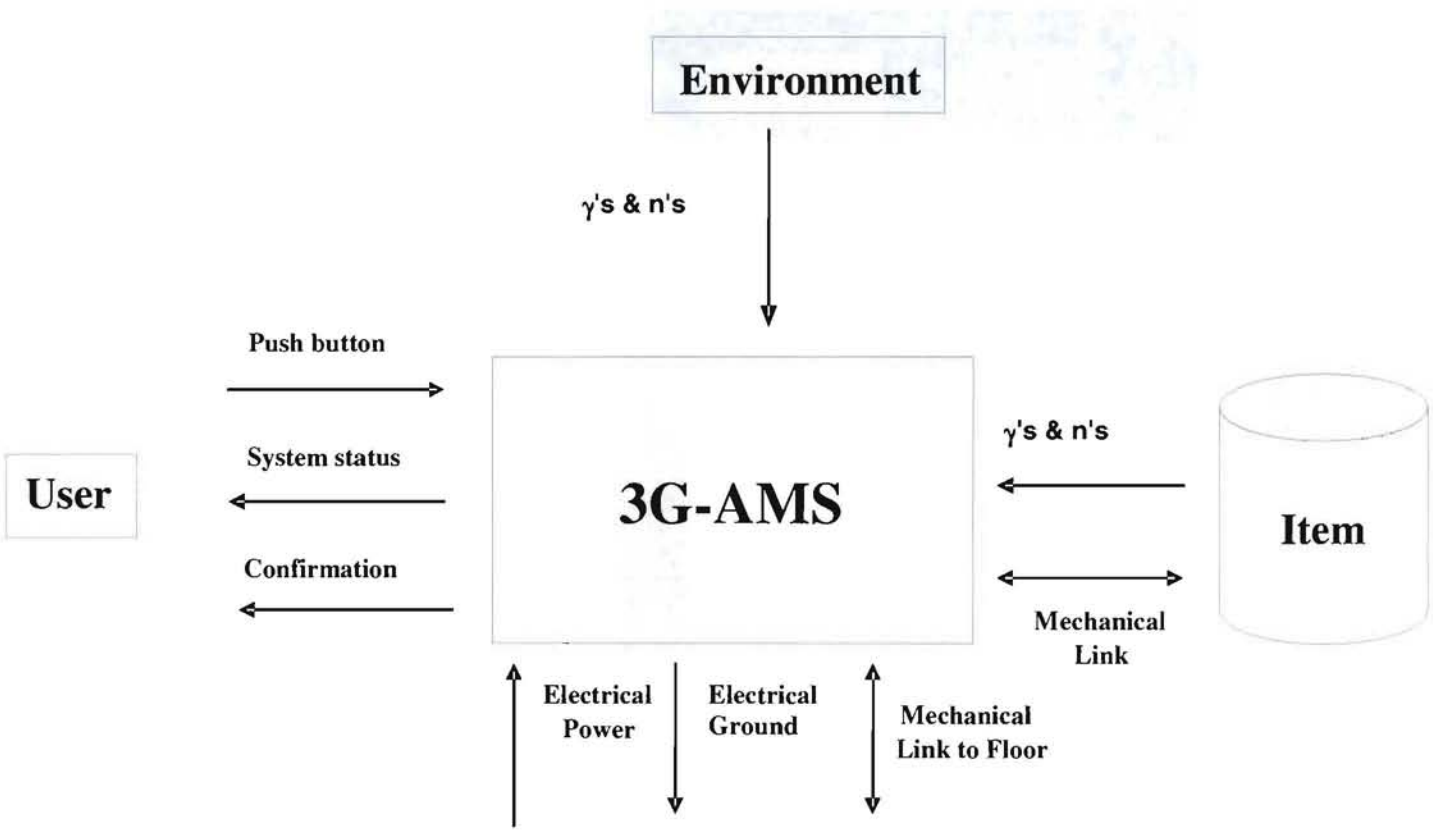

Figure 9. Operational System interfaces.

At this conceptual design stage, the physical description or solution of the system exists at a high level. The detailed system description remains to be developed in ongoing work as requirements are further derived. Figure 10 presents the physical construct of the 3G-AMS system. The 3G-AMS is a collection of hardware, software, procedures, etc., working in concert to make measurements in a given facility using a system that is certified and producing results that are authenticated. The measurement and validation systems are identical physically but will be subject to differing requirements once they are identified. The certification system serves as a placeholder to capture non-device portions of the 3G-AMS that support the function of certification, such as operational procedures. The authentication system encapsulates the processes, protocols, and procedures that support authentication.

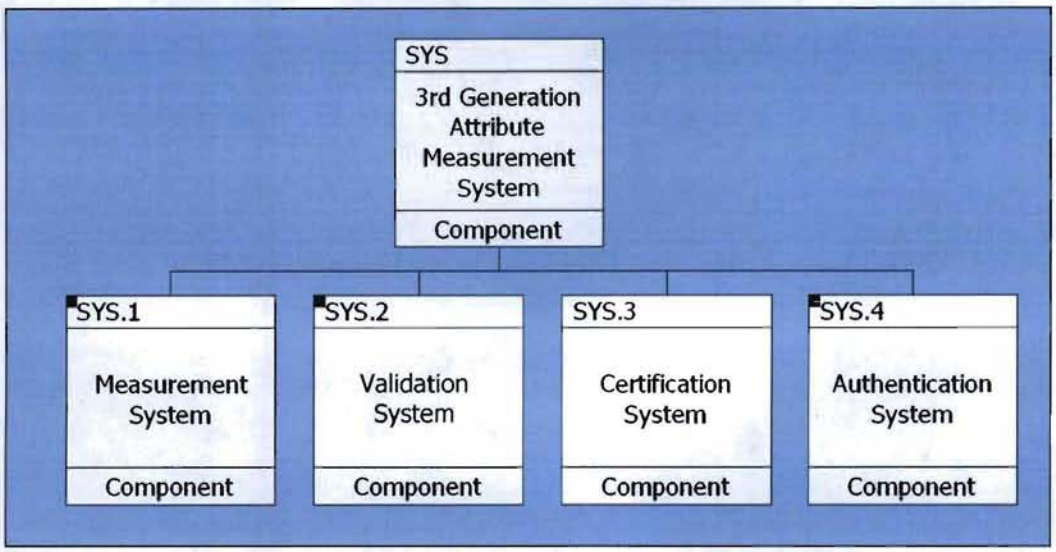

Figure 10. Physical construct of the 3G-AMS.

Figure 11 presents the physical description of the measurement system. The validation system, which is physically identical to the measurement system, will not be shown at this time. The measurement system includes all of the hardware and software associated with the assay system, which makes and processes the gamma, neutron, and time measurements. The measurement system also includes a control system, both hardware and software based, for preventing sensitive information release, while allowing the desired nonsensitive attributes to be displayed. The mechanical and power systems at this time are high-level placeholders for the mechanical and electrical power linkages for physical support and operation. Future efforts in fleshing out the physical description of these systems will delve into the details of the inputs and outputs for each system and its subsystems.

Figure 12 presents a high-level physical construct for the authentication system, showing the role of the various authentication solutions within that system. At the top level, the authentication system comprises the design and acquisition processes, as well as the

operation/test and CoK procedures. Although the authentication system will drive many of the hardware and software requirements of the measurement system, the authentication system itself is almost entirely a person or persons performing a process or procedure. The details of these critical processes will be fleshed out as part of continuing work.

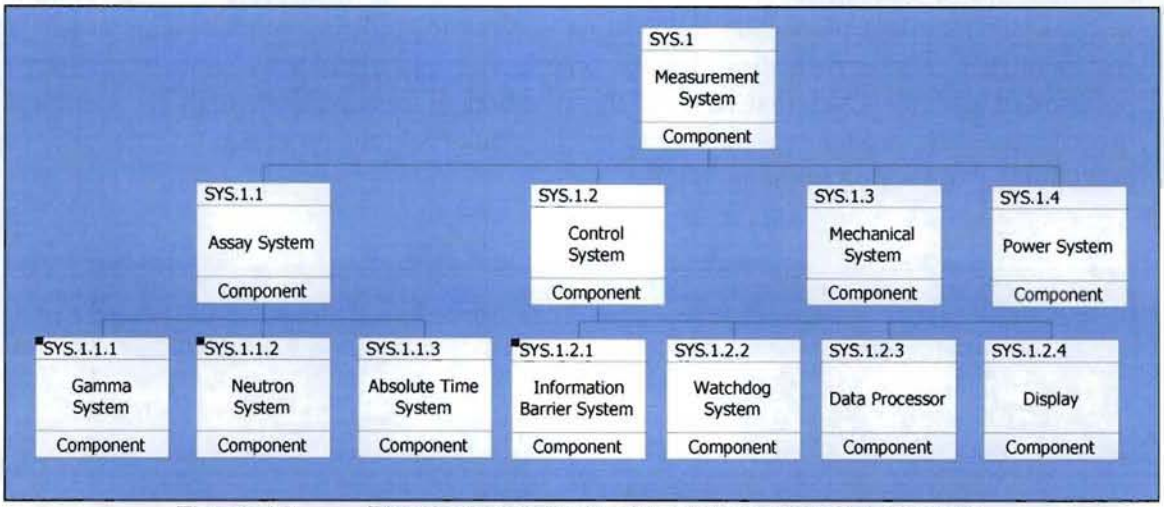

Figure 11. Physical construct of the Measurement System.

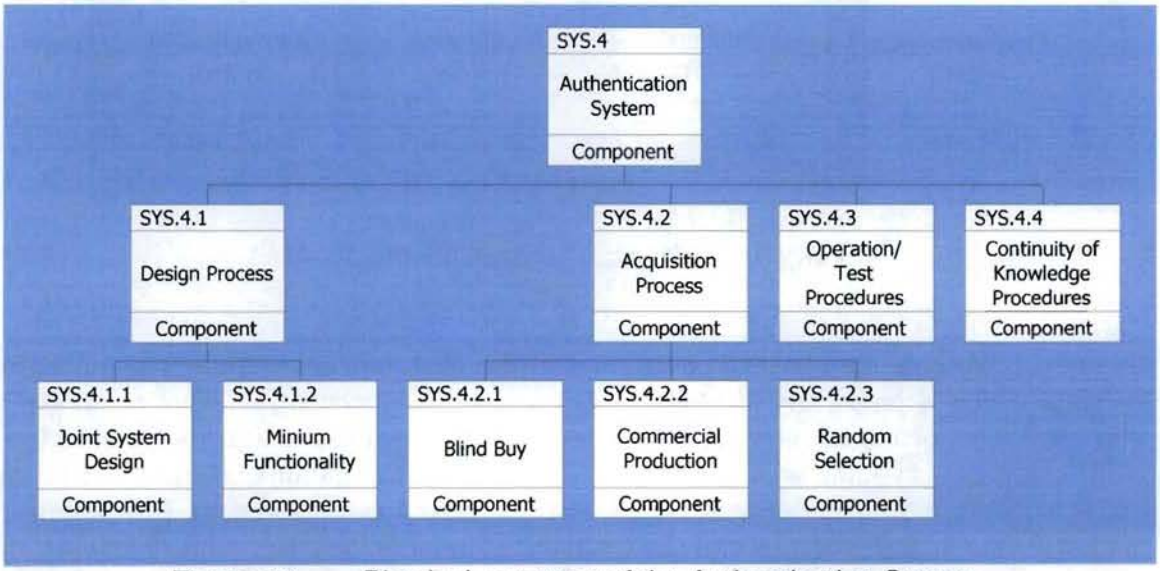

Figure 12. Physical construct of the Authentication System.

4.3 Requirements

Now that we have considered the functional and physical representations of the 3G-AMS, the remaining perspective is to consider the requirements for treaty verification. Figure 13 presents high-level requirements derivation for treaty verification. In this presentation, certification is numbered R.1 to visually designate its priority relative to the

other high-level requirements of authentication and assay confirmation. This is not to say that authentication and assay confirmation are not important, but that when requirements compete, priority will generally be given to certification. Although these requirements currently are sparse, the drivers for cost and size already can be seen. Further development will continue to flesh out requirements and identify associated performance metrics.

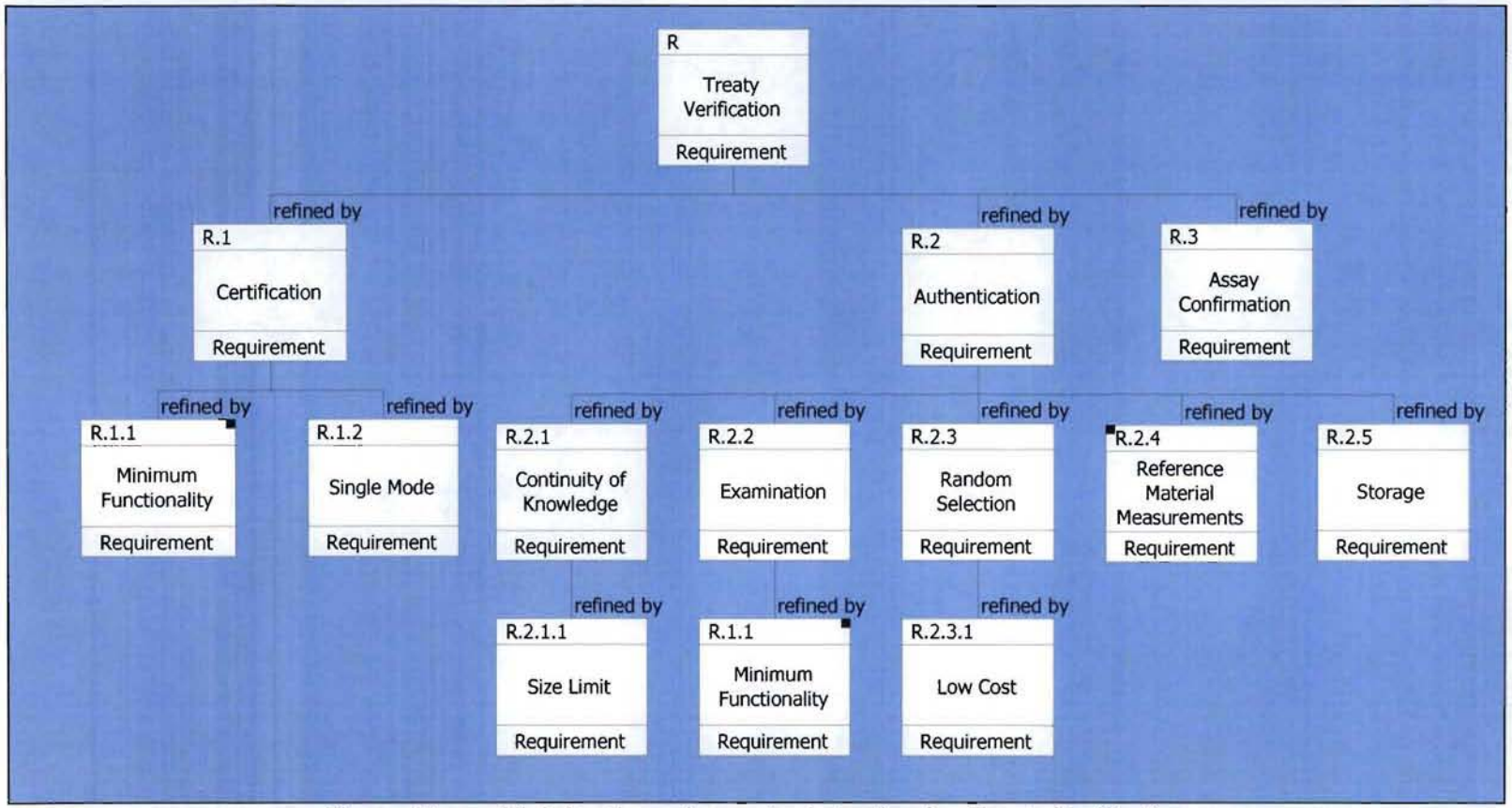

Figure 13. High-level requirements derivation for *Treaty Verification*.

5 CONCLUSIONS

Several of the precursors to the 3G-AMS, in particular the FMTTD system and the AVNG, have been certified to handle sensitive SNM. Thus, the goal of the 3G-AMS design is to improve the authenticatability of the AMS without losing the characteristics that make the system certifiable.

5.1 Authentication

For the 3G-AMS, authentication is achieved primarily by using random selection of the system/parts to be used in the measurement and validation systems. The validation modules are then brought to the monitor's home facilities and examined in detail to ensure that they operate as expected. To have this process make sense, a strict CoK must exist from the time of random selection until the modules get home. The capability to perform a sufficiently detailed examination of the validation modules must also exist.

Another level of authentication comes from using reference radiation sources to determine that the measurement system produces the correct results when measuring them. These sources would be measured in random order, perhaps multiple times, interspersed throughout the measurements of the sensitive items. A reasonable range of sources should be available to exercise the system across its expected range of operation. The sources are nonsensitive and would be measured in detail to ascertain that they are the sources we expect.

Finally, the stockpile of system parts and the reference sources would be stored in a tamper-indicating enclosure between measurement visits. Each would also have a unique identifier that could be checked at various stages of the process.

5.2 Certification

Certifiability in the 3G-AMS is achieved by careful design to avoid potential information leakage paths. Once assembled, the system comprises an enclosing Faraday cage. The integrity and continuity of the Faraday cage connections are monitored by a watchdog circuit that can power off the entire system, thereby flushing all sensitive information, if it detects an error. This process requires that there be no sensitive information stored in writeable, nonvolatile memory and that all other storage loses its contents when power is removed.

The interconnections between the system components would extend the Faraday cage between them with enclosing, conducting connections. The power into the system would be strongly filtered to eliminate any signaling.

The only accepted path of information in and out of the system would be via the lights and the button on the E-Box. These components would be kept to a minimum and would be designed to be unable to rapidly change states. (Rapidly tapping a button could be used to transfer information clandestinely into the IB. Rapidly blinking lights could be used to transfer information out of the IB.)

Additionally, the level of sensitivity of the information in the detector modules would be kept low. Calculations that produce sensitive results would take place only in the E-Box.

5.3 Advantages

The 3G-AMS described above has many advantages over previous AMS implementations. One of the conclusions of the US/UK authentication workshop was the importance of random selection, and the associated CoK issues, in the process of authenticating an AMS. In particular, the difficulties associated with maintaining CoK within a facility completely controlled by a host country, and in transporting AMS components out of the host country, were not fully appreciated. The 3G-AMS will incorporate the following.

Modularity—Although several earlier AMSs were constructed in a modular fashion, several of the modules were too large (e.g., NMCs) or had too many connections (e.g., electronic components) to allow for easy and cost-effective random selection of these components. In contrast, all modules of the 3G-AMS will be designed to be small enough to transport out of the host country (e.g., the NMC will be composed of a number of separate modules) and simple to separate from other modules (much of the complex electronic wiring will be eliminated in the unified electronics module). These changes will increase the monitor's confidence that the module tested in their home country is the same module that was randomly selected in the host's facility.

Low-Cost Construction—The reduction in size and cost of each individual module will allow more frequent random selections. The size will be reduced either by breaking large components into several smaller pieces or by integrating several functions into a single purpose-built module. Cost reductions are achieved by again breaking expensive components into several modules, as well as eliminating unnecessary functionality and cabling between modules.

Reduced reliance on tags and seals—The 3G-AMS will be designed to allow frequent "reauthentication" by random selection as opposed to "authenticating" a large system and then maintaining it, in an authenticated state, within the host's facility between monitoring visits.

In addition, the design of an AMS without an open mode will significantly simplify both the AMS hardware and the procedures for operating the AMS.

6 REFERENCES

1. P. J. Karpius and R. B. Williams, Designing Minimum-Functionality Attribute Measurement Hardware, Los Alamos National Laboratory draft report (October 2009).

2. Morag Smith, Peter Karpius, Jonathan Thron, Richard Williams, Duncan MacArthur, et al., NG-AMS Authentication Working Group Presentations, Los Alamos National Laboratory report LA-UR-09-0996 (2009).

3. Jonathan Thron and Pete Karpius, "Next-Generation Attribute Measurement System Documentation", Los Alamos National Laboratory report LA-UR-08-06492 (2008)

4. John M. Puckett, Diana Langner, Sin-Tao Hsue, Duncan MacArthur, Nancy Jo Nicholas, Rena Whiteson, Thomas B. Gosnell, Zachary Koenig, James Wolford, Massimo Aparo, Juri Kulikov, Julian Whichello, Valery J. Poplavko, Sergei Feodorovitch Razinkov, Dmitriy S.

Semenov, and Vladimir Terekin, "General Technical Requirements and Functional Specifications for an Attribute Measurement System for the Trilateral Initiative," in Proceedings of the INMM 42nd Annual Meeting, Indian Wells, California, July 15–19, 2001.

5. US-UK EIVR 58 Authentication Workshop, Sandia National Laboratories report, March 9–12, 2009.

6. US-UK EIVR-58 Information Barrier Workshop, Los Alamos National Laboratory report LA-UR-07-2183 (April 2007).

7. Trilateral Initiative Demonstration, Los Alamos National Laboratory, June 28–July 2, 1999.

8. "Fissile Material Transparency Technology Demonstration," Los Alamos National Laboratory report LA-UR-00-2239 (2000), http://www.lanl.gov/orgs/n/n1/FMTTD/index_main.htm.

9. Richard Williams, Norman Johansen, Peter Karpius, Duncan MacArthur, and Morag Smith, "Implementation of an Information Barrier for the Next Generation Attribute Measurement System," in Proceedings of the INMM 48th Annual Meeting, Tucson, Arizona, July 8–12, 2007.

10. "Fissile Material Transparency Technology Demonstration," Los Alamos National Laboratory report LA-UR-00-2239 (2000), http://www.lanl.gov/orgs/n/n1/FMTTD/index_main.htm.

11. "Next Generation Attribute Measurement System," in Proceedings of the 49th INMM Annual Meeting (July 2008).

12. "Next Generation Attribute Measurement System," in Proceedings of the 48th INMM Annual Meeting, July 2007.

13. D. Desimone, D. MacArthur, and J. Thron, "Minimum Functionality Attribute Measurement System-Software Implementation," Los Alamos National Laboratory draft report (October 2009).

14. Douglas R. Mayo and Duncan W. MacArthur, "Neutron Measurement Systems: Current Capabilities and Limitations," Los Alamos National Laboratory report LA-UR-08-1358 (March 2008).