PNNL-SA-34871

Authentication of Radiation Measurement Systems for Non-Proliferation

R. T. Kouzes
B. D. Geelhood
R. R. Hansen
W. K. Pitts

July 2001

Prepared for the U.S. Department of Energy under Contract DE-AC06-76RLO 1830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-ACO6-76RL0183O

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

PNNL-SA-34871

Authentication of Radiation Measurement Systems for Non-Proliferation

R. Kouzes
B. D. Geelhood
R. R. Hansen
W. K. Pitts

July 2001

Prepared for
the U.S. Department of Energy
under Contract DE-AC06-76RLO 1830

Pacific Northwest National Laboratory
Richland, Washington 99352

ABSTRACT

Radiation measurement systems are central to the affirmation of compliance with a variety of agreements related to arms-control and non-proliferation. *Authentication* is the process by which the Monitoring Party gains appropriate confidence that the information reported by a monitoring system accurately reflects the true state of the monitored item. Authentication utilizes a set of tools to provide evidence that a system performs its required and defined tasks. These tools include: functional testing using trusted unclassified calibration sources, evaluation of documentation including the software, evaluation of hardware, random selection of hardware and software, and usage of tamper indicating devices. Procedures for carrying out authentication are central to the successful implementation of the complex process of authenticating systems throughout their lifecycle that can be divided into the elements of design, fabrication, installation, and operations. In this paper, we focus on US authentication requirements for bilateral agreements. Radiation measurement systems are now being specified that will be the subject of US authentication activities. We introduce the concept of Authentication Assurance Levels to measure the effectiveness of authentication.

INTRODUCTION

The end of the Cold War has resulted in unprecedented arms control agreements and initiatives between the United States (US) and the former Soviet Union countries to reduce the number of nuclear weapons and to safeguard the dismantled fissile materials. Following the breakup of the Soviet Union, the U.S. Congress enacted the Cooperative Threat Reduction (CTR) Program (originally called the Nunn-Lugar Initiative) to assist former Soviet Union countries in enhancing the safety, security, control, accounting, and centralization of nuclear weapons and fissile materials. The Defense Threat Reduction Agency (DTRA) is charged with administering the objectives of the CTR Program, including the safeguarding of fissile materials via the Fissile Material Control Program.

Bilateral non-proliferation and arms-control agreements and negotiations held between the US and the Russian Federation (RF) are leading to the disposition of nuclear weapons material and the deactivation and decommissioning of production and processing facilities. There is a new population of material being stored that has originated from the nuclear weapons programs, which will place new requirements upon information security and authentication beyond those traditionally considered. The material in question has classified characteristics, which results in measurement data that is classified, and thus requires a barrier to prevent the Monitor from gaining sensitive information. The desirability of this material is greater than material that has been previously placed under international safeguards. The plutonium and highly enriched uranium (HEU) material from these efforts will ultimately be processed into reactor fuel or be buried with highly radioactive waste. The International Atomic Energy Agency (IAEA) is also involved in this effort through trilateral discussions and possibly separate agreements between the US and the IAEA, and the RF and the IAEA. Such agreements involving weapons states generally involve some level of transparency, where a Monitoring Party enters a Host Party facility and confirms that the conditions of the agreement are being satisfied to some level of confidence. Because of the possible classified nature of the information, new constraints are placed upon monitoring measurement systems, and both the Host and the Monitor must work harder to gain a baseline of trust.

The Plutonium Disposition agreement is an example of a bilateral, reciprocal agreement under negotiation between the US and the RF to dispose of 34 tons of weapons grade plutonium originating from weapons or production facilities in each country. Under another agreement, the US has been constructing a Fissile Material Storage Facility (FMSF) at Mayak near the Ural Mountains of Siberia, which is planned to begin operation in 2003. Located at one of the Russian

Federation's former weapons production facilities, the FMSF will store up to 50 tons of RF weapons-origin plutonium, and possibly HEU, for up to 50 years. The US Department of Defense's DTRA/CTR program is overseeing the construction of the FMSF.

A number of radiation measurement systems are under discussion and development for possible use in future confidence building activities or for possible affirmation of compliance with non-proliferation and arms-control regimes. Authentication, vulnerability assessment, certification, and demonstration of operational functionality are all required for a viable measurement system. This paper will discuss the technical basis of authentication from a US perspective applied to bilateral discussions and agreements, and will introduce a new methodology for potentially measuring the effectiveness of authentication.

DEFINITION OF RELATED TERMS

Authentication is the process by which the Monitoring Party gains appropriate confidence that the information reported by a monitoring system accurately reflects the true state of the monitored item. A US joint Department of Energy and Department of Defense Authentication Task Force has developed an unpublished report on procedures and requirements for authentication of systems, from which the above definition, and those that follow, have been extracted [1]. Information in this article is consistent with the deliberations of that task force. The use of "appropriate confidence" in this US definition of authentication implies a weighing of consequences in determining the cost and effort associate with gaining confidence in a specific regime, which will need to be determined on a case-by-case basis. The need for determining the appropriate authentication activity for a regime has motivated the definition of the Authentication Assurance Levels discussed below.

Vulnerability Assessment is the set of procedures, typically used by the Host Party, to identify potential threats to a system and to establish that a system adequately protects classified information. Monitoring Party concerns of system vulnerability are an aspect of authentication. From the Monitor's point-of-view, a vulnerability assessment could involve a review of the authentication process to determine if compliance can be adequately confirmed.

It should be noted that the definitions of terms vary somewhat between various technical communities, which can lead to some confusion. In the US usage, authentication is the activity applied to equipment to assure correct results and data are obtained, while the IAEA typically applies authentication to the verification of data validity and vulnerability assessment to the equipment assurance [2, 3, 4]. In the end, all parties generally share a common interest in the protection of the Host's classified information and in the Monitoring Party's desire for correct results.

Because of a requirement to protect any classified information of the Host Party, many of the measurement systems developed for non-proliferation and arms-control utilize an *Information Barrier* (IB) to prevent the Monitoring Party from observing such classified information. An IB consists of technology and procedures that prevent the release of Host-country classified information to a Monitoring Party during a joint inspection of a sensitive item, while promoting assurance of an accurate assessment of Host country declarations regarding the item [1, 5, 6]. The IB blocks the Monitor from access to any classified information, but allows the Monitor to obtain complete knowledge of the data processing, while converting the classified information into an unclassified result confirming whether the measured material conforms to the Host's declaration to meet pre-agreed criteria. Authentication carefully explores that data processing by involving a combination of detailed examination of systems and documentation, functional testing, and analysis of the security function for systems. Authentication may be applied independently of whether or not a system incorporates an IB. The presence of an IB complicates the process of building trust.

Information barrier protected systems may operate in *open* and in *secure* modes, where open mode provides access to details of unclassified data for the purpose of functional and other testing, while secure mode is used with classified data, and provides only simple pass/fail/error types of output information.

Certification includes all processes required for the Host to allow operation of a system within its facility. Certification includes the process by which a Host Party assures itself that a monitoring system (which may have an integrated IB) will not divulge any sensitive information about a monitored item to a Monitoring Party. We include here the RF attestation process as part of certification.

When measuring classified items, the information extracted and presented is necessarily limited. Measurement systems can be categorized as *attribute measurement* systems or as *templating* systems. An *attribute* is a specific physics related quantity, such as the ratio of two isotopes as determined from a gamma ray spectrum. The system that makes a measurement and analyzes the data to produce an attribute value must include physics knowledge of the observation. On the other hand, a templating system can be implemented to make a comparison of measurements, such as parts of gamma ray spectra, between an unknown item and a known item. The templating system may just state that the two items are similar without any physics based analysis of the data. Attribute measurement systems are typically specific instantiations of radiation measurement systems that are being developed in the US and the RF for possible use in future verification or confidence building activities.

There are two basic requirements of an attribute or template measurement system: protection of classified information during and after measurements, and credible performance of the system for the measurement. Part of a solution for the requirement to protect the Host Party's classified information leads to the concept of "*Host-supply*." Under the Host-supply scenario, the Host Party would supply the system to be used by the Monitor in a Host facility in order to provide paramount protection for any Host classified information. Host-supply means that the Host has last private access to a system prior to use, whether it is built by the Host party, the Monitoring Party, or a third party [5,6]. The crucial authentication issues for the Monitor then are that a measurement system correctly measures the agreed upon attributes or template, and that there be no hidden features in the system to pass erroneous information.

A demonstration, the Fissile Material Transparency Technology Demonstration at Los Alamos National Laboratory, was conducted by the US in August 2000, of an information barrier protected attribute measurement system to show the ability to make the type of measurements required for non-proliferation without compromising classified information [7].

AUTHENTICATION FOR FMSF

Authentication is specific to each regime where it is applied. Here we consider the specific application of US authentication under the bilateral agreement for transparency at the Mayak FMSF [8]. Preliminary discussions have been held with the RF regarding cooperative development of attribute measurement systems that could be used to implement monitoring requirements currently under discussion for the FMSF. These measures would provide the US with an appropriate level of confidence that the material designated for storage at the FMSF is from dismantled nuclear weapons, is safely and securely stored, and is not reused for weapons purposes. Work related to the FMSF is being supported by the DTRA/CTR at several of the Department of Energy National Laboratories. Pacific Northwest National Laboratory has the lead for authentication of systems for the FMSF under the DTRA sponsored project.

The FMSF will satisfy the need for long-term storage of plutonium, and possibly HEU, in the Russian Federation. Plutonium is planned to be stored at the FMSF as two 2-kg metal spheres in

barrels (AT400R) that will be stacked four high in nests. As currently planned, a nest could hold up to 8 barrels, four with plutonium, and four that could possibly contain HEU. Radiation measurement systems are being considered for use at the FMSF to implement the monitoring requirements that are currently under discussion. These measurement systems would be assembled by the RF (i.e., Host-supply) to measure agreed upon attributes. It is planned that the PNNL led authentication team will authenticate the initial operation of these attribute measurement systems.

AUTHENTICATION ASSURANCE LEVELS

One of the important topics of discussion for a transparency regime is how much authentication activity is sufficient to provide the appropriate amount of confidence for the Monitoring Party. This need for determining the appropriate level of authentication activity has motivated the definition of the Authentication Assurance Levels to provide a means to measure the degree of confidence gained from a collection of activities.

The information technology community has defined a standard called the Common Criteria [9], which defines a set of "Evaluation Assurance Levels" (EALs) that are a set of criteria for evaluation of information technology security. The EAL concept can be extended to define levels of authentication, and the associate procedures to reach these levels, with regard to a Target of Evaluation (TOE), which in this case is a radiation measurement system. Evaluation has been the traditional means of gaining assurance, and is the basis of the Common Criteria approach. Evaluation techniques can include, but are not limited to:

- analysis and checking of process(es) and procedure(s);
- checking that process(es) and procedure(s) are being applied;
- analysis of the correspondence between TOE design representations;
- analysis of the TOE design representation against the requirements;
- verification of proofs;
- analysis of guidance documents;
- analysis of functional tests developed and the results provided;
- independent functional testing;
- analysis for vulnerabilities (including flaw hypothesis);
- penetration testing.

The Evaluation Assurance Levels provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. There are seven hierarchically ordered EALs:

- EAL1 - functionally tested
- EAL2 - structurally tested
- EAL3 - methodically tested and checked
- EAL4 - methodically designed, tested and reviewed
- EAL5 – semi-formally designed and tested
- EAL6 – semi-formally verified design and tested
- EAL7 - formally verified design and tested

EAL1 is the entry level, summarized as a simple performance test. Up to EAL4 increasing rigor and detail are introduced, but without introducing significantly specialized security-engineering techniques. EAL1-4 can generally be retrofitted to pre-existing products and systems.

PNNL has developed a definition of Authentication Assurance Levels (AALs) based upon the Evaluation Assurance Level concept [10]. The definition of AALs will allow for quantizing the level of authentication reached for a given system and allow decisions to be made about tradeoffs of authentication procedures and the desired level of authentication. The IAEA has also prepared an evaluation standard based upon the Common Criteria, and has defined the analogous Vulnerability Assessment Levels (VALs) [11].

The AALs as defined range in value from 0-4, with 4 being the level that provides the most confidence that a system meets its security objectives.

To obtain a high level of authentication assurance, the authenticating authority must identify all required assurance components prior to the development of a system to be authenticated and provide them to the developer to assist in designing the necessary authentication features into the system. If developers are to produce systems that are expected to be authenticated at Authentication Assurance Level 4 or higher, significant improvements in automated system development practice will be required. System development life cycle and quality standards similar to Integrated for Systems Engineering/Software Engineering/Integrated Product and Process Development, ISO12207, and ISO15288 should be adopted or developed at the national level.

The Authentication Assurance Levels provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. They are hierarchically ordered inasmuch as each higher AAL represents more assurance than all lower AALs. The increase in assurance from AAL to AAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigor, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements). Each AAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

The five defined Authentication Assurance Levels and their correspondence to the EALs are as follows:

• AAL0 (unauthenticated)	~EAL1 & EAL2 functionally and structurally tested
• AAL1 (minimally authenticated)	~EAL 3 methodically tested and checked
• AAL2 (limited authentication)	~EAL 4 methodically designed, tested and reviewed
• AAL3 (critical authentication)	~EAL 5 semi-formally designed and tested
• AAL4 (optimal authentication)	~EAL 6 verified design and tested

For example, consider what AAL2 means. AAL2 (limited authentication) is applicable in those circumstances where developers or users require a moderate level of independently assured security and are prepared to incur additional security-specific engineering costs. AAL2 requires the co-operation of the developer in terms of the delivery of design information and test results. AAL2 requires additional components from each of the Security Assurance Requirement classes except guidance documents. Authentication analysis is supported by the low-level design of the modules of the TOA, covert channel analysis and a subset of implementation of the TOA Security Functions. Development controls are supported by a life-cycle model, identification of tools, and partially automated configuration management.

The AALs give a standard against which a specific authentication regimen can be measured, and provide a basis for the comparison of activities to help determine the appropriate level of authentication required for a monitoring system in a specific regime. PNNL is applying this AAL ranking approach to authentication efforts for the FMSF.

AUTHENTICATION BASICS

A monitoring system must be designed from the start to facilitate the authentication process. Thus, the design task becomes much more difficult than merely designing a functional system. An information barrier, if present, further complicates the authentication process. Designing for authentication is especially important in a resource-limited regime, where the potential gain from an expedient design decision must be balanced against the cost of the additional authentication effort it may produce. The authentication process involves searching for both inadvertent design or implementation flaws leading to incorrect results, and deliberate covert features designed into the

system for some advantage (often called a "hidden switch"). It is important to realize that authentication goes well beyond functional testing, since such testing will not necessarily reveal a hidden switch. The authentication effort can be viewed as gaining a detailed step-by-step knowledge regarding all the data processing occurring within the automated measurement system. Emphasis is placed on complete documentation as a means of reducing the cost associated with reverse engineering the system to acquire knowledge regarding all the data processing.

Authentication can be described by a set of high-level guidelines. The basic tenets of authentication are that systems: 1) are designed for correct operation; 2) are assembled as designed; 3) function as designed; and 4) do not contain hidden features that allow the passing of material inconsistent with accepted declaration. Authentication of systems by a Monitoring Party involves a collection of tools and methods and is operationally realized through:

- The measurement of unclassified radiation reference sources,
- Complete documentation for all hardware and software,
- Surveillance plus tamper indicating devices placed on system components and enclosures,
- Random selection of system hardware and software modules for examination, and
- Thorough private testing of duplicate systems and components in Monitoring Party facilities.

Authentication can be facilitated by following a set of reasonable, basic guidelines when a system is being specified and designed. These include:

- Documentation should be complete for all aspects of system hardware and software.
- Hardware components should be simple and without extraneous functionality.
- Hardware components should be laid out for easy physical examination.
- Physical enclosures and shielding should provide a two-way information barrier to prevent both disclosure of information and remote control signals.
- Identical and modular hardware components should be used across a system.
- Hardware and software components should be selected on the basis of availability and shareability of complete documentation.
- Operating systems should be minimal or non-existent.
- Software should be transparent and well documented.
- Software should be simple, concise, and without extraneous functionality.
- Unused hardware should be rendered inoperable.

System components should be the most basic possible for the measurement task, containing only the required functionality. Since the cost and difficulty of Authentication rises with included functionality and the interaction between system components, extraneous functionality is extremely expensive.

LIFECYCLE OF A MEASUREMENT SYSTEM

Procedures for carrying out authentication are central to the successful implementation of the complex process of authenticating systems. The procedures must allow for the varying requirements of authentication throughout the lifecycle of a system, which can be divided into the following elements with respect to authentication.

- Design – It is essential that systems be designed with the requirements of authentication in mind. Authentication requirements will significantly impact hardware and software design criteria and may impact the overall cost. The need for a complete understanding of the system functionality has the most impact on authentication costs because components that are not fully documented must be reverse engineered or otherwise shown to contain no covert features. Thus, components must be selected based on factors such as completeness of documentation and ease of examination. In some cases, non-optimized performance may have to be accepted to meet the programmatic authentication goals. For example, an older generation of processor might be preferred for simplicity over a newer, more powerful one with a wide array of unnecessary features. Hardware and software design criteria and procurement decisions can greatly influence

the available options and costs for authentication. Thus, the authentication and design teams should work together during the design phase. The quality of the overall design must be judged in terms of facilitating authentication and being robust behind an information barrier. Facility design and facility monitoring system design decisions can likewise impact the ability to authenticate systems.

- Fabrication – Authentication of a system requires that the procurement, fabrication, assembly, and testing proceed in a manner that has been agreed to by all parties. Authentication activities during fabrication may include monitoring the actual fabrication practices on-site, review of documentation for compliance, sub-assembly testing, or random destructive or non-destructive testing of components, and an exhaustive review of all software (source code, compiled/executable, and embedded). It may be necessary to transport a system to a Host facility after the system has been authenticated. In this case, the equipment might be sealed, stored, and subsequently transported in a mutually agreeable manner for installation at the Host facility in order to maintain continuity-of-knowledge of the security of the system.
- Installation – Installation for systems requiring authentication must be documented by detailed installation and test procedures. Appropriate physical control or oversight must be maintained of the system during this phase, unless authentication occurs after installation. For example, installation activities will likely be observed by the Monitoring Party to include equipment installation, software installation, calibration, and testing. Functional testing will be performed as part of the acceptance testing process for a system during the installation phase. Functional testing is limited to determining if the system is improperly designed, erroneously fabricated, or broken. Functional testing cannot reveal a selectively triggered hidden feature. Limited resources preclude exhaustive functional testing and an exploratory search for a covert feature.
- Operations – Once a facility becomes operational, access may be limited for the Monitoring Party. Some systems may only be used intermittently; in this case, periodic re-authentication prior to each use may be required. For example, the Monitor must be assured that any software controlling the system has not been swapped between monitoring visits. Other systems may be in continuous use and re-authentication would by necessity be accomplished by means that do not hinder operations. Whether systems operate in Monitor attended or unattended mode will also impact what authentication measures are required. For any complex system some amount of maintenance, upgrade and repair is expected. Re-authentication may be required following such events. Procedures will be required to assure that equipment (e.g., systems, spares, and sources) left in a stored condition between Monitoring Party on-site visits, has remained in a protected state. If the equipment has not remained in a protected state, some level of re-authentication will be required.

APPROACHES TO AUTHENTICATION

Some authentication activities will be common across the lifecycle elements discussed above, while others will be unique to one aspect of the lifecycle. The outcome of authentication is a level of confidence that accurate and reliable information is provided to the Monitoring Party, and that irregularities are detected. The Monitoring Party requires the ability to authenticate the correct operation of a system under a variety of conditions spanning a range of operational and off-normal scenarios. Authentication utilizes a set of tools and approaches to provide evidence that a system performs its required tasks, including the following:

- Functional Testing Using Trusted Unclassified Calibration Sources – Radiation sources, including sources similar to the stored items, play an important role in verifying the correct functioning of an information barrier protected system. The Monitor will independently validate these unclassified radiation sources on a separate system where access to the raw data can occur. Artificial sources of data, such as a recorded pulse train from a similar system or a mathematical model of the system, can be a valuable cross-reference means of validating physical sources and of functionally testing a system over a broader range of source values. An additional feature of an artificial data source is that it may, in principle, be used to transfer a calibration point between identical measurement systems.

- Evaluation of Data – The quality of the data provided by an automated measurement system must be validated. Depending upon the complexity of the system this may be a simple task or this could be a very time consuming and difficult task. The Monitor will gain considerable confidence in an information barrier protected system by confirming the correctness of the numeric measurement results. During open-mode testing, the level of confidence increases with the amount of Monitor access to the data (e.g., ability to remove raw data on media, ability to examine raw data on the system, ability to view intermediate results, and ability to view numeric results and error estimates). Private measurements with a duplicate system where the Monitor can gain complete access to data from sources provide the most confidence in data quality. The validation of the data displayed, stored, or removed is possibly semi-independent of the authentication of the software and hardware that has been used, since it may also depend on the data source (e.g., radiation source or video picture). Data must be protected from tampering throughout its lifecycle.
- Evaluation of Documentation – Examination of hardware, software, operations and maintenance documentation, and a comparison to the as-built system can be an important authentication tool. Examination of documentation can also help define sensitive design points for targeted authentication efforts.
- Evaluation of Software – Software exists at several levels in systems (e.g., firmware, embedded software, operating systems, acquisition software, and analysis software). A detailed examination of all software, including source code, is central to authentication. A necessary component of the software evaluation is rebuilding a duplicate executable code from the provided source codes using the same compilers, build instructions, and associated software tools originally used to produce the executable code. In addition, all the software and firmware installed in the system must be shown identical to the examined and rebuilt code. Without proven equivalency of source code and installed executable code, detailed examination does not create assurance. A means for determining changes in the agreed upon software should be incorporated in the design and examination procedures. All software must be available in machine-readable source code form, and be fully documented. An alternate means of precluding tampering with commercial software that has a significant mass market might be independently obtaining a duplicate copy through an anonymous buy and comparing it to resident code.
- Evaluation of Hardware – A variety of hardware makes up a system (e.g. detectors, computers, power supplies, data acquisition boards, etc.). An examination of these components is central to authentication. The ability to photograph components down to board level during on-site monitoring visits provides assurance that the system remains unmodified. Comparisons of these photographs to those in the documentation and those of the duplicate system build assurance. Visual examination and comparison of the hardware on-site is valuable, but not as effective as photography. Private examination of hardware in the duplicate system is a very powerful confidence builder. Signals can be traced and measurements made on the duplicate system that are not possible during a brief period of joint examination prior to use. However, authentication is facilitated by the ability to make some electrical measurements during joint examination.
- Random Selection of Hardware and Software – Random selection of hardware and software components or complete systems is a powerful authentication tool. Any party attempting to subvert any particular module must do so with the knowledge that the Monitor will potentially be carefully examining a randomly selected module during private inspection at a Monitor's facility. Random selection consumes spare modules and requires a sufficient initial procurement. Random selection will be one of the tools used during on-site authentication efforts. Several random-selection schemes are possible. A large number of duplicate components or systems can be procured or built. The Monitoring Party can then select from these components or systems for use during equipment assembly or operation. At the same time the Monitoring Party can also select specific components or systems to be shipped off-site for further private examination. Any remaining components or systems would be placed in secure storage for use in future random selection schemes. At installation, a random selection scheme could select a complete system to be installed in the facility and a duplicate complete system for private examination. During subsequent monitoring visits, the Monitor could select a module for replacement under a random

selection scheme where the Monitor selects one module from storage as the replacement and another for private examination. A variation would allow the Monitor to privately examine the replaced module when appropriate. Random selection can be used on less expensive individual software-bearing-components prior to each use to confirm the controlling software in the system is unchanged. If a system repair is required, a replacement could be randomly selected by the Monitor from the spares pool, and another for private examination.

- Usage of Tamper Indicating Devices – Tags, seals, and other tamper indicating devices (TIDs) are important verifications of the physical integrity of systems. TIDs provide some assurance of continuity-of-knowledge of a system and its components, which means trace-ability through time of the secure state of the system. TIDs are of great importance for equipment that operates in an unattended mode, i.e., when the Monitoring Party is not present. Unique TIDs can be a useful means of identifying components subject to a random selection scheme and a means of ensuring that modules or software-bearing-components have not been swapped out.
- Usage of Surveillance – To increase the level-of-confidence that systems are not modified or altered by the Host Party, surveillance systems are routinely used to augment the protection that TIDs provide. Defeating an enclosure sealed with a TID that is viewed by a video surveillance system, for example, requires the generation and simultaneous application of two separate tampering strategies.
- Usage of Procedures – Documented procedures must be provided for all aspects of authentication and for any other on-site activities that affect the reliability of a system to provide accurate information. Formal procedures, for example, clarify the respective roles of the Host and Monitor Parties during random selection.

AUTHENTICATION OF EXAMPLE RADIATION MEASUREMENT EQUIPMENT

Fig. 1 shows a generic radiation measurement layout as an example of the type of attribute measurement system being considered for use to confirm compliance with nonproliferation agreements. This generic system consists of a high purity germanium detector (HPGe) for gamma ray measurements plus a neutron detector system. The HPGe could potentially determine such attributes as the presence of plutonium or highly enriched uranium, the isotopic ratio of ^{240}Pu to ^{239}Pu or uranium enrichment, and the presence of plutonium metal (absence of oxide or other compounds). The neutron detector system may range in complexity from a single neutron detector, a neutron coincidence counter, or a Neutron Multiplicity Counter (NMC). An NMC consists of dozens of ^{3}He detectors in a large moderating enclosure capable of measuring several parameters about the observed item when combined with the HPGe results. These parameters could include mass of plutonium, neutron production from impurities and the matrix material, and neutron multiplication.

An item of material to be measured will be enclosed in a container that is placed near the detectors. The data are collected with a simple data acquisition system that in this example includes an Information Barrier (IB). The IB is a physical and logical barrier that protects the Host's classified information from disclosure to the Monitor. The IB includes procedures as well as hardware and software. The IB is also designed to prevent the input of an external signal into the measurement system, reducing the likelihood that a hidden switch may be successfully used to subvert the measurement system. The presence of the IB means that Monitors will not be able to observe the actual data from the detector system when it is measuring a sensitive item. Instead, only pass or fail lights will indicate that the system has passed or failed the observed item with respect to the negotiated attributes for the material. There may also be error indicators. The IB would include a security watchdog to shut down the system and purge all data if a problem arises such as opening of the system when a sensitive item is present. The presence of the IB, and the resulting lack of detailed information about the data collected, increases the requirement for system authentication, and adds substantially to the problems of building a robust radiation measurement system.

PNNL has established an Authentication Laboratory for the testing of radiation measurement systems with large quantities of plutonium oxide in a dedicated laboratory at the Plutonium Finishing Plant located at the Hanford site in Washington State. This facility is designed for measurements required to clarify physics issues related to attributes [12], and testing analysis and measurement equipment such as that which may be used at the FMSF. Such testing of equipment is required for developing the methods and procedures that will be used for on-site authentication of any Russian Federation developed instruments, should that be negotiated. In addition, if equipment is brought back to the US following random selection at a Russian Federation facility, the Authentication Laboratory will be available for detailed examination for authentication of the Host supplied equipment.

The initial authentication of a monitoring system would take place during installation and acceptance at a facility. Assemblies would be sealed with tamper indicating devices. Photographic records could be produced. Random selection of components and/or systems would also be made at this time. Some items randomly selected could be shipped back to the US for detailed examination. Functional testing with radiation sources and electronic signals could be performed to exercise the system attributes. Once a system was authenticated, some means would be used to provide confidence regarding the security of the system between US Monitor visits. When a US Monitor arrives during a scheduled visit of the facility, the system would possibly undergo some routine authentication activities to assure that the system was still operating reliably.

It is proposed that there would be such information barrier protected radiation measurement systems produced by the RF for use by US Monitors at the FMSF. Such systems might be used to measure a statistically determined sample of containers from the FMSF.

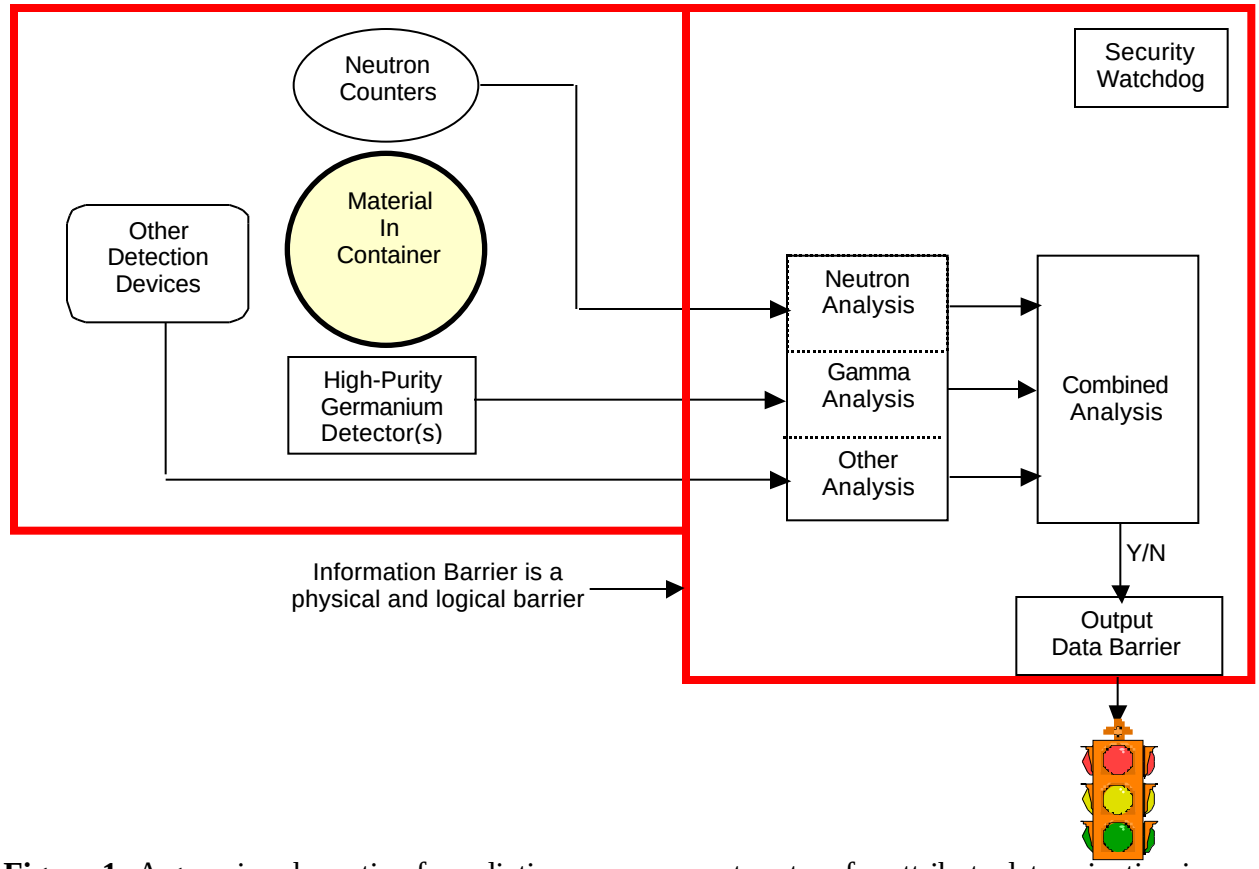

Figure 1: A generic schematic of a radiation measurement system for attribute determination in an arms-control application. The information barrier includes both procedures and technology to prevent the release of Host Party sensitive information.

SUMMARY

Authentication is a necessary aspect of the implementation of systems for the assurance of compliance with non-proliferation and arms-control agreements. It is a necessary component of a regime in which measurements must be made on classified or sensitive items and materials. A consistent basis for this authentication activity has been developed by the United States technical community applied to bilateral activity. Efforts to apply authentication to radiation measurement systems are now being implemented.

ACKNOWLEDGEMENTS

This work was supported by the U.S. Defense Threat Reduction Agency and by the U.S. Department of Energy. Pacific Northwest National Laboratory is operated for the U.S. Department of Energy by Battelle under contract DE-AC06-76RLO 1830. The joint DOE-DoD Authentication Task Force has discussed and evaluated the issues presented here. This paper was presented at the IEEE Nuclear Science Symposium, San Diego, CA, November 2001.

REFERENCES

[1] R. Kouzes, L. Bratcher, T. Gosnell, D. Langner, D. MacArthur, J. Mihalczo, C. Pura, A. Riedy, P. Rexroth, J. Spingarn, and M. Scott, "Authentication Procedures," presented at the INMM Annual Meeting, Indian Wells, CA, July 2001.

[2] J.C. Andress, "The Assurance of Genuineness," presented at the 17th European Safeguards Research and Development Association (ESARDA) Annual Symposium on Safeguards and Nuclear Material Management, Aachen, Germany, May 9-11, 1995.

[3] C. R. Hatcher, S.T. Hsue, and P. A. Russo, "Authentication Of Nuclear Material Assays Made With In-Plant Instruments," IAEA-SM-260/103, presented at the International Symposium on Recent Advances in Nuclear Material Safeguards, Vienna, Austria, November 8-12, 1982.

[4] "Procedure for the Authorization of Equipment Systems and Instruments Software for Inspection Use," Department of Safeguards, IAEA, Vienna, Austria, February 2001.

[5] Joint DoD/DOE Information Barrier Working Group, "Functional Requirements and Design Basis for Information Barriers," Pacific Northwest National Laboratory, Richland, WA, Rep. PNNL-13285, May 1999.

[6] J. L. Fuller, "Information Barriers," Pacific Northwest National Laboratory, Richland, WA, Rep. PNNL-SA-33328, June 2000.

[7] Fissile Material Transparency Technology Demonstration at LANL, (2000, August) [Online] Available: http://www-safeguards.lanl.gov/FMTT/index_main.htm.

[8] B. Geelhood, R. Kouzes, W. K. Pitts, "Design Guidelines for Authenticable Systems," Pacific Northwest National Laboratory, Richland, WA, Rep. PNNL-13386, November 2000.

[9] "The Common Criteria for Information Technology Security Evaluation," ISO 15408/1999, 1999.

[10] R.T. Kouzes, J.R. Cash, D.M. DeVaney, B.D. Geelhood, R.R. Hansen, R.B. Melton, "Authentication Assurance Levels: A Strategy for Applying the ISO Common Criteria Standards," Pacific Northwest National Laboratory, Richland, WA, Rep. PNNL-13587, July 2001.

[11] M. DeVaney, R. Hansen, R. Kouzes, R. Melton, "A Review Of The IAEA Vulnerability Assessment Level Scheme: Applicability To DTRA and DOE Programs in the FSU," Pacific Northwest National Laboratory, Richland, WA, Rep. PNNL-13743, December 2001.

[12] A. Peurrung, R. Arthur, B. Geelhood, R. Scheele, R. Elovich, S. Pratt, R. Kouzes, "The 871-Kev Gamma Ray From Oxygen-17 And The Identification Of Plutonium Oxide," Nucl. Instr. Meth., vol. 474/3, pp285-293, November 2001.