PNNL-SA-35296

IAEA Symposium
October 2001
Vienna

AUTHENTICATION OF MONITORING SYSTEMS FOR NON-PROLIFERATION AND ARMS CONTROL

R. T. Kouzes
J.L. Fuller

October 2001

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

Pacific Northwest National Laboratory
Richland, Washington 99352

DISCLAIMER

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-35296

IAEA Symposium
October 2001
Vienna

AUTHENTICATION OF MONITORING SYSTEMS FOR NON-PROLIFERATION AND ARMS CONTROL

R.T. Kouzes
J.L. Fuller

October 2001

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

Pacific Northwest National Laboratory
Richland, Washington 99352

AUTHENTICATION OF MONITORING SYSTEMS FOR NON-PROLIFERATION AND ARMS CONTROL

R.T. Kouzes and J.L. Fuller
Pacific Northwest National Laboratory
Richland, Washington

ABSTRACT

Radiation measurement and monitoring systems are central to the affirmation of compliance with nuclear material control agreements associated with a variety of arms control and non-proliferation regimes. A number of radiation measurement and monitoring systems are under development for this purpose, and the correct functioning of these systems need to be authenticated. Authentication can be operationally described as the process by which a Monitoring Party to an agreement is assured that measurement systems are assembled as designed, function as designed, and do not contain hidden features that allow the passing of material inconsistent with an accepted declaration.

INTRODUCTION

Authentication of monitoring instrumentation has taken on new importance because of the conditions of Host-supply and the use of information barriers required for observation of sensitive material. The end of the Cold War has resulted in unprecedented arms control agreements and Transparency Initiatives between the US and the countries of the former Soviet Union to reduce the number of nuclear weapons and to safeguard the dismantled fissile materials. Following the breakup of the Soviet Union, the US 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 US Department of Energy, through the MPC&A Program, and the US Defense Threat Reduction Agency, through the Fissile Material Control Program, commonly work toward the CTR goals.

Bilateral non-proliferation and arms-control agreements and negotiations held between the US and the Russian Federation (RF) are leading to the joint disposition of nuclear weapons material and the deactivation and decommissioning of production and processing facilities. A new population of material is being stored that has originated from the nuclear weapons programs, which will place new requirements upon information security and authentication beyond those of the traditional safeguards process. 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. Agreements generally involve some level of transparency, where a Monitoring Party enters a Host Party facility to gain confidence that the conditions of the agreement are being satisfied.

A number of radiation measurement systems are under development for use in potential confidence building activities. Certification, demonstration of operational functionality, and authentication are all required for a viable measurement system.

Under one bilateral agreement, the U.S. Department of Defense, Defense Threat Reduction Agency, Cooperative Threat Reduction (DoD DTRA/CTR) Program is constructing a Fissile Material Storage Facility (FMSF) at Mayak to hold up to 50 tons of plutonium from the disassembly of Russian Federation nuclear weapons. Negotiations are being held between the US and the Russian Federation for cooperative development of attribute measurement systems to provide confidence that the material is of weapons origin, is safely and securely stored, and is not reused for military purposes. Pacific Northwest National Laboratory leads a multi-laboratory team for authentication of monitoring equipment at the FMSF.

There are two basic requirements for an attribute measurement system: protection of classified information, and assurance of credible performance of the system for the measurement. The technology used to protect classified information is referred to as an information barrier, which is used on monitoring systems that are exposed to Host Party classified materials. An information barrier impacts the system design and authentication methodology.

When sensitive items are to be inspected, the most likely scenario is one of *Host supply*. Under this scenario, where the Host country supplies a system for the needs of the Monitoring Party in a Host facility, the crucial authentication issues are that a measurement system correctly measures the attributes, and that there be no hidden features in the system that allow it to pass out-of-specification items.

The process of authentication involves aspects of a measurement system throughout its lifecycle, including system design, possible off-site authentication activities, on-site authentication activities, and authentication following repair. Hardware and software design criteria and procurement decisions can make future high confidence authentication possible or impossible. Facility decisions can likewise ease the procedures for authentication since reliable and effective monitoring systems and tamper indicating devices can provide the assurance needed in the integrity of such monitored items as measurement systems, spare equipment, and reference sources.

As indicated above, the *combination* of constraints on monitoring systems is new:

- Monitoring systems measuring negotiated attributes of sensitive material
- Host supplied monitoring equipment in order to protect classified information
- Information Barrier implemented to provide protection of Host classified information
- Host operation of equipment under Monitor observation.

The US has defined *Authentication* as 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 a report on procedures and requirements for authentication of systems, from which the above definition has been extracted [ATF2001].

It should be noted that 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 are obtained, while the IAEA typically has applied authentication to the verification of data validity, and vulnerability assessment to the equipment assurance [Andress1995, Hatcher1982, IAEA2001]. 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 the requirement to protect the classified information of the Host Party, the measurement systems developed for non-proliferation and arms-control utilize an Information Barrier to prevent the Monitoring Party from observing such classified information. An *Information Barrier* 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 [IBWG1999, ATF2001, Fuller2000]. The information barrier blocks the Monitor from access to any classified information, but allows the Monitor complete knowledge of the data processing, converting the classified information into an unclassified result confirming whether the material conforms to the Host's declaration to meet pre-agreed criteria. Authentication carefully explores that data processing, involving a combination of functional testing, detailed examination of systems and documentation, and analysis of the security function for systems behind an information barrier. Information barrier protected systems may operate in *open* and *secure* modes, where open mode provides access to details of unclassified data for the purpose of functional testing, while secure mode is used with classified data and provides only simple pass/fail types of output information.

AUTHENTICATION BASICS

A measurement 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. 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 continuity of 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 continuity of 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 inspection, and
- private testing of duplicate systems in Monitoring party facilities.

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

- 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 share-ability 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.

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 increased functionality and 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 [Geelhood2000]. Authentication requirements will significantly impact hardware and software design criteria and may impact the overall cost. The transparency of the system has the most impact on authentication costs because non-transparent components must be reverse engineered or otherwise shown to contain no covert features. Thus, components must be selected based on transparency factors, complete documentation and ease of inspection. 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).

- 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 will largely 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 inspections. Other systems may be in continuous use and re-authentication would of necessity be accomplished by means that do not hinder operations. Whether systems operate in inspector attended or unattended mode will also impact what authentication and continuity of knowledge measures are required. 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 the 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 may be in addition to, and possibly independent of, the authentication of the software and hardware that has been used. Data must be protected from tampering throughout the entire lifecycle.

- Evaluation of Documentation – Examination of hardware, software, operations and maintenance full and complete 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 to be 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 inspection 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 inspections 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 makes on-site authentication more expeditious and provides time for the use of a larger set of authentication tools. Signals can be traced and measurements made on the duplicate system that are not possible during a brief period of joint inspection prior to use. However, authentication is facilitated by the ability to make some electrical measurements during joint inspections.

- Random Selection of Hardware and Software – Random selection of hardware and software components or complete systems is a powerful (perhaps the most powerful) authentication tool. Any party attempting to subvert any particular module must do so with the knowledge that the Monitor will have the right to examine one of these modules during private inspection at a Monitor's facility. Random selection consumes spare modules and requires a sufficient initial procurement. However, the Monitor never has last private access prior to a classified measurement. Random selection will be one of the tools used during on-site authentication efforts. Random selection can be applied at the component level or the system level. 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 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 systems to be installed in the facility and a duplicate complete system for private examination. During subsequent inspection 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 software-bearing-components prior to each use to confirm the controlling software in the system. If a repair is required, a replacement would be randomly selected by the Monitor from the spares 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. Tamper indicating devices provide some assurance of continuity-of-knowledge of a system and its components. Tamper indicating devices 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 Monitoring Parties during random selection.

AUTHENTICATION ASSURANCE LEVELS AND AUTHENTICATION

PNNL has applied the Common Criteria approach to create a definition of *Authentication Assurance Levels* (AALs) that are defined to quantify the level of assurance reached for a system subject to a set of authentication procedures. [Kouzes2001] The AAL definition allows for quantifying the level of authentication reached for a given system and allows decisions to be made about tradeoffs of authentication procedures and the desired level of authentication. The AALs will be used for the evaluation of authentication measures carried out at the FMSF. The IAEA has also prepared an evaluation standard based upon the Common Criteria.

The Common Criteria (CC) is an internationally recognized, multi-part standard for the evaluation of security properties within Information Technology (IT) products or systems [ISO 15408/1999 – "The Common Criteria for Information Technology Security Evaluation"]. The CC provides a set of composition rules to develop a rational and repeatable graded assurance package. The graded assurance package establishes a set of levels composed of criteria for evaluating a system or product. As the levels increase, the assurance that a product meets the security and functional requirements also increases. Since the CC only provides a set of composition rules, the final set of evaluation levels can be modified to meet the specific needs of an application.

Evaluation has been the traditional means of gaining assurance, and is the basis of the Common Criteria approach. Evaluation is performed on a system, called the "target of evaluation". 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 a target of evaluation and its design;
- Analysis of the target of evaluation design 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.

Assurance levels define a scale for measuring the criteria for the evaluation of a security target. Evaluation Assurance Levels (EALs) are constructed from assurance components. Every assurance family (i.e. groupings of components) contributes to the assurance that a target of evaluation meets its security claims. EALs provide a uniformly 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. The increase in assurance across the levels is accomplished by substituting hierarchically higher assurance components from the same assurance family and by the addition of assurance components from other assurance families.

Authentication Assurance Levels (AALs) are modeled after the CC's EALs and can be described by a set of high-level guidelines. The AALs range from 0-4, with 4 being the level that provides the most confidence that the system meets its security objectives. To obtain a high level of authentication, 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. 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).

The five 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

AAL0 (Unauthenticated) is applicable where no confidence in the correct operation can be expected due to the lack of assurance measures taken by the developer or authenticating authority. This AAL is used where, although some assurance measures might have been used, none are sufficient to provide any measure of confidence in system operations. For example, the developer does not develop, provide, or maintain any of the documentation on system design, development, and operations, nor does the developer allow members of the authenticating authority to participate in system design review, or to witness a comprehensive test of the system.

AAL1 (Minimally Authenticated) is the minimum level of assurance that any equipment used in monitoring regimes should have. An authentication at this level should provide evidence that the Target of Authentication (TOA) functions in a manner consistent with its documentation, and that it provides useful protection against identified threats. Co-operation of the developer is required in terms of the delivery of design information and test results. AAL1 is applicable in

those circumstances where developers or users require a low level of independently assured security in the absence of ready availability of the complete development record. The developer conducts functional and high-level design testing, and independent testing is conducted to ensure only that security functions perform as specified.

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.

AAL3 (Critical Authentication) is applicable where there is a need for a higher level of independently assured security in a planned development, and a requirement for a rigorous development approach without incurring unreasonable costs attributable to specialized security engineering techniques. AAL3 is the preferred assurance level that any equipment used in monitoring regimes should have. AAL3 requires that the system be highly resistant to exploitation. A developer designed lifecycle model, the tracking of security flaws, and independent testing of a selected sample of developer tests enhance assurance.

AAL4 (Highest Authentication) is the maximum level of assurance economically possible for equipment used in monitoring regimes. It is applicable where the value of the protected assets justifies the additional costs. AAL4 permits developers to gain a high level of assurance from the application of security engineering techniques to a rigorous development environment in order to produce a premium TOA for protecting high value assets against significant risks. AAL4 provides complete automation of configuration management, prevention of modification and compliance with implementation standards. Semi-formal responses from the developer are required for functional specifications, high-level design documentation and the TOA security policy model. The independent vulnerability assessments must ensure the system's resistance to external attacks. The developer must conduct a systematic search for covert channels and test the low-level design. Development environment and configuration management controls are further strengthened.

AUTHENTICATION OF RADIATION MEASUREMENT EQUIPMENT

Figure 1 shows a generic radiation measurement layout with an information barrier 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 can 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 even a Neutron Multiplicity Counter (NMC). The NMC consists of many ^{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 include mass of plutonium, neutron production from impurities and the matrix material, and neutron multiplication.

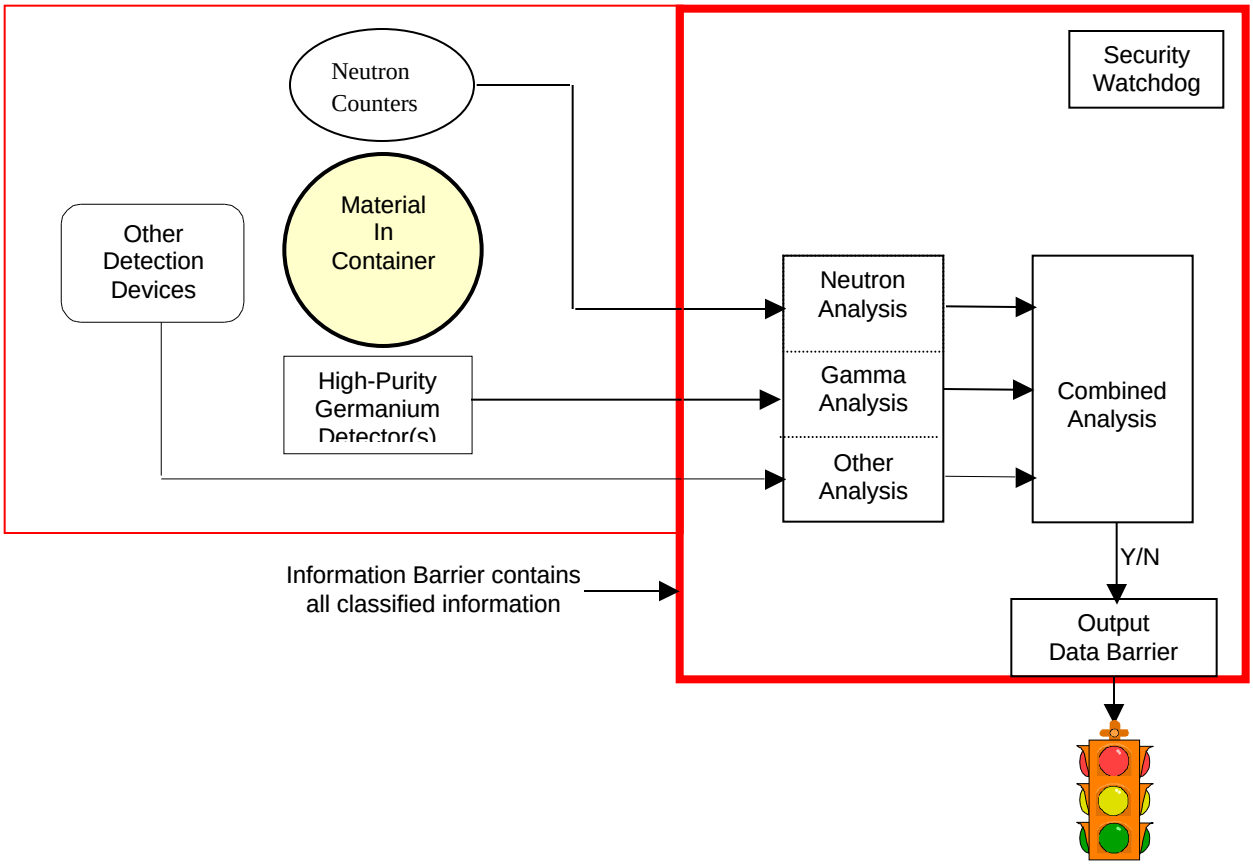

Figure 1. A generic schematic of a radiation measurement system for attribute determination in an arms-control application.

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 includes an Information Barrier (IB). The IB protects the Host's classified information from disclosure (such as the isotopic composition of plutonium in the Russian Federation) to the Monitor. In addition, the Information Barrier is 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 Information Barrier means that US inspectors will not be able to observe the actual data from the detector system or touch the system. Instead, only a red light or green light will indicate that the system has failed or passed the observed item with respect to the negotiated attributes for the material. The information barrier includes a security watchdog to shut down the system and purge all data if a problem arises such as opening of the system when a classified item is present. It is the presence of the

information barrier, and the resulting lack of detailed information about the data collected, that results in the requirement for system authentication and adds substantially to the problems of building a radiation measurement system.

EXAMPLES OF AUTHENTICATION DURING NORMAL OPERATIONS

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

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

Following a repair or upgrade of a system, it will be necessary to re-authenticate the system.

APPLICATION OF TOOLS FOR AUTHENTICATION

Table 1 provides examples of a few of the possible uses of authentication tools at various stages of a system lifecycle. These examples show how tools can be used at various points as a system lifecycle progresses. The cumulative effect is to help ensure that confidence is established in the system and that the system is designed and implemented to be authenticable and to provide reliable measurements. Each entry in the table will have associated mutually agreed procedures for implementation.

Generally speaking, as the required level of confidence is increased, the cost and time needed to authenticate the system will grow. Policy decisions will determine the desired level of confidence in a system. This then implies the level of technological implementation that will meet the requirements. Examples of how different tools can be used to increase confidence are shown in Table 2.

Tool→ **Lifecycle Element**	*Functional Testing*	*Evaluation of Data and Documentation for Hardware and Software*	*Random Selection*	*Usage of TIDs and Surveillance*	*Usage of Procedures*
Design		Specify and select authenticable components.			Follow authentication guidance.
Fabrication	Component testing.	Generate complete documentation and revision history. Compare to independently procured components.	Quantity purchase of commercial off-the-shelf components.		Follow authentication guidance.
Installation	System testing with physical and electronic sources.	Assure complete documentation. Comparison of design to as-built system. Comparison of software to documented source. Photographic baseline.	Random selection of system hardware or software components, or of entire systems for private examination.	Place TIDs on system components, enclosures, spares, sources, and rooms.	Follow defined procedures for entry and exit, functional testing, random selection, system operation, and placement of TIDs.
Operation	Random selection of system testing with physical and electronic sources.	Random comparison of system components with documentation including photographs.	Random selection of components such as PROMS; random selection of test sources.	Remove and inspect TIDs; evaluate facility monitoring video coverage of systems.	Follow defined procedures for entry and exit, functional testing, random selection, system operation, and placement of TIDs.

Table 1. Examples of some of the possible uses of authentication tools at various stages of a system lifecycle. Clear guidance in the above areas must be provided to achieve cost and schedule estimates.

Tool→ **Level of Confidence**	*Functional Testing*	*Evaluation of Data and Documentation for Hardware and Software*	*Random Selection*	*Usage of TIDs and Surveillance*	*Usage of Procedures*
Modest Confidence Level Examples	On-site functional testing with randomly selected sources.	Validate completeness of crucial documentation.	Random selection of system hardware or software components during on-site inspections.	Passive TIDs applied to measurement equipment and reference sources.	On-site procedures to verify continuity of knowledge for measurement systems and reference sources.
Medium Confidence Level Examples	On-site functional testing with a set of physical and electronic sources.	Validate completeness of crucial documentation and make selected comparisons to as built hardware and software.	Random selection of system hardware or software components, or of entire systems initially, and during on-site inspections.	Passive TIDs applied to measurement equipment and reference sources; active TIDs on selected rooms and equipment.	On-site procedures to verify continuity of knowledge for measurement systems and reference sources.
Higher Confidence Level Examples	On-site functional testing with set of physical and electronic sources; Monitoring Party-site full functional testing program.	Validate completeness of documentation and make complete comparisons to as built hardware and software.	Random selection of system hardware or software components, and of entire systems initially, and during on-site inspections.	Active TIDs applied to measurement equipment, reference sources and rooms; facility monitoring of all equipment and material, including video surveillance.	On-site procedures to verify continuity of knowledge for measurement systems and reference sources.

Table 2. Examples of level-of-confidence in a system versus possible uses of authentication tools to obtain that level of confidence. These are examples only, and are not meant to imply that a level-of-confidence is reached through the listed activities alone.

SUMMARY

Authentication is a necessary aspect of the implementation of systems for the assurance of compliance with non-proliferation and arms-control agreements. The United States technical community has developed a consistent basis for this authentication activity.

Some high level conclusions and recommendations are:

- Procedures must allow for authentication throughout the lifecycle of a system.
- Authentication procedures must be defined and jointly accepted for each application, each system, and each applicable lifecycle element.
- The Monitoring Party should negotiate the ability to authenticate the correct operation of a system under a variety of conditions spanning the range of operational and off-normal conditions and scenarios.
- Policy guidance should establish the desired level of confidence required from the authentication process, which will then determine the authentication activities.
- Systems must be designed for the ability to be authenticated, and to minimize the amount of authentication required to achieve confidence in system operation.
- Simplicity of design and good engineering practices are desirable to reduce the cost and time required for authentication.
- System design must consider how on-site procedures and conditions might affect the robustness of the hardware design and operation.

REFERENCES

[Andress1995] J.C. Andress, *The Assurance of Genuineness*, 17th European Safeguards Research and Development Association (ESARDA) Annual Symposium on Safeguards and Nuclear Material Management, Aachen, Germany, May 9-11, 1995.

[ATF2001] Authentication Task Force Report, June 2001. Washington, DC.

[Fuller2000] J. L. Fuller, *Information Barriers*, PNNL-SA-33328, Pacific Northwest National Laboratory, Richland, WA, June 2000.

[Geelhood2000] B. Geelhood, R. Kouzes, W. K. Pitts, *Design Guidelines for Authenticable Systems*, PNNL-13386, Pacific Northwest National Laboratory, Richland, WA, November 2000, updated May 2001.

[Hatcher1982] C. R. Hatcher, S.T. Hsue, and P. A. Russo, *Authentication Of Nuclear Material Assays Made With In-Plant Instruments*, IAEA-SM-260/103, International Symposium on Recent Advances in Nuclear Material Safeguards, Vienna, Austria, November 8-12, 1982.

[IAEA2001] *Procedure for the Authorization of Equipment Systems and Instruments Software for Inspection Use*, Department of Safeguards, February 2001, IAEA, Vienna, Austria.

[IBWG1999] Joint DoD/DOE Information Barrier Working Group, *Functional Requirements and Design Basis for Information Barriers*, PNNL-13285, Pacific Northwest National Laboratory, Richland, WA, May 1999.

[ISO15408] ISO 15408/1999, *The Common Criteria for Information Technology Security Evaluation*, 1999.

[Kouzes2001], 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*, PNNL-13587, Pacific Northwest National Laboratory, Richland, WA, July 2001.

Acknowledgement
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 Memorial Institute under contract DE-AC06-76RLO 1830.