PNNL-13386

Design Guidelines for Authenticable Systems

B. D. Geelhood
R. R. Hansen
R. T. Kouzes
K. R. Ames
M. M. Curtis
J. R. Griggs
W. K. Pitts
M. H. Ralston
B. A. Roberts
D. C. Stromswold
J. E. Tanner
H. A. Undem

Revision 1 November 29, 2000
Revision 2 March 8, 2001
Revision 3 April 2, 2001
Revision 4 April 19, 2001
Revision 5 May 14, 2001
Revision 6 June 12, 2001
Revision 7 July 31, 2001 – facility monitoring section rewritten

July 2001

Prepared for
the Defense Threat Reduction Agency
and the U.S. Department of Energy

Pacific Northwest National Laboratory
Richland, Washington 99352

Summary

Measurement systems are being developed in support of arms-reduction negotiations to verify the disassembly and storage of nuclear weapons and materials. Authentication, certification, and demonstration of operational functionality are all required for a viable measurement system. This document discusses in detail issues related to authentication.

Authentication is the process through which the monitoring party gains appropriate assurance that the information reported by a monitoring system accurately reflects the true state of the monitored item. Thus, the monitoring party is assured that measurement and monitoring systems are assembled as designed, function as designed, and do not contain hidden features that allow the passing of material inconsistent with accepted declaration. Such a hidden feature could be software or hardware that responds to some external trigger signal and alters the correct response to a measured item. Functional testing alone would not detect such a hidden feature unless the host is compelled to supply the trigger signal.

The only way to achieve authentication is to have complete openness in all hardware and software of the measurement system. The ability to thoroughly inspect all hardware and software items and compare them with thorough documentation is essential. This ability to authenticate a system must be included during its design. The potential gain from design decisions expedient for construction should be balanced against the cost of the additional authentication effort.

The basic features of a system that allows authentication are that it

- be assembled as designed
- function as designed under all environmental and radiation conditions
- have completely transparent architecture to allow continuity of knowledge (CoK) regarding all the data processing within the system
- not contain hidden features that allow the passing of material inconsistent with accepted declaration.

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

- Documentation must be complete for all aspects of system hardware and software.
- Hardware components must be simple and without extraneous functionality.
- Hardware components must be laid out for easy physical examination.
- Hardware that is unused must be disabled.
- Physical enclosures and shielding must provide a two-way information barrier.
- Identical and modular hardware components should be used across a system.
- Software operating systems should be minimal or non-existent.
- Software must be transparent and well documented (The software package shall include: commented source code, executables, build instructions, copies of compilers used, copies of all objects used, and algorithm explanations).
- Software must be simple, concise, and without extraneous functionality.

Operationally, authentication is achieved by

- comparing the complete system with its detailed design documentation (both hardware and software)
- using reference sources to test radiation measurements
- using tamper-indicating devices (TIDs) to limit possible alterations
- randomly selecting system hardware and software for detailed inspection
- privately testing duplicate and/or randomly selected systems or subsystems.

In addition to the detection systems used to perform measurements on individual items, Facility Monitoring Systems (FMSs) are essential to provide CoK related to item accountability over material previously verified. These systems are designed to detect tampering with accountable items and the measurement systems and unauthorized attempts at removal of items. Authentication of FMSs is crucial to assess the extent and frequency of re-measurement and re-verification efforts since quality and redundant systems provide additional confidence that tampering with or diversion of material has not occurred. For example, authentication of the FMS provides assurance that hidden features are not present in the system that would defeat the integrity of monitoring stored canisters.

Abbreviations and Acronyms

ACR	Absolute Control Room
ADC	analog-to-digital
AMS/IB or AMS for short	Attribute Measurement System with Information Barrier
ASIC	Application Specific Integrated Circuit
BIOS	basic input output system
CoK	continuity of knowledge
COM	communications
DIO	digital input output
DP	detection probability
DTRA	Defense Threat Reduction Agency
EPROM	Erasable Programmable Read-Only Memory
EEPROM	Electrically Erasable Programmable Read-Only Memory
FAP	false alarm probabilities
FMS	Facility Monitoring System
FMSF	Fissile Material Storage Facility
FMTT	Fissile Material Transparency Technology
FPGA	field programmable gate array
HPGe	high purity germanium
IAEA	International Atomic Energy Agency
IC	integrated circuit
I/O	input output
ISA	industry standard architecture
LCD	liquid crystal display
LEDS	light-emitting diodes
MCA	multichannel analyzer
MC&A	Material Control & Accountability
NMC	neutron multiplicity counter
OTP	One-Time-Programmable
PROM	programmable read-only memory
RAM	random-access memory
RD	Recording Device
RF	radio frequency (not used for Russian Federation in this document)
SAIC	Science Applications International Corporation
SNAP	Shielded Neutron Assay Probe
TID	tamper indicating device
TRADS	Trusted Radiation Attribute Demonstration System
UPS	uninterruptible power supply

Contents

1.0 Introduction

This report provides general guidance on designing authenticable[(a)] nuclear measurement and monitoring systems. The report also provides specific guidance on authentication for the equipment to be built by the Russian Federation and installed at the Fissile Material Storage Facility (FMSF) in Mayak where weapons-origin plutonium (and possibly highly enriched uranium) will be stored. This equipment includes the Attribute Measurement System with Information Barrier (AMS/IB or AMS for short) and the Recording Device (RD) that are anticipated for use by the United States during monitoring of the plutonium. The RD will observe each canister entering the FMSF and provide confidence that each canister contains plutonium with isotopics consistent with weapon-grade plutonium. The AMS will measure a statistical sampling of canisters from storage to provide confidence that each sampled canister is consistent with the declared mass of plutonium in metallic form with weapons-grade isotopics. This report also addresses the Facility Monitoring System (FMS) in the FMSF that will monitor the plutonium canisters during the times between inspections. Table 1.1 shows the plutonium attributes and anticipated equipment for use in these measurement systems.

Table 1.1. Measurements and Equipment for the AMS, RD, and FMS

System	Plutonium Attribute	Equipment
AMS	Presence	HPGe[(a)]
	Isotopic ratio	
	Mass	
	Non-oxide form	NMC[(b)]
RD	Presence	HPGe
	Isotopic ratio	
FMS	--	Video
	--	TIDs[(c)]
	--	Radiation sensors

(a) HPGe = high purity germanium.
(b) NMC = Neutron multiplicity counter.
(c) TIDs = Tamper Indicating Devices.

The equipment for FMSF will be constructed by the Russian Federation ("Host supply") in order to provide assurance that classified information about the plutonium is not provided to the United States during monitoring activities. An information barrier in the equipment will prevent this disclosure, and for the RD and AMS, only a limited output of attribute measurement results (e.g., "pass" or "fail" display lights) will be provided. Assurance of correct output from the limited display will be achieved by functional testing using known radioactive sources and by other authentication activities using random selection, detailed documentation, and private examination.

(a) The term "authenticable" is used in this paper to describe a monitoring system for which the monitoring party can gain appropriate assurance that the information reported by the system accurately reflects the true state of the monitored item.

Authentication goes beyond functional testing to inspect thoroughly the hardware and software to ensure that no hidden feature is present that would interfere with the correct measurement and display of results. Such a feature could be a "hidden switch" that responds to a transmitted signal or set of circumstances to provide an incorrect measurement result regarding a plutonium-containing canister. Software residing in programmable read-only memory (PROM) is especially vulnerable to modification by the host to erroneously pass items when selectively triggered. To effectively prevent hidden switch implementations, authentication should include verifying the state of the system before each use and significant previous private examination of the system (or a duplicate) to facilitate the joint inspection of the system.

Authentication is an extremely important part of measurement-system development. If the monitoring party cannot establish the credibility of the measurement system, then it would be much more cost effective to merely trust the host's declaration regarding the canister contents than to trust the host's declaration regarding the measurement system.

The funds for designing, constructing, and authenticating these systems come from the same limited source. Thus, the cost effectiveness of the overall process should be considered when making design decisions before constructing measurement systems. For example, using software without available source code may save a little procurement time or money, but it requires a huge reverse engineering cost to produce logical and human-readable source code for an effective authentication effort. In a resource-limited regime, cost-effective authentication is important, and credibility can be gained when design features facilitate authentication efforts.

The following sections of this report contain authentication guidelines with increasing degrees of specificity. Section 2.0 provides basic guidance that applies to all measurement systems. Section 3.0 provides general guidance on the authentication of hardware (gamma-ray and neutron sensors, electronics, and computers). Section 4.0 provides general guidance on the authentication of software, including system and application software. Section 5.0 provides authentication guidance for the FMS. Section 6.0 provides guidance specifically for the AMS. The appendix contains additional elaboration and background information related to some of the previous sections of the report. Hyperlinks are included in the main text to jump to the appropriate section of the appendix and also to return to the main report. Hyperlinks are also present in the table of contents to jump to sections of the main text.

2.0 Basic Authentication Guidance

Authentication can be described by a set of high-level guidelines. The basic tenets of authentication are that systems

- be assembled as designed
- function as designed under the full range of environmental and radiation parameters
- have completely transparent architecture to allow CoK regarding all the data processing within the system
- not contain hidden features that allow the passing of material inconsistent with accepted declaration.

Authentication of systems involves a collection of tools and methods, and it is operationally realized through

- the use of reference unclassified calibration sources
- complete design documentation for all hardware and software
- TIDs
- random selection of system-hardware modules
- comparison of system software to a previously authenticated copy
- privately testing duplicate and/or randomly selected systems or subsystems.

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

- Documentation must be complete for all aspects of system hardware and software.
- Hardware components must be simple and without extraneous functionality.
- Hardware components must be laid out for easy physical examination.
- Hardware that is unused must be disabled.
- Physical enclosures and shielding must provide a two-way information barrier.
- Identical and modular hardware components should be used across a system.
- Electronics and interconnections must be easily traced (no wire-wrap or hand-wired boards)
- Operating systems should be minimal or non-existent.
- Software must be transparent and well documented (including commented source code, executables, build instructions, and algorithm explanations).
- Software must be simple, concise, and without extraneous functionality.
- Software must not be self-modifying and preferably execute in place from the PROM.

3.0 Hardware Authentication Guidance

Authentication guidance in this section concerns hardware, in particular gamma-ray and neutron sensors, their supporting electronics, and computers.

3.1 Gamma-Ray and Neutron Sensors

This section provides guidance on designing gamma-ray and neutron sensors so that their operation can be readily authenticated.

3.1.1 Interference from Nearby Sources – Preventable Through Shielding or Protocol

Authentication of the gamma-ray and neutron sensors must show that the accuracy of the radiation measurements of an inspected item is not significantly degraded by nearby radioactive sources, including plutonium.

Either shielding or protocol can achieve the necessary freedom from interference. Sensor shielding will limit the potential interference of nearby sources on the gamma-ray peak amplitudes and neutron counts from the canister under inspection. Protocol can control the sources allowed in the measurement room during canister measurements. For further information see Appendix A, Section A.3.1.1

3.1.2 Variable Aperture - Use of a Variable Aperture Must Not Adversely Affect the Results

If an automatic variable aperture for the HPGe sensor is used, authentication tests must show proper processing of both the signal and background data with respect to aperture opening.

An automatic variable aperture opens and closes to control the gamma-ray flux reaching the detector. This aperture can be a viable information barrier tool because it limits inferred classified information from count rates and distances. Authentication must show that the measurement system properly accounts for changing detector efficiency with aperture opening.
For further information see Appendix A, Section A.3.1.2

3.1.3 Dead Time - An Attenuator is Preferable to Raising the Discriminator

For authentication purposes, a fixed, tungsten (or other high-Z) attenuator is preferred over electronic methods for controlling measurement deadtime in the gamma-ray measurements.

High count rates can adversely affect gamma-ray measurement systems. The count rates can be limited by an attenuator between the source and detector or by an electronic lower-level discriminator. The attenuator is preferred because an electronic lower-level discriminator does not prevent spectral distortion due to pulse pile-up. For further information see Appendix A, Section A.3.1.3

3.1.4 Shared Signals - Sharing Signals Must Not Significantly Degrade the Quality

If signals from gamma ray or neutron sensors are shared by multiple measurement systems, the sharing must not degrade the individual systems.

The sharing of signals from a single HPGe detector could degrade the input pulses and distort spectra. Neutron signals are less susceptible to distortion because they would likely be shared after passing a discriminator and being converted to logic signals.
For further information see Appendix A, Section A.3.1.4

3.1.5 Radio Frequency (RF) Sensitivity - The System Must Be Tolerant to RF Signals

RF signals must not degrade either gamma-ray or neutron system operation or be capable of triggering a hidden switch.

Authentication is concerned with remote-control possibilities as well as measurement integrity (e.g., no gamma-ray spectrum distortion or extraneous neutron counts).
For further information see Appendix A, Section A.3.1.5

3.2 Electronics for Gamma-Ray and Neutron Sensors

This section addresses authentication issues related to the electronics used with gamma-ray and neutron sensors. These electronics include amplifiers, discriminators, multichannel analyzers, commercial components and electronics, and other items.

3.2.1 Transparent Electronics – All System Electronics Must Be Completely Transparent

The sensor electronics and multichannel analyzer (MCA) system must be completely transparent in function (i.e., fully understandable) with no possibility of a hidden switch. Transparency includes having complete documentation for software source code for imbedded microprocessors and schematic descriptions of all custom or programmable components.

If there is reasonable functional capability for a component to alter the measurement result, authentication requires sufficient information to verify that the measurement result is properly processed through that component under all circumstances. Assurance of credible performance requires precluding hidden switch triggering by completely understanding the electronic design. Of particular concern is I/O functionality where alternate data could be readily substituted. The MCA builds and holds spectral data that could be altered in selected channels or have entire spectra replaced.

For authentication purposes, using an all-hardware MCA or building the spectral histogram in the analysis computer under interrupt control is recommended over using a nontransparent commercial MCA containing embedded CPUs.

Adequate documentation for full transparency might not be available when building spectral histograms using a commercial computer, such as a Canberra Inspector. The use of module-based systems (e.g., NIM, VME, or CAMAC) should be considered to achieve an all-hardware system.

For further information see Appendix A, Section A.3.2.1

3.2.2 MCA Resident Memory – System Shall Store One Spectra at a Time

If a MCA with multiple data buffers is used, the extraneous functionality must be mitigated. For example, to ensure that a multichannel analyzer is properly processing the just-measured data, the multiple buffers of the MCA shall all be actively cleared before the start of each measurement to prevent any spectral substitution within the MCA. These buffers should also be actively cleared after transferring the spectral data for analysis to minimize the residence time for classified information within the system. Alternatively, all but the base-memory buffer could be defeated.

3.2.3 Continuity of Knowledge - The State of the System Must Be Known at All Times

The state of the system before each measurement campaign should be completely known to the monitoring party. This requires either a means of verifying all jumper and adjustment settings or eliminating all access to the system after an initial authentication. For further information see Appendix A, Section A.3.2.3

3.2.4 Analog Front Ends - Authentication Effort Will Require Access to Analog Signals

The design of the analog front-end circuits should facilitate authentication and possibly accept input from electronic calibration sources (e.g., pulser).

Authentication issues concern the capability to monitor pulse shapes at the input to the discriminator. The capability of the front-end electronics to accept input from an electronic calibration source (pulser) is desirable for checking discriminator operation, double counting, line reflections, or ringing. For further information see Appendix A, Section A.3.2.4.

3.3 Computers

Lacking a U.S. prototype for an authenticable information-barrier-protected system, these comments relate to functional components included in previous demonstration systems. Previous systems do not set a precedent that unauthenticable systems are acceptable. There are several unresolved issues related to 1) the acceptability of open or dual-processor modes (e.g., classified and unclassified processing periods on the same central processing unit [CPU]), 2) the acceptability of various display types, 3) effective tamper-resistant sealing methods, 4) the acceptability of including hardware debugging features, and 5) the acceptability of extra input/output (I/O) to facilitate hash function or other comparisons of resident software to a golden copy. These comments address only possible computer implementations without endorsing any.

The following are reasonable computer considerations for an authenticable system design:

3.3.1 Visual Inspection - All Computers Need To Be Visually Inspectable

The compact design of laptop computers limits visual inspection, with a risk of damage during disassembly. While desktop computers are minimally inspectable, a single-board computer (such as the

PC-104 architecture) is much more easily inspected. If the Russian Federation designers implement a system with the Greenstar ISA[a]-bus card based MCA, there are commercially available development platforms that allow a PC-104 computer to interface with the Greenstar on an ISA bus. This would be more satisfactory than using an old desktop computer to gain ISA-bus slots.

3.3.2 Unused Input/Output Ports – These Ports Need To Be Rendered Useless

Unused I/O ports could be used to covertly pass a trigger signal for a hidden switch into the CPU. Both desktop computers and single-board computers typically have unused I/O ports that could potentially be used for covert signal information, such as triggering a hidden switch. These ports need to be rendered useless. The preferred method is by grounding all unused lines to preclude another component from usurping control of any line. For further information see Appendix A, Section A.3.3.2

3.3.3 Video Card – It Complicates Authentication and May Be Extraneous

Alternative output methods are preferable to the use of a video card, which can be difficult to authenticate. Using the communications (COM) ports on the CPU card is preferable.
For further information see Appendix A, Section A.3.3.3

3.3.4 Digital I/O Card – A Simple, Easy to Authenticate Card Is Required

The use of a digital input output (DIO) card without a "re-programmable" feature is recommended. If a programmable logic component is used, the use of one-time-programmable (OTP) field-programmable gate arrays (FPGAs) is preferred to FPGAs that are routinely reprogrammed at power on. However, the means for authenticating the FPGA programming must be provided including all the input files (e.g., source code, schematic capture, layout) used to uniquely specify the design.

If a DIO card is used in conjunction with a FPGA (as was done with the FMTT[b]-AMS computational block computer), authentication needs to verify the design FPGA programming and verify that the correct programming is still resident. Interrupt capability is not justified for the DIO controlling the display, and such capability should be considered extraneous and disabled.
For further information see Appendix A, Section A.3.3.4

3.3.5 Parallel Port Card - Operation of this Card Must Be Authenticable

If a parallel port card is used to interface with the analog-to-digital (ADC) data bus, operation of the parallel port card must be authenticable.

Previous comments relating to the DIO card apply. Clearly, interrupt capability for the ADC is justified.

3.3.6 Memory - Unused Sections of Memory Should Be Eliminated

(a) ISA = industry standard architecture
(b) FMTT = Fissile Material Transparency Technology

Unused sections of memory are potential locations for unexamined software or covertly stored data. Defeating address lines accessing unused sections of memory would disable the extraneous basic input output system (BIOS), Electrically Erasable Programmable Read-Only Memory (EEPROM), or PROM memory. Correct sizing of memory components is preferable. Unused flash memory, EEPROM, and/or static memory should be properly and verifiably disabled and/or erased.

Any unused memory bytes should be set to a value that requires a block erase before writing individual data bytes. Programming application software into EEFROM containing the BIOS may be a viable alternative to using one-time PROM for that software. This is subject to an acceptable method of verifying the memory contents before each use. The socketed PROM facilitates random selection better than a soldered in place PROM or flash memory.

3.3.7 Non-Volatile Memory – Must Be Identified and Contents Disclosed and Verified

All non-volatile memory should be identified in the documentation along with the prescribed contents for that memory. At power up and power down, all the non-volatile memory should be actively loaded with prescribed contents or have the contents confirmed by credible software compare.

Non-volatile memory is primarily a host certification issue, but authentication will ensure that all non-volatile memory is properly documented and loaded to avoid later right-to-use issues. It is desirable to compare flash memory software such as the BIOS to a pristine copy in the once-programmed PROM.

A method is needed to verify that the BIOS software and application software matches a “golden copy.” One method of verifying the BIOS is a bit-for-bit comparison at power up to an image on the randomly selected PROM containing the application software. Another software verification method uses a hash function, which requires 1) input of monitor-selected seed data and 2) an alphanumeric display of output strings. For further information see Appendix A, Section A.3.3.7

3.3.8 Input Devices – Input Device Should Not Be Capable of Passing Covert Signal

All the input devices should prevent passage of any covert signals by the operator to the software.

The authentication effort will seek out any means of operator and/or host-controlled input not explicitly permitted by protocol. For example, the time interval between button presses or the duration of a button press could trigger a hidden switch. Examples of indirect host-controlled input are a bar code value and canister weight. For further information see Appendix A, Section A.3.3.8

3.3.9 Output Devices - The Output Devices Are a Means of Divulging Classified Information

Alphanumeric or graphical display of output (rather than just PASS/FAIL lights) presents potential risks to the host’s classified information. However, during unclassified operation, such a display can be useful for system checking and creating monitor confidence. A dual mode of operation in which the alphanumeric or graphical display is removed during classified measurements may satisfy both host and monitor needs. If the host provides the external display device, the monitor should authenticate the device. It would be easy for the external display to project erroneous authentication/calibration

information. The system design must support an open mode (if used) in a manner that prevents the system from sensing if it is open or secure mode. For further information see Appendix A, Section A.3.3.9

3.3.10 Raw Data – Recording Raw Data Could Aid Private Authentication and Debugging

Raw data (e.g., spectrum) is typically classified, but a system that contains the means for recording this data from unclassified test sources would greatly aid both debugging and private authentication. The recording device could be an external disk drive or a printer that is removed during classified measurements.
For further information see Appendix A, Section A.3.3.10

3.4 Other

This section contains authentication issues not directly related to the radiation sensors and their electronics.

3.4.1 Data Barrier – The Simplest Data Barrier Is Preferred

All features need to be necessary and documented. An IB implementation should provide a clear boundary between classified data and unclassified data. For further information see Appendix A, Section A.3.4.1.

3.4.2 Security Watchdog – Feature Must Be Authenticable

If a power-down feature (security watchdog) is used, its features must be authenticated. The security-watchdog section is a design feature that the host may choose to implement to protect classified information.

The ability to manually power down the system with an external button or automatically power down when any of the access doors are opened is a valuable feature if the host desires more assurance than provided by the protocol agreements. The switches and relays must be well documented and free of extraneous features. Switch-failure modes and reliability should be documented. The data-collection and analysis within the IB system should not have access to security monitoring information to preclude any covert impact on the results due to system configuration.

3.4.3 Circuit Boards - Printed Circuit Boards Must Be the Standard

Hand-wired and wire-wrap circuits are not readily authenticable during a brief joint inspection because continuity measurements are required to trace each wire. The ability to access the hardware to make continuity measurements may be problematic under protocol negotiations. In any event, tedious and time-consuming continuity measurements are an unwise use of time under limited joint-inspection protocols.

3.4.4 Programmable Logic Chips - Programmed Logic Chips Require Special Consideration

It is more desirable to use custom components that allow verification of the programming than the type that does not. For example, FPGA can be readily verified if properly designed. However, verification of the programming in a general Application-Specific Integrated Circuit (ASIC) may be more difficult. For further information see Appendix A, Section A.3.4.4

3.5 Hardware Documentation

The following documents are needed to perform accurate authentication of the system. The documentation in all forms provided must be clear and readable.

- System Functional Description Document
- Preliminary Hardware Design Document (Conceptual Design)
- Final Hardware Design Document (Detail Design)
- Hardware Test Plan and Test Procedures Document
- Hardware Configuration and Quality Assurance Plan Document; Detailed Circuit Schematics
- Functional Descriptions, Operating Procedures, Calibration Procedures for all operational modules.
- System Documentation including:
  - Detailed Parts List for all Circuit Schematics
  - Manufacturers' Data Sheets for all components (integrated circuits, resistors, capacitors, inductors…)
  - Detailed Cabling and Wiring Interconnections Diagrams
  - Firmware code for all programmable devices (μControllers, PLDs, PROM, Flash,…)
  - Complete vendor documentation of all procured hardware—such as operating procedures, calibration procedures, circuit diagrams, parts lists, embedded code in any programmable device, packaging mechanical drawings,…
  - Procurement history for all components, including lot numbers and production runs
  - Circuit board layout files (e.g., Gerber Files)
  - Mechanical Drawings of all Electronic Enclosures

- Circuit description of electrical feed, cabling, and uninterruptible power supply (UPS)

- Schematics, layout, masks, and production run data for all ASICs custom manufactured for this system.

· Hardware Acceptance Test Results

· Hardware Operational Test Results.

4.0 Software Authentication Guidance

Complete transparency is fundamental to authenticable software. The software documentation package will include:

- complete machine-readable commented source code for all software residing on the system
- a complete machine-readable image of all executable code residing on the system
- all additional software (e.g., compilers, libraries) and build instructions to independently compile the provided source code into an exact duplicate of the provided executable code
- complete documentation explaining the data collection and the analysis algorithms.

A means must also be provided for verifying that the software running on the machine exactly matches the provided executable code. These requirements trap any covert attempts to alter the results by forcing a description and/or evidence into the documentation provided. This will also provide an easy means of confirming that the software source code is complete and accurately represents the code controlling the system during each measurement campaign. The authentication team will independently produce executable code from the submitted source code and require an exact match to the submitted executable code and the executable code installed in the system. Without complete source code, CoK regarding the data processing is impossible. If undocumented software collects, transmits, or processes measurement data, the monitor has no confidence that the undocumented software has not altered the results.

General Requirements on All Software

- The software shall be concise and single purpose.
- The software shall not contain extraneous functionality.
- The software shall not include self-modifying code.
- The software shall not include dead or unused code.
- The software shall not contain unused variables.
- The software shall avoid complex library.
- The software shall include source code with explanatory comments that explain each operation or equation.
- The software documentation shall include algorithms and explanatory documentation.

- The software shall be difficult to modify once installed. The executables shall reside on one-time PROM rather than magnetic media. Execution in place (XIP) is highly desirable to preclude any modifications while the software is loaded or executed.

4.1 System Software

Authentication issues for operating systems, libraries, and compliers are addressed in this section.

4.1.1 Operating Systems - Operating Systems Are Generally Not Authenticable

The preferred approach is to eliminate the operating system by writing bootable application software.

Microsoft Windows and Microsoft MS-DOS are very undesirable for authentication because of their complexity. Corruption of the operating system would be essentially undetectable. Alternative operating systems are available, but they are less preferable than bootable application software. No more than one operating system type or version shall be used throughout the system.
For further information see Appendix A, Section A.4.1.1

4.1.2 Libraries - Use of Large, Complex Libraries for I/O Functions Is Highly Undesirable

Input/Output is particularly vulnerable to hidden switch problems, and the source code for the library routines may not be available. For further information see Appendix A, Section A.4.1.2

4.1.3 Compilers - An Authenticable Compiler Must Be Used

Use of an open-source compiler (Fortran or C) or assembler (Assembly language) is preferred. No more than one compiler per programming language shall be used throughout the system. The software package must include working copies of all compilers and/or assembler, which are identical to that used by the host to produce the executable code. The package will also include complete instructions to identically reproduce the executable code from the source code. The authentication team will verify that the source code produces an identical executable code. For further information see Appendix A, Section A.4.1.3

4.1.4 Interrupts - The Appropriate Use of Interrupts Is Acceptable

Clearly, if the spectral histogram is built in the analysis computer, an interrupt-based program is more efficient. Authentication will ensure that interrupt capability is not usurped for undesirable purposes.
For further information see Appendix A, Section A.4.1.4

4.2 Application Software

The application software used during the FMTT demonstration raised issues that were described during a lessons-learned meeting at the Science Applications International Corporation (SAIC) Threat Reduction Center (September 2000). One major lesson was the difficulty in debugging software behind an information barrier. Thus, the application software should be mature and very robust. These

authentication requirements and tests represent an effort to achieve reliable operation behind an information barrier.

The authentication team requires machine-readable source code for all application software for more than just the inspection comparison reasons normally associated with authentication.

4.2.1 Data-Collection Software – Must Be Well Documented

The data-collection software should include documentation related to:

- all commands sent to the MCA to control it and request data transfers
- the data format for the data transferred between the MCA and the analysis computer. This should include what is contained in each byte or word and the format of each data element (integer, real, etc.). For example, the Canberra time format must be explained in sufficient detail to write a conversion routine into standard units (hours, minutes, seconds, etc).
- the data format, which must be fixed. It is unacceptable for the location of data elements to change dependent on MCA setup parameters.
- all error conditions, which must be explained, including root causes and error-recovery actions to be taken.

4.2.2 Gamma-Ray Analysis Software - Analysis Software Must Be Robust and Accurate

The software should include a robust (operating correctly under a broad range of radiation and environmental conditions) automatic-energy-calibration feature based on finding a predetermined list of peaks as the basis of the calibration. The analysis software must also perform satisfactorily under conditions of changing background due to nearby plutonium. The analysis software will be subjected to stress testing to determine the limits of robustness. The analysis software must fail gracefully when is limits are exceeded. When relevant, the software must calculate the correct isotopic ratio. For further information see Appendix A, Section 4.2.2

4.2.3 Neutron-Analysis Software - Analysis Must Be Robust and Accurate

The neutron analysis must provide the correct results over a wide range of masses, count rates, deadtimes, source geometries, source forms, nearby source interferences, and matrix compositions. The authentication team will examine the NMC analysis software for potential hidden switches.

The authentication team will examine the NMC analysis software for extraneous functionality. For example, database features are extraneous to the information-barrier application and will be confirmed as completely removed.

- The authentication team will examine robustness against external nearby sources.

- The authentication team will examine robustness over a range of matrix effects because the source might not be presented in the declared matrix.

- NMC analysis has exhibited problems when the source contains unexpectedly high levels of (α,n) producing materials. Negative mass values can occur when the totals rate is very high. The authentication team will document the limits of applicability of the analysis to such problems.

- The authentication team will examine the NMC analysis software for potential hidden switches.

- The authentication team will examine the NMC analysis software for extraneous functionality. For example, database features are extraneous to the information barrier application and will be confirmed as completely removed.

4.2.4 Protection of Classified Data

The computational block or output-controlling software must be simple and reliably protect all the classified data in the system.

- This software does not have to be located on a separate computer from an authentication point-of-view. For example, if the software tasks are separately executed from a batch file, the simple computational block software can be adequately separated from the complex analysis software without using a separate computer. The laudable goal of using simple computational block software is to make the certification and authentication tasks easier by handling the final threshold comparisons and unclassified output in a concise and easily understood routine. If one of the analysis computers in the Fissile Material Transparency Technology Demonstration system ran the computational block software, examination of the computational-block computer and its associated BIOS and operating system could have been eliminated from the authentication task.

- The logic of this software module should be easy to follow and free of library calls.

- This module should control the timing of the PASS/FAIL/ERROR outputs to prevent potential disclosure of classified information by means of the measurement duration or the time between start and an error condition.

- This module should provide the only method of controlling the PASS/FAIL/ERROR outputs in the entire software package. An electronic search for other use of these data ports will be made.

- For easy certification, the software should erase and/or overwrite classified data when it is no longer required. For example, overwriting the RAMDISK image of the spectral data at the completion of each analysis cycle provides additional confidence that classified data are irrecoverable when the system is powered down.

4.2.5 All Software Should Be Modular

The software should be modular (collection, analysis, and output) so that various portions can be extracted and run on test data. Modules with identical functionality should use identical software. For further information see Appendix A, Section A.4.2.5

4.2.6 Self-Modifying Software and Fixed Parameters

The software shall not be self-modifying, and parameters used that are considered fixed or constant shall be read-only and non-modifiable. If the software is self-modifying, the detailed examination of software is far more complex and resource consuming. For further information, see Appendix A, Section A.4.2.6

4.2.7 Program Overlays

The use of program overlays to allow large codes to fit within limited memory is discouraged. However, this approach may be required if an operating system is not used. If overlays are used, they must be clearly documented, and each overlay should perform a logical and sequential task without jumping between additional overlays.

4.2.8 Code and Data Segments

Software should be written to conform to code and data-segment separations. Special parameters, which should not be modified (e.g., threshold values, library data—peak energies and intensities, etc.), should reside in a separate common block, which can be protected by a range of addresses when operating under a debugger.

4.2.9 Multiple Capabilities for I/O

The software package should not have multiple capabilities to handle each I/O port.

4.2.10 Specific Compiler or Operating System

The software should not be specific to one compiler or operating system because that might facilitate specific coded hooks to implement a hidden switch.

4.3 Software Documentation

The following list of documents is deemed to be the minimum needed to perform accurate authentication of the system.

- System Functional Description Document
- Software Requirements Document
- Preliminary Software Design Document (Conceptual Design)
- Final Software Design Document (Detail Design)
- Software Test Plan and Test Procedures Document
- Software Configuration and Quality Assurance Plan Document

- List of system software, including operating system, compilers, databases, etc.
- List of computer hardware, including CPU, hard drives, peripheral equipment, etc.
- Software Coding Standards Document
- Software Installation and Maintenance Plan
- System's Users Guide Document
- Software Source Code (machine readable format)
- Software Executable Code identical to that loaded on the system (machine-readable format)
- Build instructions to generate an identical executable from the source code
- Explanatory documentation of algorithms and analysis techniques used (detailed rather than summary)
- Explanatory documentation of all data transfer formats and command instruction formats
- Explanatory documentation of all I/O handshaking protocols and error checking used
- All documentation provided with commercially purchased software
- Software Acceptance Test Results
- Software Operational Test Results

5.0 Facility Monitoring Authentication Considerations

5.1 Facility Monitoring System (FMS) Authentication Introduction

Simply stated, the purpose of the FMS is to assure that containers that have entered into Continuity of Knowledge (CoK) cannot be moved or switched without detection and monitoring and thus remain in item accountability. The FMS is also intended to give assurance that the AMS, the RD, the FMS itself, and other materials and equipment under seal are not tampered with. As such, the FMS is primarily aimed at preventing the Host from circumventing FMSF agreements and to learn of any diversion attempts. The FMS is not intended to provide operational security for the facility.

The purpose of this section of the document is to provide design guidance to assure that the FMS has the capability to perform this purpose without being unnecessarily compromised and that the FMS can be readily authenticated.

Authentication is a suite of activities that occur on at least three levels, to wit:

- Functional authentication, wherein it is ascertained that the functional specifications of the FMS are sufficient to assure that the system as implemented by the facility construction entities will meet the top-level functional requirements for continuity of knowledge as reiterated above.
- Installation authentication, wherein it is ascertained that the FMS has been installed, connected, and programmed so that it functions as specified and that its functionality cannot be nullified by built-in vulnerabilities. Specifically, the authentication team will search for hidden switches that would allow the host to subvert the FMS at will.
- Operational authentication, wherein surveillance data is collected for analysis and it is ascertained that the FMS has not suffered any functional degradation or been modified since the previous authentication inspection.

In our design guidance considerations, we will attempt to address potential authentication concerns at all three levels. However, since the actual design of the FMS is far from final at this point, the considerations will be more general and aimed at providing design guidance. The upside, of course, is that there may be time to avoid authentication problems by considering the points raised here during the design phase.

5.2 General FMS Concerns

A single monitoring system is seldom used in nuclear fuel stores since its failure might require the total re-verification of all items. Dual or multiple coverage is often used to provide defense-in-depth to avoid loss of CoK whenever a single element is compromised. Dual systems must be functionally independent and not subject to a common tampering or failure mode. Usually dual systems incorporate some combination of video surveillance and TID usage. The design of the FMS should clearly define each coverage layer including a list of sensors and systems included in each layer. In addition, the design should clearly define all trigger and data pathways to facilitate evaluation of coverage independence and highlight any critical pathways or components. In a complex system, there may be a tendency to add extraneous sensors or to cross link data in effort to enhance efficiency or protection. When several sensor

types and triggering schemes are utilized, additional *de facto* layers of protection may be introduced and these layers should be clearly identified.

The regime requirements of regarding the localization of each item under CoK should be clearly stated and related to the primary mission of the FMS. For example, if the mission is to prevent diversion of material out of the FMSF Mayak storage building, perimeter or choke point monitoring may be sufficient. If the mission is to verify the location of every canister at any given time, more comprehensive monitoring is required. Regime requirements for real-time video in contract to intermittent frame storage should also be clearly stated and related to the primary mission of the FMS. For example, observing the application of a TID or the retrieval of a canister for AMS measurement with video rather with an inspector in place is not consistent with intermittent frame storage.

If the FMS collects video or radiation measurements in addition to the use of passive TIDs, the issue of classified data must be addressed early in the design. If the video shows security measures, it may require mitigation measures such as 1) an information barrier, 2) field-of-view limitations, or 3) limitations on the use of the video records. The radiation measurements made by the RD and AMS systems require an information barrier. A potential FMS radiation sensor such as a gross gamma ray or neutron sensor is not expected to reveal classified information (e.g., plutonium isotopics due to lack of energy resolution). The FMS design should include sufficient analysis to allow resolution of any security issues prior to the final design review so timely FMS certification is not at risk. Since access to actual data simplifies authentication of the FMS, an FMS design that meets requirements without incorporating an information barrier is highly desirable.

The FMS is expected to monitor itself to prevent tampering with components in a manner that would allow undetected diversion of material. The FMSF regime uses 1) the RD to initiate item accountability, 2) the AMS to confirm canister contents and 3) the FMS to maintain CoK using video systems, radiation monitors, TIDs, and data processing as directly specified for the FMS. Thus, the FMS is expected to monitor all these items to prevent tampering. The quality of the anti-tamper protection offered by FMS determines the extent and frequency of item re-measurement and component re-authentication.

The authentication team believes that two realistic threats must be considered. Threat #1 involves a potential diversion of a significant amount of material by the host nation. Under that threat, the value of host-supplied TIDs is minimal because identical replacements would be easy to come by. Threat #2 involves a potential diversion of a small amount (1 to 10 canisters) by well placed insiders. Under Threat #2, the host-supplied TIDs may have some value, but one can not discount the risk that the insider group exerts some control over the host-supplied TIDs. The video surveillance could be used to provide some knowledge regarding placement and storage of canisters without use of monitor-supplied and monitor-witnessed TIDs. Without details of the facility-monitoring plan, one cannot be *a priori* satisfied that dual coverage is adequately supplied when discarding the value of TIDs that a monitor supplies and observes. Some of the following explanatory comments include that TID-related concern of the authentication team. These concerns are not meant to preclude other potential solutions that might meet strict CoK guidelines.

The following factors must be considered in facility monitoring authentication:

- The FMS must be examined sufficiently to provide assurance against circumvention or defeat by either the host nation or well placed insiders. This examination includes the use of complete

documentation, which enables the monitor to search out potential “hidden switch” methods of usurping the system for any unauthorized purpose. This examination also includes private examination of exact duplicate subsystems and components at a Monitor-controlled site. Both functional tests and targeted tests aimed at demonstrating “hidden switch” problems are included.

- CoK requires that all plausible material diversion paths out of the FMSF must be covered. Authentication will evaluate the effectiveness of the FMS in detecting unauthorized removal of canisters.

- The system uses components that are authorized for use at the facility in question. If a portion of the FMS design is disabled or disallowed, the overall effectiveness of the system is compromised.

- Individual components of the system must be evaluated, and their integrated application at the facility should also be tested. The results of this testing, along with requisite modifications to correct any deficiencies, should be used along with statistical methods and vulnerability assessments to create a plan for maintaining system authentication.

5.3 Primary FMS Elements

The goal of a safeguards system is dual or redundant coverage of all the items in accountability to provide a CoK even if the primary system fails. The primary FMS coverage is often provided by seals/TIDs. Thus, seals, which prevent modification of canister or component contents, will be discussed first. Video surveillance, which attempts to track and locate canisters, often provides the second redundant coverage of the containers. Video surveillance of the seals also provides additional confidence that tampering has not occurred. The video surveillance may contribute to both coverage methods and thus require some independence or selectivity in data collection where seal monitoring video is maintained separately from canister tracking video.

5.3.1 Seals/TIDs

The role of seals in maintaining CoK is central. Robust canister seals are fundamental to item accountability and provide a rationale for tracking items rather than using mass accountability. Canister seals are used to assure that the fissile material (shown by the RD to be within a canister) is not removed from a canister. Nest-cover seals are also crucial in providing assurance that containers are not removed from or added to nests without monitoring-party knowledge. While the canisters are stored in the nests, they are out of direct video surveillance. Thus a video monitored nest-cover seal could be considered an important means of maintaining dual coverage over the stored material.

There are conflicting views regarding the efficacy of seals depending on type of seal, who supplies them, who controls them prior to application, who applies them, how and by whom they are checked, who removes them, and who has custody after removal. It would be helpful to the authentication team and, we suspect, to the design and negotiation teams if there were an agreed-on US requirement for seals to be used in the Mayak FMSF.

The remainder of this discussion on seals/TIDs assumes the following:

· Bilateral Seals -- The US will have the right to supply, apply, examine, remove, and keep some seals and also to approve the specific design features that accommodate the application of these seals.

· Containers, shrouds, nests, equipment, and enclosures sealed with such seals will be considered to be under CoK. The regime has not finalized the desirability and/or method of sealing of shrouds and/or nests.

· Unilateral Seals -- The facility operator will also have the right to supply, apply, examine, remove, and keep some seals as a means of deterring insider threats and maintaining administrative controls.

· Operator-supplied seals will not confer US-recognized CoK.

To be valid, a seal must have two characteristics – uniqueness and break detection. Tests in US laboratories have demonstrated that it is possible both to duplicate seals and to design seals which can be opened and re-closed without giving a tamper indication. No known seal is completely impossible to defeat, but being able to produce the seals, have custody of them before use, and to retain custody after use for private examination makes defeat much more difficult and less likely. The video surveillance of the seals greatly enhances acceptance of seals as a means of maintaining CoK.

Design Considerations:

Seals will be required for at least six specific applications:

· Sealing the AMS – including the AMS enclosure, AMS subsystem enclosures, the room where it is stored, the cabinets where AMS parts, components, software, and other associated equipment and material are stored.

· Sealing the RD – including the RD enclosure, RD subsystem enclosures, the cabinets where RD parts, components, software, and other associated equipment and material are stored.

· Sealing the FMS – including the FMS components such as 1) all sensor enclosures, 2) all access points to sensor cables, and 3) all data-collection and review computers along with their associated components and software. Seals also protect FMS tools, spares, and radiation sources used for calibration and authentication.

· Sealing AT400R containers, which are verified by radiation measurement to contain weapons-origin material.

· Sealing container shrouds, which contain up to four AT400R containers in baskets that are placed as a unit into a nest.

· Sealing all nests where verified and unverified weapons-origin material is stored.

Note: The first five applications are straightforward uses of TIDs/seals and the authentication team sees no need to elaborate on them. The last requirement has been subject to some vigorous discussion.

Nest-Cover Seal Issue

It is the contention of the authentication team that nest-cover seals are the only practical way to assure that the population from which random samples are withdrawn for AMS-based verification remains in place (with additions, but no unauthorized withdrawals) and therefore gives meaning to statistical sampling. The following discussion explains the rationale behind this position.

It is not reasonable to expect, in the opinion of the authentication team, that a combination of video cameras and radiation sensors (and even including motion sensors, which have not been explicitly specified as part of the FMS) could resist spoofing efforts and reliably detect any and all movements of

containers out of or into nests during the long periods when US inspectors are not present. To support this point of view, we offer the following ways in which the combined system could be spoofed or defeated:

- power failure of sufficient duration to exhaust batteries
- shielding of radiation sensors so they won't trip cameras
- 'accidental' cutting or shorting of signal wires
- placing posters with normal scenes in front of video cameras
- hidden switch designed into cameras to recycle the normal scene

Some of these techniques, if used alone, would still give indications that an off-normal event occurred, but there would be no way to characterize the event. However, if used cleverly and in combination, it is clear that 'shell games' could be played with stored containers unless the nests are sealed.

The entire issue of Seals/TIDs for Mayak is currently the subject of a complete test and evaluation report, which has been released in draft and will be released in final form shortly (Tanner 2001).

It is important to remind everyone, however, that there is currently no authenticable seal for the nest covers. The problem was generated by the fact that the current design does not allow any IAEA class seal to unambiguously connect the nest cover to the nest-mating assembly. It is also our understanding that wires from cable-variety seals will not be permitted to drape across the floor, nor will any non-flush assembly be allowed. The floor must remain perfectly flat at all times, without restrictions or tripping hazards. The problem of the nest cover will require additional considerations by the FMSF team.

A possible alternative nest-cover seal would not be attached between the cover and the surrounding nest-mating assembly, but rather provide an indication that the nest cover has been moved. For example, reflective particle paint or a label-like seal applied to the underside of the lip of the lifting-structure hole (lipped blind hole in the center of the nest cover) would be gouged by the lifting mechanism. Alternatively, some sort of gravel or beads placed within the lifting-structure hole would have to be either removed prior to a lift or disturbed by the lifting mechanism. A before and after photographic comparison would be used to periodically examine such nest-cover seals for unauthorized nest openings. An active seal could respond to acceleration or motion.

Based on an examination of a sample nest cover at PNNL, it appears that it would be possible to modify the nest covers to accept an IAEA class cable seal and that such a seal could be kept entirely below the level of the floor surface. As envisioned, the nest seal would seal not to the surrounding nest-mating assembly, but to the shroud under the cover. Sealing to the massif is possible, but would probably require more extensive modifications to the nest covers and to the nests themselves.

Installation Considerations:

While the TID/seal components are not installed in the same sense as the other elements of the FMS, their use during the installation of the FMS will be vital. Installation inspectors will be responsible for carefully examining and documenting each enclosure to be sealed to guard against trapdoor features. They will also need to allow time in their work planning to apply seals to work in progress at the end of each workday so that modifications are not made during their absence. Large numbers of temporary seals are likely to be needed during installation, so installation planning should assure that an adequate number are on site in containers that are sealed when unattended.

Operational Considerations:

The use of seals is linked to the sampling plan and the plan for authenticating the FMS, the AMS, and the RD. Prior to an inspection visit, the inspection team must assure that they have an adequate number of seals of the required types and that all team members are fully trained in the use of each type of seal. From a TID/seal perspective, an inspection will not be complete until removed seals have been examined in US labs for evidence of tampering or attempted tampering.

5.3.2 Video Surveillance System

The primary purpose of the video system is to back up the seals/TIDs in assuring that items under CoK are not moved or tampered with. As a CoK system, the video surveillance system provides a video record for later analysis of canister-related activities and movements. This includes the processing and loading of containers verified by the RD, any unloading of containers from the nests, and other off-normal events, such as an entry to room 358. Depending on regime use of the video surveillance system, the video system may require the ability to monitor seal application or canister movement in real-time with a high frame transmission rate. The video requirements must be consistent with the regime use. It is desirable to limit the FMS to intermittent frame transmission and have inspectors in place to directly witness TID applications and canister movements related to AMS measurements. The video will also maintain a visual record of the status of objects under CoK when no activity is scheduled – in essence documenting periods of time when 'nothing happened'.

The video surveillance system could be used to:

- Discover any unauthorized movement or removal of the containers after entry into FMSF Mayak
- Discover any tampering with container bar code labels or TIDs
- Discover any tampering with the contents of the containers
- Discover any attempts to swap containers within FMSF
- Track and localize canisters within the FMSF
- Electronically witness Russian application of TIDs as a replacement for an *in situ* US inspector solely as a witness of TID applications.
- Provide CoK regarding the measurement systems used to bring canisters into container CoK.

It is likely that the following video camera will be used due to IAEA acceptance:

Camera:	Aquila DCM-14 camera approved by the IAEA
Frame Info:	770x520 EIA black & white (analog, approximate pixel equivalent)
Compression Info:	JPEG compression to approximately 10-20 Kbytes/frame
Data Transfer Info:	RS-485 serial port at 5 seconds per frame DES-encrypted

Our recommendations are not based on this particular camera, but we regard it as a good candidate.

Design Considerations and Recommendations:

- Camera locations – Dual coverage using opposing cameras is suggested to make detection of camera tampering more likely. When each camera is within the field-of-view of another, camera TIDs are protected and confirming views of all activities are provided. Camera locations providing redundant coverage prevent crucial views from being easily blocked. If the camera is mounted high on the wall (above the top of the doorway) pointed across the room at the subject doorway, a temporarily placed

object will not readily block an important section of the camera view-of-view. Mounting cameras high on the wall will also make an attack on the camera more difficult to make without being detected by the opposing camera.

- Camera lenses – Manual zoom lenses for cameras would allow viewing angles to be optimized during installation. The ability to remotely change lens zoom settings is undesirable because it is unnecessary during unattended operation and it may be a potential spoofing mechanism. It is desirable to have a large depth-of-field for the video camera lenses because the canister will likely move through a room in the direction the camera is pointing when opposing cameras are used. A depth-of-field limitation may require increasing the number of cameras.
- Battery backup – Backup power for video cameras allows normal operation to continue during power failures. Backup lighting during power outages is necessary for uninterrupted video surveillance. A strobe lighting system could be used with flashes for the desired frames as a means of minimizing power requirements. Since video frames are normally acquired for local storage at the highest triggered frame rate at random intervals, the strobe should not provide sufficient additional information to aid subversion of the system.
- Low-light video cameras – Cameras should be able to capture images in low-light conditions, such as when emergency lighting is being used.
- Operator controls – Controls should allow operators to concentrate on images instead of system operation. At a minimum, the operator needs to be able to quickly sequence images and to easily compare images from several cameras for the same time frame. Ability to 'bookmark' video images or sequences for easy return would also be very valuable. (good human factors design)
- Workstations – Video review is facilitated by at least 2 operator workstations with the ability to switch between cameras, make archival recordings, and make 'instant replay' analysis of video footage.
- Data recording capability – Multiple camera views should be recorded simultaneously along with readings from other sensors to allow post-event analysis.
- Coordination with other sensors to record off-normal events
- Lighting – lighting levels must be high enough so that potentially important activities cannot be hidden in shadows or by using low-contrast camouflage.
- Suggested camera characteristics – b/w cameras, which have much higher resolution in low light, may be best suited for this application
- Encryption – DES-level encryption of video data between the camera modules and the collection computer allow authentication of the signal content.
- Frame compression – Image files should be compressed using JPEG compression. A compression ratio of 50:1 preserves image resolution, is widely accepted and will keep data storage requirements reasonable.
- Camera software – Each camera should be equipped with scene-change sensing software that will trigger capture and transmission of video at a higher frame rate for a pre-determined surrounding interval. The interval duration can be preset inside the camera enclosure.
- Data buffer – Each camera should have the ability to buffer up to 5 minutes of real-time or interval video in the camera enclosure for transmission to the central computer. Frames should be continuously captured and buffered at a relatively high frame rate (12-60 frames per minute) so that the frames immediately prior to a triggering event can be transmitted to the main computer for archival and analysis along with other sensor readings associated with the triggering event. (Readily available 128Mb memory modules should meet this requirement).

- Event triggered video – The video surveillance system should be triggered to record frames at a higher rate whenever
    - Radiation-emitting containers pass through a portal entering or leaving a room
    - Radiation-emitting containers are present in a room
    - Motion is detected in the room (if motion sensors are used)
    - The image analysis software within the camera module detects a scene change.
- Triggering sensors – The use of multiple trigger sensors is recommended. For instance, a motion detector and a radiation detector might be mounted in the same room with a video camera. An area radiation sensor is recommended to determine when a radiation canister is present within a room. A portal radiation detector is recommended to determine when a radiation canister enters or leaves the room. It may be advantageous and desirable to place sensor elements within the same enclosure as the video camera and protect all elements and trigger pathways with the same TID.
- Trigger pathways – Redundant-triggering paths should be used. When one of the sensors detects an off-normal condition, it should send a trigger signal directly to all the video cameras in the same room. The video frame should include edge-encoded information regarding the trigger signal (e.g., which signal caused the trigger and an indication of the magnitude of the change). A direct trigger pathway is recommended in contrast to a network-based trigger from a central computer as a simpler approach. Under a network-triggering scheme, the trigger signal is encrypted into the routine state-of-health signal sent to the central computer, which will, in response, send an encrypted trigger signal to the video camera to transmit additional frames temporally held in local memory. Similar provisions could also be used for sensors not collocated with cameras.
- Triggered video interval – The triggered video interval should be symmetric about the trigger event. Thus, storage at a higher frame rate should occur for ±60 seconds relative to the trigger event. Saving frames prior to a motion-triggered event is valuable when attempting to preclude or discover an attack on the camera. It is also equally valuable to view both the approach and departure of a canister moving through a portal radiation detector. This requirement for symmetric storage at a high frame rate requires continuous local collection and storage at the highest triggered frame rate.
- Triggered video frame rates – The usual surveillance cameras (DCM-14) used for safeguards have a maximum data transfer rate sufficient to transmit one frame every 5 seconds. However, the maximum frame rate for storage under triggered conditions can be higher since the camera has an internal buffer and might be able to catch up using transmissions following the trigger. However, the system must clearly identify the means of handling a potential buffer overflow error when subsequent triggers prevent catching up on the frame transmission before the internal buffer recycles. The frame storage rate must be sufficient to capture the event causing the trigger. Thus, several frames should be stored during the time of passage through the room or past a portal sensor.
    - Untriggered baseline rate – at least 1 frame every 30 minutes
    - Radiation-in-area triggered rate – 1 frame every 60 seconds
    - Motion or portal triggered rate – 1 frame every .04-1 seconds
    - Scene-change triggered rate – 1 frame every 1-5 seconds

  Running through a room at about 6 m/s is consistent with 1 frame/second, walking through a room is consistent with 0.2 frames/second, and walking within the view-of-view of a portal sensor is consistent with 0.04 frames/second. The triggered frame rate should also be sufficient to capture any attempt to spoof the camera by modification or placing a safe picture in front of the lens. It would be difficult to approach a camera in view of the opposing camera, climb up to it and perform the spoofing activity within 5 seconds. The lowest acceptable frame storage rate is desired from the point-of-view of minimizing storage media size on the main collection computer.

- Untriggered video frame rates – Locally the camera will acquire frames at the maximum triggered rate to allow for storage of scenes prior to the trigger event. The maximum collection rate is also necessary for potential triggering based on scene-change software within the camera. Random interval triggering should be built into the camera enclosure so that a video frame will be collected randomly within an average interval to make it difficult to attack the camera between frames. During an initial phase without video triggering, the video rate should be as high as the data transmission and storage capacity of the video collection computer allows. The data transmission rate appears to be the major bottleneck when several cameras use a shared transmission pathway to a collection computer. If the system data capacity is specified as being sufficient to contain data triggered at the maximum rate, collecting video at the maximum rate is prudent until a working trigger scheme is implemented during phase II. This allows retrieval of all the data that is desired under a triggering scheme. The authentication team recommends capturing and storing images no less often than every 30 minutes during unattended operation when triggering is available to initiate a higher frame rate. The triggered rate should not be lower than the minimum time required to pass through a doorway/portal. Several frames should be acquired during the minimum passage time through a room.
- Data transmission pathway – The camera has a frame transfer limitation of 1 frame every 5 seconds, which hinders system performance. Using a multiplexed transmission scheme from multiple cameras to a common data collection computer is not recommended because it makes this limitation more unmanageable.

Installation Considerations:

Given the likely levels of US manpower to be available during installation and the projected long absences from the site, the authentication activities carried out during installation should be very carefully planned to assure time is spent on the most important activities. One of the most important activities during installation will be to assure that the cameras achieve coverage of the desired fields of view. Since facilities always have deviations from the design documents, it will be important to verify that as-built conditions do not compromise the ability of the cameras to cover the intended and required areas.

- Make sure cameras view & record declared areas
- Test trigger conditions
- Search for hidden switches using visual methods and high-frequency signals
- The DSM-14 cameras contain a manufacturer-set cryptographic key within each camera for signal authentication. However, some additional capability such as inspector presence in the video image at logged times may be required to authenticate video signals and data lines during the initial installation and future operational visits.
- The cryptographic algorithms used in the FMSF may be of Russian origin and require evaluation regarding the difficulty of swapping video images undetected.

Operational Considerations:

Video system authentication activities during site visits should be limited to replacing any malfunctioning video system components, readjusting mis-aimed cameras, gathering recorded data for offsite analysis, and, as time permits, analyzing the video records of off-normal events. Authentication will probably also entail examinations, tests, or code changes to assure that the encryption of the signals between the cameras and the computer has not been compromised. Protocol should allow a means of directly confirming that the signal comes from the expected camera. This could be achieved by a random replacement of some cryptographic keys associated with cameras and radiation sensors followed by immediate examination of that data. Although cryptographic keys could be broken the short time

between the change and inspector examination of data precludes a problem. Another method is for one inspector to observe other inspector in a near-real-time picture or a carefully logged times during a walk through. An ability to change cryptographic keys in the field could be detrimental and a potential spoofing method.

5.3.3 Radiation Sensors

The radiation sensors in this section are gross-count sensors for area and portal monitoring. These comments do not apply to the AMS or RD systems, only to radiation sensors employed as part of the FMS to detect presence or movement of SNM containers within the FMSF. There are a number of potential roles that radiation sensors might play depending on the types and mounting locations agreed to with the facility host. The primary purpose indicated in the FMS TSOW is as a trigger to increase the frame rate of the video surveillance. In addition, these radiation sensors can be used to track canisters within the FMSF especially if the portal sensors indicate the direction of motion. Radiation tracking could be considered another layer of protection to complement TIDs and video. The most likely agreed role will be to monitor portals and doorways. Radiation sensors may also be allowed above the massif where they can detect the opening of nests and/or the removal of containers from the nests. Radiation sensors may also be temporarily or permanently placed in massif vent tubes to monitor the presence of nuclear materials while they are in the nests.

Design Considerations:

Unless shielded or otherwise rendered inoperative, these radiation sensors will be able to give reliable indications of when canisters containing fissile material are present. Thus, they will be useful video surveillance triggers. However, as gross-count sensors, they cannot be expected to distinguish weapons material from non-weapons material so it must be assumed that radiation sensors are subject to false positives from non-weapons-material radiation sources. However, the presence of non-weapons-material sources should be considered an off-normal event worthy of video surveillance and not really a false alarm trigger.

The portal sensors are desired to be somewhat directional and aimed across a doorway. The directionality reduces the background rate due to other canisters staged in the room and increases the ability to determine the direction of movement through the portal. For example, a pair of neutron sensors mounted on opposite sides of the wall through which the canister passes can use the thick concrete wall as the shield which enables the temporal signals to distinguish which side of the wall the source is currently on and hence the direction of motion. The asymmetrical spatial signal introduced by the wall is an important means of avoiding being spoofed by a source approaching and leaving a symmetrical sensor from the same side. It would be easy to reduce sensitivity to room background by shielding the active neutron sensor element with thick slabs of polyethylene in directions other than across the doorway. The background rate will depend largely on the variable location and number of nearby canisters, so complex modeling of the portal scenario may not be necessary.

Area radiation sensors on the ceiling of a processing room or the massif would likely be non-directional except for the shielding incidentally due to the massive concrete ceiling. These sensors will only provide an indication of the presence of radiation within the room in excess of a set threshold. It would be unrealistic to expect area radiation sensors to detect attempts to substitute one container for another.

Any attempt to track canisters to nest locations within the massif with area radiation sensors will be difficult. The large concrete room will be a neutron cave with a large population of scattered neutrons. Thus, there will be a component (about 30%) of the neutron signal that will be somewhat uniformly spatially distributed. These scattered neutrons will have lower energy and be more readily detected by thermal neutron capture than unscattered neutrons spatially distributed with geometrical information related to the source. There are much easier methods of tracking the canister to the nest:

- Video surveillance of the crane control console where the crane position is displayed to high precision
- Tapping off the crane position sensors
- Labeling the nest covers and noting the position from an overhead video camera
- Scaling the range to several fixed video cameras from the apparent canister size

The desirability of tracking canisters to individual nests will depend of the regime requirements. In one possible regime, the inspectors may be able to monitor nest loading and unloading operations directly and place seals on full nests. In another possible regime, it may only be necessary that the canisters remain within some perimeter.

If inspectors are permitted to temporarily place radiation sensors in the massif ventilation tubes, those sensors might be able to sense the presence or absence of canisters at each of the eight expected storage elevations. Signals from nearby nests will likely contribute to each measurement and require probing multiple tubes to discover a single missing canister. Indirectly this scheme might detect the removal of one or more containers from one of the surrounding nests without opening any nests. If radiation sensors are occasionally allowed in the ventilation tubes, the design should clearly show the signal pathway to the FMS computers. The use of radio telemetry for the data signals may be problematic.

The sensitivity of all radiation sensors should be such that sufficient signal counts are acquired during a typical transit time through the field of view to achieve at least a 5-sigma increase over background. When the net signal equals the background count, the observed count doubles and one generally has more confidence in the detection than if the increase is only a fraction of the background count. If the background produces 25 counts in the time-of-passage interval (e.g., 1 to 5 seconds), the Poisson standard deviation is 5 counts. Thus, a signal doubling background would be sufficiently significant from a statistical viewpoint. The minimal useful sensor area and efficiency will yield 25 counts from a canister passing by.

The algorithms used to determine a trigger condition should use either the median count rate of the previous several minutes of data from that sensor or some decaying average value covering several minutes. These algorithms are not difficult to implement, but require local storage for up to 10 minutes of radiation data in the processor used to determine if a radiation-based trigger signal is warranted.

Neutron sensors are generally more useful for detecting the passage of plutonium because the neutron background is low and very stable compared to the gamma-ray background. Other moving sources of neutrons are very unlikely in the FMSF environment and should be monitored by video if they occur. However, the highly enriched uranium (HEU) loaded canisters will not be strong neutron sources. A gamma-ray sensor would be necessary to track HEU canisters. The gross gamma-ray sensors may be susceptible to false alarms due to non-canister radiation sources (e.g., luminous dial watches, thorium, etc.) and to shadowing the thorium activity in the opposite wall.

As with the video system, it is necessary to authentic the radiation signals in the sense of proving that the signals come from the expected sensors rather than elsewhere. Some means of controlling the vulnerability of the system to signal interception and spoofing is required. Since the data rate of the radiation signals is much less than the data rate of video signals and more random in data content, use of the same encryption scheme for the radiation sensors may not be warranted. Thus, any encryption or a digital signature scheme for the radiation sensor data should be carefully defined in the design and separately evaluated.

Installation Considerations:

As with the video system, time for installation inspections is likely to be limited so activities should be prioritized. If radiation signals are encrypted, less time will be devoted to assuring integrity of cable runs so that more time can be spent conducting sensitivity tests using calibrated sources to assure that the sensors as installed are able to detect sources at specified ranges, angles, and strengths with assumed levels of shielding. In addition, visual and electronic tests will be conducted to look for hidden switches. The FMS radiation signal readout should allow the inspector to monitor time-tagged radiation signals in near real-time so walking a radiation source through the facility while carefully logging the time when passing various sensors confirms signal labels, lines, and sensitivity.

Operational Considerations:

Since time on-site is likely to be needed mostly for container verification, authentication of the radiation-sensing system during visits should consist of replacing any defective system elements, performing calibration tests on randomly-selected sensors, and gathering recorded data both at sensor enclosures and the central computer for analysis and correlation with video and other data. Whether this analysis can be completed onsite or not depends on the number of triggering incidents between visits and the number of inspectors on the team. It also depends on protocol allowing radiation data to be removed from the site, which is highly desirable. During a two-month operational period, a large number of radiation trigger events will occur if canisters are being processed. Each canister loaded into the massif will pass several radiation portals in route to the massif. Consideration of each radiation trigger event might require comparing the radiation log to the movement log and the video records. Individually analyzing all radiation triggers in a manual fashion during a monitoring visit will be problematic.

5.3.4 Control/Logging and Review Computers

The FMS contains several computes located at individual sensors and at the more central nodes of the proposed network. All the considerations (contained in sections 3.3 – Computers and 4.0 – Software) apply to the computers and software controlling the FMS for both data collection and review. Additional FMS-specific considerations are listed below.

Design Considerations

Minimum complexity consistent with desired functionality should be the design goal for the computer systems. The system should not be so complicated that an inspector conversant with computer use cannot readily be trained to understand the system architecture and software modules. The inspectors will likely not be highly trained computer professionals. It would be better, in the opinion of the FMS authentication team, to rely more on inspector interaction with the FMS and as little as possible on software features.

The FMS has massive amounts of disk storage to store data collected during the interim between inspector visits. It is recommended that the control software be stored on PROM rather than on magnetic media to reduce the opportunity to covertly change the control software. This also reduces system vulnerability to a mechanical failure in an overworked disk drive or accidental overwriting. PROM storage of the control software is consistent with the AMS and RD design specifications.

The amount of memory required for storing several months of video and ancillary data from the many cameras and sensors will be huge. In fact the storage requirements may be a pinch point in the system design, which determines operational parameters like frame rates. The designs and specifications should include a quantitative estimate of the non-volatile storage requirements. The data transmission rates especially for video data are also expected to be a design pinch point requiring detailed evaluation during the specification and design phases. The designs and specifications should include a quantitative estimate of the data handling capacity of proposed I/O subsystems.

The proposed design suggests that sufficient memory be available to store video at the highest triggered data rate for several months. This is a fine fail-safe approach to prevent loss of coverage if the system continually triggers a high rate of data storage. However, if that storage capability is present, it might as well be continually used. This might reduce system complexity by eliminating trigger pathways.

The central data-collection computer and data-collection network should not be used to trigger video storage at higher frame rates. It is simpler to locally provide trigger signals and less susceptible to a common mode failure at the central computer. The use of the network as a trigger pathway requires linkage of the radiation collection computer and the video collection computer at a high level. The failure of this linkage would disable the entire video triggering system in contrast to only disabling a few cameras if a local trigging pathway were used.

The proposed RS-485 communication pathway between the video camera and the data-collection computer has a 5-second per frame capability. This throughput is low compared to the desired functionality. The design and specifications should carefully consider, propagate, and document this inherent limitation.

The automatic collection of data planned for Phase II should be implemented during Phase I. Manual collection of the data from the cameras and other local storage is a waste of the inspector's time.

Remote calibration of sensors using the central computer is a planned Phase II enhancement that we believe is a bad idea. With solid-state electronics, the needs for sensor re-calibration are much less than in years past and we would prefer that the calibration of a sensor could not be disturbed without breaking the seal on its enclosure and physically adjusting it.

The sophisticated computers required to support the FMS should be selected with a careful view to export control restrictions. It may be necessary to scale back the level of computer technology or to arrange an exemption from export control restrictions. Selection should also be based on the availability and shareability of detailed documentation.

Installation Considerations

The computer system will be vulnerable to both hardware and software tampering during installation. Maintaining physical control of the computer system will not be easy during this time, but keeping the computer cabinet and all peripherals sealed when observers are absent during installation should be possible. Guarding effectively against any software tampering may be practically impossible, so procedures should be in place to log all software modifications and make a complete copy of the final as-installed system software for offsite analysis. A random selection scheme to provide the monitoring party with exact duplicate copies of all software bearing components is highly recommended. Once the system is operating correctly, a final inspection should be made of the enclosures and data cable runs looking for hidden trapdoors and/or switches that could be used to compromise the integrity of the system.

Operational Considerations

During the period between inspections, the US should review the as-installed software and may decide an upgrade is required. If upgrades are made, changes must be subject to change control with exact duplicate copies provided to both parties well in advance of any modifications. The advance copies allow inspection and private examination prior to any joint installation at the beginning of the designated inspection visit. At installation, a random selection scheme will be used to provide the monitoring party an exact duplicate copy of the host-supplied software or software bearing component.

5.4 Other FMS Concerns

5.4.1 Data-Sampling Plan

The data-sampling plan used to select canisters for measurement by the AMS during inspection visits is crucial to the overall success of the regime. The canister population that is the basis for the statistical sampling has to be controlled to some degree for the statistical sampling to be meaningful. Clearly, if all the sampling performed before the FMSF is half loaded can not usefully address canister contents yet to be delivered. The authentication team will address concerns regarding a viable sampling plan in the process of authenticating the entire system. The sampling plan must address storage of measured and unmeasured canisters and what fraction of each subgroup is measured during each inspection visit to most efficiently achieve confidence in the results (see Appendix A.5.4.1). The sampling plan must also address the procedures for handling false canister failures because that will strongly affect the number of visits required before discovering a fractional diversion. If a canister fails due to measurement error it is desirable to remeasure it rather than raise the threshold for the number of failed canisters necessary before a diversion concern is raised. The threshold must be higher to accommodate erroneous failures than necessary if measurement error failures are adequately resolved. Since the number of samples per visit are small, Poisson statistics rather than Gaussian statistics should be used as the basis.

5.4.2 Encryption Schemes

The use of encryption schemes for handling video signal authentication may be problematic. The encryption scheme will have to be open and available to both parties (see Appendix A.5.4.2). Russian law and export control requirements must be considered during system specification and design.

6.0 AMS Specific Authentication Considerations

This section provides design guidance on producing an AMS that is easily authenticable within the timeline of the Mayak FMSF project. Additional guidance can be found in Sections 3.0 and 4.0 of this document.

Refer to Section 2.0 of this document for basic authentication design guidance and best practices.

The funds for designing, constructing, and authenticating these systems come from the same limited source. Therefore, it is important that the cost of design, construction, functional testing, and authentication be considered for each decision. For example, it may be cheaper to procure and easier to design software for a windows operating system, but the complexity and associated cost of the authentication task would adversely affect the FMSF timeline and budget.

6.1 General Guidelines for Attribute Monitoring System

6.1.1 Essential Requirements for an Authenticable System Are the Following:

- The system must be designed in a modular way to allow for maintenance and random selection of subsystem (e.g., MCA) and board level (i.e., individual circuit boards) components.

- All sensor systems must be completely transparent in function. If there is reasonable functional capability for a component to alter the measurement result, the authentication team requires sufficient information to verify that the measurement result is properly processed through that component under all circumstances. Assurance of credible performance requires precluding “hidden switch” triggering by completely understanding the electronic and software design. Transparency with complete documentation shall be required to prevent exploitation of all recognized potential hidden switch mechanisms. In addition, conservative operation of every device capable of altering the results shall be required to minimize the capacity for altering results. For example, to ensure that a multichannel analyzer is properly processing the last-measured data, all buffers within the MCA shall be cleared prior to the start of each measurement to prevent any spectral substitution.

- The monitoring party must have complete knowledge of system status before each measurement campaign, and significant prior examination of the system (or a duplicate replacement based on a random selection scheme). For example, all jumper and adjustment settings must be verified, or access to the system after initial authentication must be precluded. Good design practice minimizes or preferably eliminates the use of jumpers and switches. Also, all device programming must be demonstrated to match the corresponding baseline programming in the documentation before each use.

- All physical enclosures must provide for the use of TIDs (tags and seals) or the use of built-in tamper-indicating features. In addition, the enclosures must satisfy appropriate RF shielding standards, eliminate ground loops, and meet generally accepted standards.

- There must be rigorous monitoring and tracking of the design, including freeze dates.
- Within the context of the Mayak FMSF project, the Authentication Team should participate in design reviews and furnishing guidance toward design for authentication.

6.2 Hardware Guidelines for Attribute Monitoring System

6.2.1 Essential Hardware Documentation

The following documents are needed to perform accurate authentication of the system. The documentation in all forms provided must be clear and readable.

- System Functional Description Document
- Preliminary Hardware Design Document (Conceptual Design)
- Final Hardware Design Document (Detail Design)
- Hardware Test Plan and Test Procedures Document
- Hardware Configuration and Quality Assurance Plan Document with Detailed Circuit Schematics
- Functional Descriptions, Operating Procedures, Calibrations Procedures for all operational modules
- System Documentation including:
  - Detailed Parts List for all Circuit Schematics
  - Manufacturers' Data Sheets for all components (integrated circuits, resistors, capacitors, inductors…)
  - Detailed Cabling and Wiring Interconnections Diagrams
  - Firmware code for all programmable devices (μControllers, PLDs, PROM, Flash,…)
  - Complete vendor documentation of all procured hardware – such as operating procedures, calibration procedures, circuit diagrams, parts lists, embedded code in any programmable device, packaging mechanical drawings, …
  - Procurement history for all components, including lot numbers and production runs
  - Circuit-board layout files (e.g., Gerber Files)
  - Mechanical Drawings of all Electronic Enclosures
  - Circuit description of electrical feed, cabling, and UPS
  - Schematics, layout, masks, and production-run data for all ASICs custom manufactured for this system.
- Hardware Acceptance Test Results
- Hardware Operational Test Results

6.2.2 Essential Hardware Requirements

- All hardware and system designs must be well documented and easily understandable. Code (including all firmware), schematics, block diagrams, and other design documentation must be provided in English, preferably in electronic form, and with a hardcopy backup.

- All adjustable or programmable devices or their enclosure will need to be tagged and/or sealed. One-time programmable devices with the capability to readout the current programming are preferred to devices programmed at power up.

- All custom circuits must be realized on printed circuit boards; preferably these boards will be free of buried conductors for ease of inspection. Since size is not an issue, two layer boards are preferable to boards comprised of three or more conducting layers. Change orders must be fully documented. Any necessary modifications should be implemented in a new board, eliminating jumpers and switches.

- Production runs shall be sufficient to produce boards and components for the AMS, spares, multiple copies for inspection, and archived copies.

- Components shall be purchased in sufficient quantities to furnish spares throughout the expected lifetime of the AMS. Spare components shall be stored in a tagged and sealed enclosure. The random selection process will consume considerable spares, and this must be taken into account.

- Programmable devices not subject to a random selection scheme should be soldered to the circuit board. Those subject to device-level replacement under a random selection scheme should be socket mounted to facilitate that scheme.

- The hardware must be modular to facilitate testing and random selection. The ability to remove or randomly select subsystem (e.g., MCA) and component level (i.e., individual circuit boards) pieces is essential.

- All hardware and computer boards need to be laid out for easy physical/visual examination. The ability to photograph both sides of all circuit boards is essential for authentication.

- All circuits should be laid out for easy inspectability. Techniques with inaccessible leads, such as flip-chip technology using ball-grid array components, should be avoided.

- Whenever possible, integrated circuits that are not subject to random selection should be specified as soldered, surface-mount components rather than packaged components in a socket. If the component is subject to random selection the component should be affixed using a socket.

- The electronics and hardware must be robust and capable of withstanding the expected operating environment.

- Appropriate system packaging shall be required to ensure that signals cannot emanate from, or penetrate into the system. For example, approved RF shielding practices should be followed.

- Original manufacturers' names and part numbers must be retained and visible on all integrated circuits. Some companies alter or change this information. The parts list will also contain all the original vendor's identification along with current markings.

- All non-volatile memory should be identified in the documentation along with the prescribed contents for that memory. All unused sections of non-volatile memory shall be properly and verifiably disabled and/or erased.

- A method for compiling a golden or reference copy of all firmware and verifying that it matches the firmware existing on the system is essential.

- Circuits containing programmable devices should be designed so these devices cannot be reprogrammed in circuit. For example, on some microprocessors or flash memories, the voltage on one line must be raised substantially above the operating voltage for the chip to be reprogrammed. The design should make this impossible in a manner that is readily inspectable.

6.2.3 Desired Hardware Requirements

- Identical and modular hardware components should be used across the system.

- The use of FPGAs is preferable to a customized ASIC specific to this project. The FPGA is preferable when the firmware can be tested and verified. An OTP device is preferable to a random-access memory (RAM) based device since it would be more difficult to change the contents of this device after it is authenticated. To ensure that the contents are not changed, the ability to reprogram the device should be disabled, but the ability to verify the contents of the device should be left intact.

- The use of discrete components (i.e., operational amplifiers and lower level discriminators) is recommended for the analog front-end rather than mixed-signal integrated circuits.

- The complexity of the hardware should be minimized, and all extraneous functionality should be eliminated. For example, if one computer is capable of performing all required functions, it is preferable to restrict the design to one computer rather than use multiple computers. If multiple computers must be used, it is preferable to restrict the design to one specific computer type (i.e., same vendor, model, and revision) to avoid authenticating different hardware sets, BIOS software, and operating systems.

- "Dumb" hardware is preferable where possible. For example, if the design does not need a UPS capable of communicating, then use a version without this extraneous feature.

- An external display for use during open or unclassified mode is desired.

6.3 AMS Software Guidelines

6.3.1 Essential Software Documentation

High-level descriptions of various software modules and various design documents are very useful in providing instructions and conceptual explanations regarding the functionality in each module. However, if a covert feature is deliberately inserted into a module, the overview documentation probably will not mention it. In the search for covert features, the most useful documentation is that which is forced to include information on all features, both overt and covert. For software, the commented source code is the highest level of software documentation that is forced to include all covert features. However, that requires that the completeness and accuracy of the source code be independently verified when the provided source code is built into executable code, which exactly matches the installed executables.

The following list of documents is deemed the minimum needed to perform accurate authentication of the system:

- System Functional Description Document
- Software Requirements Document
- Preliminary Software Design Document (Conceptual Design)
- Final Software Design Document (Detail Design)
- Software Test Plan and Test Procedures Document
- Software Configuration and Quality Assurance Plan Document
- List of system software, including operating system, compilers, databases, etc.
- List of computer hardware, including CPU, hard drives, peripheral equipment, etc.
- Software Coding Standards Document
- Software Installation and Maintenance Plan
- System's Users Guide Document
- Software Source Code (machine-readable format)
- Software Executable Code identical to that loaded on the system (machine-readable format)
- Build instructions to generate an identical executable from the source code
- Duplicate copies of all compilers, libraries and other objects necessary to independently build an identical executable from the source code.
- Explanatory documentation of algorithms and analysis techniques used (detailed rather than summary)
- All documentation provided with commercially purchased software
- Software Acceptance Test Results
- Software Operational Test Results

6.3.2 Essential Software Requirements

- All software must be transparent and well documented. The source code, including comments and documentation, needs to be provided in English, and preferably in electronic form and hardcopy backup.

- The use of generic operating systems should be minimal or nonexistent, and a self-bootable application is desirable. If an operating system is used, it should be generated using an open-source, commonly available compiler. This should allow for selectively generating the system code by specifying input variable parameters and/or modules to be included, and the source code should be openly available.

- There should be early agreement on the source code and version, including comparison of working version and reference copies.

- The build date of all software components shall be easily extracted and verifiable.

- The software design and documentation should conform to all reasonable and applicable clauses of ISO standard ISO/IEC 15409:1999.

- The software shall have extraneous functionality removed.

- The software shall have unused or dead code removed.

- The software shall have unused variables removed.

- The use of some commercial software (e.g., compilers or assemblers) available for independent procurement is acceptable **if** a valid means of verifying that it is not corrupted can be agreed to by all parties. For example, one possible method could be an anonymous purchase and either a digital signature or byte-for-byte comparison for each copy; however, open source code is still preferred.

- The prescribed values of all interrupt vectors and a description of their use shall be provided in the documentation package. All unused interrupts should be both 1) masked off by the software and 2) hardwired in a state that precludes their covert use.

- All data formats shall be fully documented with the numeric format of the value completely specified.

- All error conditions and their causes must be explained. The indications one would expect and any corrective actions to be taken need to be explicitly described.

- The use of referenced libraries must be avoided. Libraries shall include only those functions required and referenced by the application. Source code shall be provided for all library routines placed into the system software.

- A method for compiling a golden copy of every piece of software and verifying that it matches the software existing on the final system is essential.

- The software should be modular to facilitate authentication.

- The software shall not be self-modifying, and parameters used that are considered to be fixed or constant shall be read-only and non-modifiable.

6.3.3 Desired Requirements

- The use of overlays to allow large codes to fit within limited memory is to be strongly discouraged.
- Software should be written to conform to code (I-Bank) and data (D-Bank) segment separations. I-Bank sections should be read only.
- All software written for this application should be written in the least complex way, non-recursive, and the final product should be single threaded.
- Only one compiler for each programming language should be used throughout the system. The use of an open-source compiler or assembler is preferable.
- Open source software is preferred.
- Execute in place (XIP) software is preferred as a means of precluding any modifications while loading or executing the software.

6.4 AMS Operational Guidelines

6.4.1 Essential Requirements

- A set of reference, unclassified calibration sources corresponding to the specifications being generated must be available for use during authentication. These sources should address the need to verify operation at the individual component (i.e., HPGe detector), subsystem (i.e., attribute measurement from a HPGe subsystem), and system (complete AMS) levels. These sources would be appropriate gamma-ray and neutron sources, plus sources required for authenticating complete system performance.
- A combination of appropriate engineering methods and/or protocol shall be put in place to preclude excessive interference from other nearby sources while measurements are being conducted.
- A tagged and sealed enclosure for the calibration sources must be supplied.
- Appropriate engineering methods shall be used to ensure that deadtime and pulse pile-up do not produce visible spectral distortion.
- The analysis software and algorithms shall be robust against reasonable perturbations in stored material or matrix. These effects may include, but are not limited to, in-growth of other isotopes such as ^{241}Am, variation in the composition of polyurethane inserts, and variable backgrounds due to differing item activity. The NMC analysis shall be robust against removal of the boron loading from the surrounding shells (M perturbation) and against beryllium and/or fluorine contamination (alpha perturbation) with standard mass loading.

7.0 Conclusions

Based upon lessons learned from previous work in connection with the Information Barrier Working Group and the FMTT Demonstration, it is clear that:

- The design of an authenticable system is achievable.

- Complete system transparency requires complete documentation.

- Authentication tests described in this document can result in robust software performance without resorting to prescriptive or sole-source specifications.

It is also clear that design for authentication should be a goal of the various design teams. The technical challenge of producing measurement systems is not in achieving operational functionality but in producing a system that can satisfy all the concerns of both the host and the monitor parties.

8.0 Recommendations

Design teams are strongly encouraged to include authentication guidance into any systems being constructed for arms-control and non-proliferation applications or demonstrations. PNNL recommends the inclusion of these guidelines in the statement of work for the design and development of Russian Federation systems.

9.0 References

Dreicer, J. 2001. *Facility Monitoring System (FMS) Project, Presentation for Briefing by Tom Rutherford*, Los Alamos National Laboratory, Sandia National Laboratory, and Pacific Northwest National Laboratory.

General Accounting Office (GAO). 1998. "Nuclear Nonproliferation: Uncertainties With Implementing IAEA's Strengthened Safeguards System." Letter Report, GAO/NSIAD/RCED-98-184, Washington D.C.

Hsue, W., et al. 2000. *Facility Monitoring, Surveillance, and Verification: Safeguards and Security for the Russian Federation Fissile Materials Storage Facility*, LA-CP-00-460, Los Alamos National Laboratory, Los Alamos, New Mexico.

Hsue, W., et al. 2001. *Facility Monitoring, Surveillance, and Verification: Safeguards and Security for the Russian Federation Fissile Materials Storage Facility, Volume II: Regulations, Functional Requirements, and Conceptual Design for Domestic MPC&A and Verification System,* LA-CP-00-460-II, Los Alamos National Laboratory, Los Alamos, New Mexico.

Mangan, D., J. Matter, I. Waddoups, M. Abhold, and P. Chario. 2001. *Layered and Segmented System Organization (LASSO) for Highly Reliable Inventory Monitoring Systems (IMS),* Sandia National Laboratory, Albuquerque, New Mexico; Los Alamos National Laboratory, Los Alamos, New Mexico; and Oak Ridge National Laboratory, Oak Ridge, Tennessee.

Dr. Neumann GmbH DCM-14.

Tanner, J. T. H. A. Undem, B. A. Roberts, J. R. Griggs, and S. L. Pratt. 2001. *TID Performance Testing in Support of the Mayak FMSF,* Pacific Northwest National Laboratory, Richland, Washington.

9.1 Bibliography

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

Fuller, James L. 2000. *Information Barriers,* PNNL-SA-33328, Pacific Northwest National Laboratory, Richland, WA.

Hatcher, C. R., S. T. Hsue, and P. A. Russo. 1982. *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.

International Atomic Energy Agency (IAEA). 2001a. *Procedure for the Authorization of Equipment Systems and Instruments Software for Inspection Use*, Department of Safeguards, February 2001, IAEA, Vienna, Austria.

International Atomic Energy Agency (IAEA). 2001b. *Working Document for IT Security Evaluation Criteria for Safeguards Equipment Systems*, MSSP Task NT E 1272, Working Draft, Version 1.2, March 15, 2001, IAEA, Vienna, Austria.

Information Barrier Working Group (IBWG). 1999. Joint DoD/DOE IBWG, *Functional Requirements for Information Barriers*, May 1999.

International Standards Organization (ISO). 1999. "The Common Criteria for Information Technology Security Evaluation" 15408/1999, Evaluation Assurance Levels, Geneva, Switzerland.

Appendix A

Comments and Background Information

The contents of this appendix provide additional elaboration on selected items related to authentication. The item number refers back to specific sections in the main report.

A.3.1.1 Interference from Nearby Sources

A reasonable authentication test would require less than a prescribed error (perhaps 5%) in plutonium gamma-ray peak amplitudes due to the maximum amount of nearby plutonium allowed by protocol. Also, passive shielding surrounding all but the sensor face will collimate the field-of-view and reduce the baseline under peaks of interest due to 1) unexpected nearby radionuclide sources and 2) natural background radionuclides. Tungsten or other dense materials (e.g., lead, copper) are reasonable shielding materials for gamma rays, subject to confirmation that decay and neutron-induced peaks do not interfere with peaks of interest for the plutonium attributes. It may be necessary to install tamper-indicating devices on the sensor shielding.

This authentication input is designed to place a reasonable limit on the effects of environmental changes due to nearby plutonium. When attempting to determine the plutonium mass from plutonium peak amplitudes, one cannot tolerate large errors in the peak amplitudes due to nearby plutonium. The specifications should set a reasonable limit in peak amplitude error as a means of specifying adequate shielding. A shielding specification can be expressed in alternate manners, but all with a view toward adequately blocking gamma rays from nearby plutonium. When using a neutron multiplicity counter (NMC) for the plutonium mass attribute, the corresponding tolerable peak amplitude error due to nearby plutonium should be determined based on acceptable errors in isotopics or plutonium presence. The error in an NMC plutonium mass estimate depends on the error in isotopics.

It is important to adequately shield the neutron sensors against nearby plutonium sources. The neutron shielding materials possibly used to collimate the Shielded Neutron Assay Probe (SNAP) neutron sensors or other possible singles neutron sensors will most likely be hydrogenous and may serve to enhance neutron detection efficiency. The authentication team will carefully examine the ability of possible singles-neutron detection schemes to accurately estimate the plutonium mass in the presence of nearby plutonium sources. The authentication of a potential NMC-based scheme will include demonstrating robustness against nearby neutron sources. Return to 3.1.1

A.3.1.2 Variable Aperture

An automatic variable aperture could be a viable information barrier tool that limits inferred classified information from count rates and distances. The host is free to use this variable-aperture feature; however, for a fixed and declared container loading, a variable aperture may not be needed and has some

undesirable features. One undesirable feature is the linkage between the aperture opening and the detection efficiency. If the minimum plutonium mass is determined from gamma-ray information that uses an automatic aperture, the software requires a variable aperture correction for detection efficiency. Authentication tests will evaluate the accuracy of the correction information to preclude an obvious method of cheating on the mass. Elimination of the variable aperture greatly simplifies the system. An autonomous automatic variable aperture requires an additional input into the measurement-system computer. A computer-controlled variable aperture requires an additional output from the measurement-system computer. If this aperture feature is used and the analysis software uses a background measurement, the analysis requires some method to properly scale background plutonium peaks from nearby plutonium with the aperture opening. A reasonable authentication test could require less than a 10% error in background peak amplitudes and less than a 5% error in background-corrected plutonium peak amplitudes from the canister being measured. The mechanical and electronic implementation of the aperture illustrated by FMTT-AMS/IB[(a)] appeared authenticable, subject to complete documentation. The aperture should use the same materials as the shielding material. Return to 3.1.2

A.3.1.3 Attenuator to Reduce Count Rate

A reasonable authentication test would require less than some deadtime value, which produces no visible spectral distortion (e.g., peak broadening, after-pulses due to ringing, baseline-shape changes, energy shifts, etc.) due to pulse pile-up when viewed at a minimal lower level discriminator setting. The lower-level discriminator could be raised above the minimal level during normal operation to limit the energy window of interest or for other reasons. A maximum deadtime value between 10% (PU600) and 60% (Trusted Attribute Demonstration System [TRADS]) could be specified, but that may unnecessarily limit the Russian design. An integrated multichannel analyzer (MCA) using a digital reset scheme is more robust against high deadtime than an analog reset scheme. The storage canister (AT400R) may provide adequate source attenuation to avoid dead-time problems, but this should be demonstrated in the proposed measurement geometry. There will be a measurement design tradeoff between source-to-sensor standoff and the attenuation-disk thickness regarding the tolerable deadtime, the measurement duration, and the measurement sensitivity. Return to 3.1.3

A.3.1.4 Shared Signals

The high purity germanium (HPGe) sensor pre-amplifier generally has two independent output connectors. If additional outputs are needed, a signal splitter could be used. A reasonable authentication test would require no visible spectral distortion between spectra collected with comparable gain settings using all possible analog output combinations. A statistically valid comparison needs to be made. For example, one might require agreement within 4-sigma for at least 99% of the channels above the lower-level discriminator between two spectra. It would be permissible for the signal splitter to change the gain if that can be counterbalanced with the spectroscopy amplifier without significantly altering energy-calibrated spectra. Spectra should be independent of the status (e.g., on/off, gain settings) of the other system sharing the signal and free of any erroneous signals when the other system has major electronic problems. A signal splitter should not significantly alter the individual pulse shapes, and a logical

(a) AMS/IB = Attribute Measurement System with Information Barrier

authentication test would be to compare pulse shapes with and without the signal splitter. Distortion problems (e.g., rise time, fall time, clipping, undershoots, and ringing) should be made no worse by the signal splitter. The pulse width is especially important when operating in a high-rate environment.

The point at which the neutron signals are shared can be important. Neutron signals that have passed a discriminator and been converted to logic signals are less susceptible to distortion in a signal splitter than are analog signals. The neutron count rates from a standard source will be compared with and without the signal sharing. In addition, the neutron counts collected by the two systems sharing the signals should exactly match. Return to 3.1.4

A.3.1.5 RF Interference and Hidden-Switch Triggering

A radio frequency (RF) shield can be useful as an information-barrier tool, and the host is free to use this feature. However, authentication is concerned with remote-control possibilities. A reasonable authentication test would require no visible spectral distortion when the HPGe sensor is bombarded with RF energy over a wide frequency range (e.g., a radar gun and/or other RF source). Neutron sensors (^{3}He tubes) have a history of being sensitive to RF and radar emissions. Given that history, the authentication team will carefully check for any means of inducing extra neutron pulses and will test that the system can not easily be compromised by RF.

Authentication also requires that remote control via external signals (e.g., radio, optical, acoustical, etc.) to a potential covert receiver be impossible. Thus, the RF enclosure will be tested to show its attenuation capabilities. It will be necessary to install tamper-indicating devices on the RF shield. Return to 3.1.5

A.3.2.1 Complete Sensor Electronics

To aid in understanding, the following examples related to sensor electronics are provided.

The spectral histogram may be built in the MCA using a programmable logic chip, or the resulting spectrum may pass through programmable logic in route to the analysis computer. Depending on the internal programming of that logic, it may be possible to alter the data by either swapping in another data set or adjusting some channels. Thus, the authentication team requires the source code of all internal programming for that logic chip to determine if there is any means of altering the results and to determine potential methods of triggering such an alteration. This applies to programmable logic chips and custom logic chips programmed by the manufacturer to the users specifications.

A CPU within the MCA that is building the spectral data may be similar to a PC computer with basic input output system (BIOS), operating system, and application programs. Since such a CPU is physically capable of altering results, the authentication team requires the software source code and executable of all CPU programming (BIOS, operating system, and applications) to determine if there is any means of altering the results and to determine potential methods of triggering such an alteration. Since these software executables reside in Flash or erasable programmable read-only memory (EPROM) memories, which the designer can easily alter, it is prudent for the authentication team to rebuild and examine them.

The CPU within the MCA that is building the spectral data may be similar to the Forth engine used by Ranger, which internally contains operating-system-like code (e.g., Forth kernel) to interpret external Forth instructions. The vendor documentation on the Forth engine coupled with the Forth language documentation was adequate to evaluate the Ranger system when only the external Forth software was provided. The specifications should require selecting similar CPU components with a mass market and adequate vendor documentation, but could pass on requiring source code for internal coding. Three conditions allow passing on the source code. The Forth interpreter resides on the internal chip mask. The designer purchasing the standard microprocessor cannot readily alter this hardware resident code without destroying the CPU component. There is a mass market for the component that allows comparison to an independently purchased component.

Some CPUs contain hardwired internal microcode, which is not readily available to a user or readily altered by a user without destroying the CPU component. The specifications should require selecting similar CPU components with a mass market and adequate vendor documentation, but could pass on requiring source code for internal microcode. Return to 3.2.1

A.3.2.3 Continuity of Knowledge for State of System

External jumper settings can be verified by photographing the components or by a visual inspection of the components against a previous photograph. Internal potentiometer settings can be verified by voltage measurements. External potentiometer settings can sometimes be verified by visual inspection of dial readings, but it is difficult to visually verify screwdriver settings. Software settable parameters can be verified by numeric display when the software has been previously examined and verified as operating. The Canberra Inspector apparently uses an undocumented internal microprocessor for parameter settings. Proper validation of these parameter settings (e.g., high voltage and gain) might be alternately achieved via either voltage measurements or software quality-control analysis of each spectrum requiring consistency regarding a list of peak locations. If protocol limits such verification procedures, alternate means of implementing adjustable parameters or verifying the settings should be used. Return to 3.2.3

A.3.2.4 Front-End Electronics

It is useful to monitor the shape and height of pulses at the input to the discriminator section to verify both that the threshold setting is realistic and that the amplified pulse is not distorted. Some highly packaged front-end components may not allow sufficient access to intermediate signals. Mixed-signal integrated circuits are very difficult to authenticate.

The sensor electronics may possibly double count pulses due to line reflections or ringing. The sensor electronics may possibly miscount pulses due to weak signals driving a long line. The authentication team could statistically evaluate short counts to ensure that they follow Poisson statistics and that the results are credible. The authentication team could also examine scope traces to ensure that pulses successfully traverse long cables and properly trigger counters with very high efficiency.

An electronic calibration source (e.g., pulser) may be a useful functional-testing tool. This may require a means of disconnecting the sensor head and replacing the analog sensor signal with one from the electronic calibration source. The front-end circuits must be robust against over-voltage damage due to incorrect connections. The concept of allowing connection of an electronic calibration source may not be acceptable to the host certification process. However, it does provide valuable capability for more controlled and broader-based functional testing options. Return to 3.2.4

A.3.3.2 Unused Input/Output Ports

PC-104 CPU cards generally (e.g., Ampro 3SXi –386SX-based CPU used in FMTT–AMS/IB and Win Systems PCM-586 – 586DX-based CPU used in TRADS) have floppy disk and Integrated Drive Electronics hard-disk ports and interface lines, which are typically unused in a system with an information-barrier. There are several approaches to handling this extraneous functionality:

One could remove the existing connectors and ground several traces to disable these unused I/O lines. These extraneous lines can be more neatly rendered useless by inserting a connector that definitively sets all the unused I/O lines in some harmless manner (setting pins high or grounding them to avoid requesting computer attention). The desire is that unused I/O lines be hardwired to a fixed value so they are not available for covert signals.

These ports and interface lines could be used as digital I/O lines to control the PASS/FAIL light-emitting diodes (LEDs). The Indispensable PC Hardware Book 3rd Ed shows interface floppy-disk lines (page 787) and provides port addresses that control these lines (pages 817–821). Similarly for the hard disk, it shows line information (pages 881 and 886) and provides port addresses that control these lines and (pages 889–893). Normally, these disk lines are not used as digital I/O, but could be when using custom application software rather than the BIOS or operating system calls to control these lines. There is an advantage in using this extraneous functionality to avoid adding in extra PC-104 cards for digital I/O. Admittedly, the complexity of using these lines may exceed the complexity of authenticating additional I/O cards. The choice is clearly subjective rather than objective.

The extraneous ports can be declared useful for debugging the system and considered a feature rather than a problem. However, a means for preventing their covert use must be assured. Return to 3.3.2

A.3.3.3 Video Card

A PC-104 video card used by the CPUs of the FMTT-AMS/IB to drive temporary display terminals may be considered extraneous. The COM ports on the CPU cards could have driven display terminals and removed the requirement for another PC-104 board. Most PC-104 CPU cards typically contain two serial ports. PC-104 CPUs can easily be set up to use one serial port as the console during debugging and to provide alphanumeric display capability. This alphanumeric display is adequate for hash function and data output. Some display terminals (using only a serial port) can display graphical spectral data. Alternatively, the IB system could port the raw spectral data to an external laptop via the serial port when in open mode. The laptop could generate appropriate displays for open-mode visual analysis and could potentially store the raw data to aid offline to facilitate debugging of the analysis software with a

collection of failure cases. It is not difficult for the information barrier (IB) system software to accept only a limited number of input bytes to seed a hash function during an initial programmable read-only memory (PROM) verification and then limit serial port use to outputting blocks of data to the external laptop or terminal. Thus, it is easy to avoid requiring a video card. See later comments about output devices. Return to 3.3.3

A.3.3.4 Digital Input/Output Card

The PC-104 digital input output (DIO) card used in the FMTT-AMS/IB computational block computer had four serial ports and six DIO ports routed through a field-programmable gate array (FPGA), which was programmed at power up from a socketed non-volatile memory integrated circuit (IC). No provision for either 1) authenticating the design FPGA programming or 2) verifying that the correct FPGA programming was operational was provided. Both features must be provided if a similar DIO card is used in an authenticable computer. Source code should be made available to the authenticating team, both to evaluate the FPGA design and to program an identical FPGA for direct comparison. The One-Time Programmable (OTP) FPGA should have a means of reading out the internal programming for a bit-by-bit comparison to the monitor's "golden copy." The guidance is to use the minimum number of serial ports by minimizing the number of computers to be interconnected (1 is desired). An extra parallel port card might have provided sufficient DIO to control the FMTT data barrier because it was not necessary to use two bits for each Pass/Fail pair. It is possible to use the ON/OFF state of one bit to pass the PASS/FAIL information and then light the LEDs solely when the "measurement complete" bit was set. The interrupt capability is not justified for the DIO controlling the display, and such capability should be considered extraneous. If it is impossible to avoid the DIO interrupt feature by selecting an alternate DIO card, the interrupt feature should be disabled via hardware (e.g., tying the interrupt line in a state to prevent any requests—grounding an edge-triggered interrupt line prevents any other location from pulling the line "low" to initiate an interrupt). Return to 3.3.4

A.3.3.7 Verification of BIOS and Application Software Match of "Golden Copy"

The random-selection scheme includes selecting one PROM for use and another for the monitor's private examination. Another software verification method uses a hash function, which requires 1) input of monitor-selected seed data and 2) an alphanumeric display of output strings. Both random-selection and hash-function comparison are viable methods for confirming the contents of a socketed PROM containing the application software. The hash-function comparison is preferred for use in the field because to achieve the correct comparison value, both the algorithm and the data must be correct. This mitigates the scenario where the comparison computer and/or comparison software is compromised. If the PROM chips can be randomly selected and removed to a monitor-controlled location, the bit-for-bit comparison is preferred because it is a one-to-one comparison. Return to 3.3.7

A.3.3.8 Input Devices and Covert Signals

If limited push buttons are used, the button should set a flip-flop via its clock input, and the computer should subsequently clear the flip-flop via the reset/clear input. Alternately, the push button should set a monostable flip-flop for a predetermined but relatively long duration. This prevents the duration of a

button press from containing compromising information. The sequence of button pressing should be controlled by protocol. The interval between button pressings should also be controlled by protocol. If a keyboard or pointing device is used to initiate a hash-function test or provide any other information during a possible open mode, it should be disconnected before entering classified mode. The authentication effort will seek out for removal any means of operator and/or host input not explicitly permitted by protocol. Return to 3.3.8

A.3.3.9 Output Devices and Classified Information

The concept of operating the system in dual modes (classified and unclassified) may not be acceptable from an information-security viewpoint. This dual-mode scheme is often considered as periods processing where an unclassified processing period can follow a classified period when the computer is powered down between periods. This section address output consideration under a possible dual-mode concept. The host's certification process must be satisfied by the implementation. If an alphanumeric display is not allowed during the classified mode, all but PASS/FAIL lights could be disconnected before entering the classified mode. If an alphanumeric input is not allowed during an open mode, hash-function verification of the software becomes problematic. If alphanumeric and/or graphical output is not allowed during open mode, the value of open mode is marginal. The concept of additional or different I/O being allowed during an open mode to display intermediate results or plot spectral data is a very useful confidence-building tool available to the host, but is not fundamental to an information-barrier system. Discussion occurred regarding the capability of a permanent liquid crystal display (LCD) to protect classified information in comparison to the simple ON/OFF states of an LED array. An insider could more easily use the more versatile LCD hardware capabilities to covertly pass information, but open and examined software could easily prevent the passage of covert data. The temporary connection of a video display terminal or an external laptop computer for use as a display is not fundamentally different than the temporary use of an LCD in terms of the information-barrier risk of divulging classified information. If the host provides the external display device, the monitor should authenticate the device. It would be easy for the external display to project erroneous authentication/calibration information in accordance with a script. The host's choice of display hardware and display philosophy depends on willingness to accept software protection measures over hardware limitations. Return to 3.3.9

A.3.3.10 Debugging and Authentication Using Raw Data

Several schemes exist for recording the data. For example, a DiskOnChip could temporarily replace the PROM, or a disk drive (e.g., floppy or ZIP) could temporarily be connected. This recording means would be removed during any two-party inspection procedure involving classified materials. This feature only requires that some method of recording data not be designed out of the system. With the PC-104 architecture, this feature could be implemented by adding an additional board to the stack if necessary. It could also be implemented by plugging in an external floppy disk to the CPU board. This feature may require that the software always write out data to a device, but it could be the "NUL" device in classified mode. Alternatively, a laptop computer could be used to replace the information-barrier-protected computer system to evaluate hardware and software modules. TRADS effectively used this method where the laptop ran the same analysis software out of a batch file, but added an extra routine to save the data file to disk. A special input cable to allow a second computer to eavesdrop on the serial input stream

during authentication testing might be viable. Modification of an authenticated and fielded system should be avoided. Return to 3.3.10

A.3.4.1 Simplest Data Barrier Preferred

The flip-flop aspect of a hardware data barrier (used to hold results in simple hardware to reduce vulnerability to software changes) might be considered extraneous in the FMTT-AMS/IB implementation because it was easily possible to subvert its functionality by either the computational block software or the DIO card firmware. If this data-barrier concept is retained in the design, it should be clearly necessary and explained clearly. The hardware data barrier could be viewed as a simple non-programmable black computer.

The hardware data barrier converted electrical signals into optical signal for transmission to a stand-alone display. The stand-alone display used power from the main unit and converted the optical signals back to electronic signals to power the output LEDs. The stand-alone display might be considered extraneous because LEDs mounted on the main IB box would suffice. If this concept is retained in the design, it should be clearly necessary and explained clearly. Return to 3.4.1

A.3.4.4 Custom-Programmed Logic Chips

The programming in an FPGA can be readily verified if properly designed. If the original programming source files are available, the binary programming file can be confirmed as a golden copy. Some once-programmable FPGAs allow readout of the internal binary programming information in a serial fashion. Some FPGAs are programmable at power-up from a serial PROM. It may be necessary to require that FPGA programming be connected to the CPU in a manner that allows confirmation that it matches a golden copy imaged in the main PROM and independently verified perhaps by a hash function before each use. It may be possible to connect the FPGA to a serial port that the CPU could use to either program the FPGA or read out the FPGA programming. Verification of the programming in a general application specific integrated circuit (ASIC) may be more difficult. It is not clear how to read out the internal programming when a custom chip is programmed with a mask during manufacturing. The problem is that the host may have procured two visually identical ASICs that have different functionality and could be swapped. The specifications should recognize that it is more desirable to use custom components that allow verification of the programming than the type that does not. Thus, the use of ASICs without readout capability is discouraged. Return to 3.4.4

A.4.1.1 Operating Systems

Using Microsoft Windows is very undesirable because it is far too complex, it cannot easily be stripped of extraneous functionality, it is known to have undocumented features, and source code is not available. Other such complex, integrated, general-purpose operating systems are equally unacceptable.

Using Microsoft MS-DOS is very undesirable because source code is not generally available, and alternative DOS-like equivalents with available source code exist. However, if MS-DOS must be used, all extraneous functional units (e.g., unused external functions) must be removed from the disk or PROM

containing the operating system, and some valid means of verifying that the operating system is not corrupted must be presented and agreed to by all parties. Recompiling the operating system kernel to remove extraneous internal functionality is an option with both positive and negative aspects, but avoiding all the unused independent external programs is prudent.

Using ROMDOS by Datalight could be made more authenticable by stripping out all unused functionality and providing the complete source code for all software included in the system. The standard ROMDOS distribution includes some source codes and/or objects for some modules, which enables selective compilation of the kernel. That kernel may be sufficient for the functionality desired. Datalight requires non-disclosure agreements when complete source code is supplied, and that source code is likely subject to export control. This is because the cost corresponds to intellectual property since it greatly exceeds reproduction and distribution costs.

Some DOS work-alike operating systems are available with complete source code available. Some can be freely down-loaded from the Internet, and others are available with source code at distribution costs. These distribution schemes are not likely subject to export control because intellectual property is not being sold. Stripping extraneous functionality and providing the complete source code enhances authentication.

Open-source LINUX is more authenticable than MS-DOS without source code. However, many of the features (e.g., network implementations) are extraneous and should be stripped out by the host. Return to 4.1.1

A.4.1.2 Libraries for I/O

Input/Output libraries normally contain vast amounts of extraneous functionality. It is more cost effective to custom-program concise and task-specific software than to authenticate complex libraries. One major issue with an I/O library is that the small amount of source code actually used is scattered through huge interconnected source files.

Any routines taken from an I/O library should be stripped of all extraneous functionality, and only the source code actually used should be provided. If used no more than one I/O library shall be used throughout the system.

Compiler-library routines might be considered authenticable if the host disassembles the object code and comments on the program flow in the documentation package. Also, all extraneous functionality must be removed. Return to 4.1.2

A.4.1.3 Compilers

Using a commercial compiler or assembler available for independent procurement in the monitor's country is acceptable if some valid means of verifying that it is not corrupted can be agreed to by all parties.

The compiler should be able to produce bootable code so an operating system can be avoided in the final implementation. However, using an operating system during development and private authentication may be beneficial.

The compiler should be able to produce a textual output file containing the assembly-language instructions used to implement the higher-level language instructions. Using compilers that relate the FORTRAN line or instructions to the group of assembly-language instructions is highly preferred. This allows the disassembled executable to be directly related to the source code.

Only one type of compiler for each programming language (C, Fortran, or assembly language) should be used throughout the system. For example, it is unacceptable if some segments are written for and compiled with Borland Turbo C when other segments use Microsoft Visual C++. The authentication task would grow as some power of the number of compilers used.

The requirement for complete documentation and a copy of all source code applies to the software residing on the information-barrier-protected system. If source code for the compilers is unavailable, a less desirable alternative may be the purchase of mass-market software. A mass-market software purchase would only be acceptable if a valid means of verifying that it is not corrupted can be agreed to by all parties. However, library routines placed into the software on the system must have source code provided. Return to 4.1.3

A.4.1.4 Interrupts

Unused interrupt lines should be both 1) masked off by the software and 2) hardwired in a state, which prevents their covert use.

- The prescribed values of all interrupt vectors and the description of their use should be provided in the documentation package. The authentication team will verify that all interrupt vectors match the values provided in the documentation.

- The authentication effort will include tracing the use of each interrupt vector with a logic analyzer capable of disassembling the executed code to verify that interrupt service routines are uncorrupted from those provided in the documentation package. Return to 4.1.4

A.4.2.2 Gamma-Ray Analysis Software

- The authentication effort will include re-aligning spectra with random coefficient values of $E = A + B*chan + C*chan^2$ and expecting the analysis program to find and use the correct coefficient values.

- The authentication effort will include inserting a spectral consistency test, which requires that a set of major plutonium peaks occur at the proper energy within a peak width to a high statistical significance. The goal is to ensure proper energy calibration by avoiding errors due to incorrectly identifying peaks used for calculating energy coefficients.

- The authentication effort will degrade spectral resolution until the limits of the software are discovered and documented.

- The authentication effort will insert peaks from other possible radionuclides until the limits of the software's capability to recognize problems are discovered and documented. Some peaks will attack the auto-calibration and some the isotopic ratio calculation.

- The authentication effort will determine the limits of the software in handling background due to nearby plutonium. If protocol allows canisters to await measurements nearby, some means of avoiding erroneous results due their contributions to the critical plutonium peaks should exist and be shown effective with the maximum amount of nearby plutonium permitted by protocol. If protocol allows the movement of plutonium during measurement, the authentication tests will examine those limits as well.

- The authentication effort could determine the limits of the software in handling baseline distortions due to a high-neutron flux from nearby plutonium. The high-neutron flux causes inelastic neutron scattering with the germanium in the HPGe sensor. Such peaks have a non-Gaussian shape with a large tail to high energy due to the recoiling germanium atom, which alters the expected baseline. A 595-keV peak has a tail that extends into the PU600 region.

- The authentication effort will verify that the analysis software is capable of calculating the correct isotopic ratio for a wide range of input spectra. Spectra corresponding to isotopic ratios between 1% and 20% will be constructed from mixtures of experimental data from the available sources. The capability of the software to calculate the correct results will be documented. It is important for ivory-grade plutonium (<1% ^{240}Pu) to pass a less-than-10% ^{240}Pu attribute test rather than error out due to lack of statistical precision in the ^{240}Pu peak used by the analysis.

- The authentication effort will determine the limits of the software in handling statistical fluctuations. Non-linear regression is often used in peak fitting and analysis, but it has occasional problems due to lack of convergence, poor initial values, and/or ill-conditioned regression equations. Since these problems can be easily triggered by statistical variations, authentication efforts should include robustness tests. Several spectra will be assembled from brief slices of experimental data to provide a substantial number of different statistical variations for analysis. As a measure of robustness, the minimum spectral acquisition time to achieve consistent results will be found and documented.

- The authentication effort will determine the limits of the software in handling unusual or unexpected baseline shapes by using spectra obtained with large sources of ^{90}Sr, ^{137}Cs, ^{60}Co, and isotopes normally found in special nuclear material.

- The authentication team will evaluate the algorithms used. For example, an energy calibration scheme using the channel containing the maximum value of a peak is less desirable than one using the central channel from a peak-fitting procedure or moments calculation. The maximum-channel approach is more vulnerable to statistical variations.

- The authentication team will evaluate the robustness of the analysis against single bad channels. When the MCA overheats, the count in isolated channels can often go bad due to a set, cleared, or stuck bit. The analysis should be robust against such problems. Return to 4.2.2

A.4.2.5 All Software Should be Modular

If a single bootable application program is used instead of an operating-system-based batch stream, the operationally independent modules should be self contained and capable of being extracted and compiled and tested as individual programs. If an operating system is used, a batch file scheme starting sequential programs that communicate using data on a RAMDISK is both modular and acceptable.

If serial data are passed between several CPU modules within the system, using different I/O software for each CPU unnecessarily increases the amount of software that the authentication team must examine. Return to 4.2.5

A.4.2.6 Self-Modifying Software and Fixed Parameters

The software will be tested under debugger conditions to verify that modifications to the code (self-modifying software) or certain variables (e.g., threshold values) do not occur. Self-modifying software or software modifying pre-agreed threshold values will be rejected. One authentication test will include comparing the code executing at completion with the “golden copy” to ensure that the code portion is unmodified. The value of demonstrating that the software and certain values remain unmodified is protection against a virus-like attack that might modify the program as it is loaded or while it is running. The design specifications should facilitate finding these problems by requiring code segments and protected data segments that can be easily monitored by a debugger for violations. The storage of the executable code on a one-time PROM rather than magnetic media precludes modification of the software files. Execution in place (XIP) precludes modifications while the software is loaded or executed. Return to 4.2.6

A.5.4.1 Statistical Sampling Plan

Explanation of concerns: The second authentication consideration is the strength of the statistical sampling plan, which we have not yet seen (so we cannot provide direct commentary on it at present), and the control of the population sampled. We believe it is possible to randomly sample from areas in the storage facility that contain no bilateral tamper indicating device (TID) containers (no containers under formal CoK), and gather useful information about a larger population, provided that we have a means of ensuring that the unexamined population cannot be mixed with a population of arbitrary and Russian choice. In other words, besides having CoK for containers that we have measured and sealed, we might be able to make some probabilistic statement about “fraction defective” if we know we are drawing samples from a population whose characteristics are frozen and cannot be altered between visits. This will require CoK on the nests from which we have determined to sample. We request a copy of this sampling plan and copies of all material flow protocols at the earliest opportunity in order to examine the authentication issues involved.

The method of handling canisters that fail to pass the AMS criteria is very important. If some fraction of canisters is allowed to fail due to statistical anomalies and measurement errors during each visit, very little can be learned about the sampled population. However, if any failing canisters are re-measured to handle statistical anomalies and measurement errors, more can be learned. Return to 5.4.1

A.5.4.2 Data Encryption

Both Russia and the United States consider encryption and related tools as national-security assets. Each is likely to be unwilling to give the other side access to these. It may be that open-source encryption tools provide an acceptable compromise. Following are two good candidates:

- Open PGP (Pretty Good Privacy) - see http://www.ietf.org/html.charters/openpgp-charter.html and http://openpgp.org/

- Blowfish - see http://www.counterpane.com/blowfish.html

Also a good reference on encryption issues is available at http://www.crypto.com/.

Additional candidate open-source encryption tools may exist. Return to 5.4.2