LA-UR-12-22026
Approved for public release; distribution is unlimited.

Title: The Role of Portal Monitors in Arms Control and Development Needs

Author(s): Hauck, Danielle K.
MacArthur, Duncan W.
Browne, Michael C.
Parker, Robert F.

Intended for: 53rd Annual INMM Meeting, 2012-07-15/2012-07-19 (Orlando, Florida, United States)

The Role of Portal Monitors in Arms Control and Development Needs

Danielle K. Hauck, Duncan W. MacArthur, Michael C. Browne, Robert F. Parker.
Los Alamos National Laboratory, MS E540, Los Alamos, NM 87545

ABSTRACT

Portal Monitors are a key piece of technology which represent a union between non-destructive analysis (NDA) and chain of custody (COC) in arms control verification. This linkage between NDA and COC is often neglected and the two areas are often erroneously treated as separate issues. We describe how NDA and COC issues come together in portal monitor technology. We also discuss features associated with portal monitor implementation for potential onsite verification of treaty declarations, which provide system security and monitoring confidence, including dual video surveillance-portal systems, triggered data recording and the potential need for information barriers on portal monitor data. Basic design requirements for portal monitor systems are discussed, including power sources and modularity, as well as needed areas for additional research.

INTRODUCTION TO TREATY VERIFICATION

There are several potential scenarios in which portal monitors could be utilized to support future treaty monitoring. Verification of declared stockpile reductions, which may involve monitoring of nuclear weapons dismantlement in the host facility, is one example. In such a scenario, treaty partners may negotiate a monitoring regime that includes direct on-site measurement verification of declared dismantlement activities. The objective of such a regime would be to provide confidence that weapons presented for dismantlement were truly dismantled, and that the sensitive materials and/or components were transferred to a secure storage area.

Aspects of the monitoring regime would depend on the specific treaty and other agreements between the treaty partners. For example, due to the extremely sensitive nature of potential treaty limited items (TLIs), declarations pertaining to the TLI may be limited. In this case treaty partners could negotiate a set of TLI attributes to support verification of declarations. [1] The goals of the monitoring regime might then be summarized as confirming that:

(1) the TLI presented to the monitoring party is consistent with the negotiated attributes and,

(2) that the TLI undergoes dismantlement consistent with the declared intent.

Dismantlement can be defined simply as the separation of the special nuclear material (SNM) from the high explosives (HE). In the potential dismantlement monitoring being described here, it is possible that the materials deriving from the TLI would be presented to the monitors following dismantlement, albeit in separate containers. Figure 1 conceptually illustrates the dismantlement process. The dismantlement itself is indicated by a “black box” because monitors may not have any access to the facility during dismantlement. Limited video surveillance of the surrounding facility may be permissible, but given the sensitive nature of dismantlement it is possible that direct surveillance of the dismantlement will not be permitted. For the remainder of the paper we assume a monitoring scenario similar to the one described above to discuss measurement options and the role of portal monitors in treaty verification.

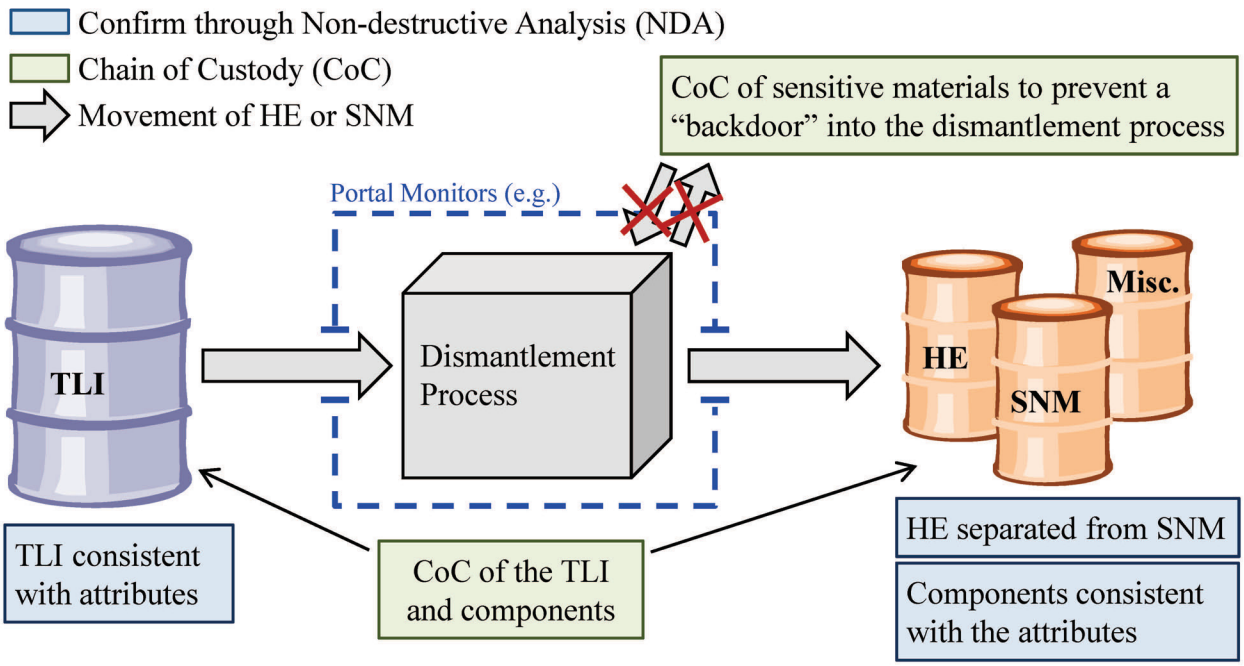

Figure 1. Dismantlement of a declared treaty limited item (TLI).
Dismantlement can be defined simply as the separation of special nuclear material (SNM) from the high explosives (HE). Monitors may not have access to the dismantlement process which is represented as a black box. With current technologies it is not possible to directly maintain chain of custody (CoC) on the SNM in the TLI to assure that dismantlement has taken place. Therefore, it is important to track SNM to assure that only SNM associated with the TLI enters or leaves the dismantlement process.

Typically, non-destructive analysis (NDA) methods (such as gamma spectroscopy and neutron counting) will be used to address the first goal of the monitoring regime; confirming that the item presented to the monitors is consistent with the negotiated attributes. An attribute is a characteristic of the TLI, such as presence of SNM, which increases confidence that the TLI is as declared. [2] A measurement system designed for confirming attributes is commonly called an Attribute Measurement System (AMS). The technical design and implementation of AMSs continues to be an active area of study. [3-6]

With currently available technologies, verification of the dismantlement process relies on chain of custody (CoC) methods, such as tags and seals, tamper indicating enclosures (TIEs) and video surveillance. Examples of how NDA and CoC are used during a monitoring regime to confirm warhead dismantlement are indicated in Figure 1. The annotations of Figure 1 are not all-encompassing, neglecting, for example, the importance of maintaining CoC on the measurement equipment.

Confirming the dismantlement process is extremely important for ensuring that the host is conforming to treaty obligations. The monitor needs to be sure, for example, that the host is not "recycling" either the TLI or the storage containers for dismantled parts, during a multiple-item dismantlement regime. CoC technologies such as tags and seals are not viable since the item does not remain in the same container. One method of verifying that the SNM presented to the monitors post-dismantlement is the same SNM in the TLI pre-dismantlement, is through tracking SNM with

radiation detection equipment. Portal monitors can be used to gain confidence that only SNM associated with the TLI is leaving or entering the processing area and that SNM has not been diverted or replaced. The dotted line in Figure 1 can be treated as a physical boundary with portal monitors to track SNM entering and leaving the process area.

Dismantlement is being used in this paper as a stand-in for any host sensitive process which involves transfer of SNM from one container to another. If, for example, an item must be placed into a specialized transport container prior to being moved, CoC on that item is lost. It becomes necessary to rely on CoC of SNM, and technology such as portal monitors, to gain confidence that the SNM that entered the process area is the same SNM that leaves the process area.

THE ROLE OF PORTAL MONITORS

Portal Monitors are useful for tracking SNM in a monitored dismantlement scenario or for monitoring any sensitive host process during which other forms of CoC of the item may be lost. Portal monitors can be regarded as a CoC technology since they allow tracking of materials relevant to the monitoring regime. However, as reasonably complex NDA measurement equipment, portal monitors are also subject to many of the design concerns of AMS equipment.[7] As such, portal monitors represent an important area of overlap between NDA and CoC. The monitoring regime can be viewed as made up of NDA, CoC and a monitoring protocol which is negotiated to describe technical use procedures, outline rights and privileges of both parties and to provide agreed-upon structure for the NDA and CoC activities (illustrated in Figure 2). NDA and CoC are often regarded as separate, distinguishable components. In reality, CoC of SNM is an important and non-trivial example of overlap between NDA and CoC.

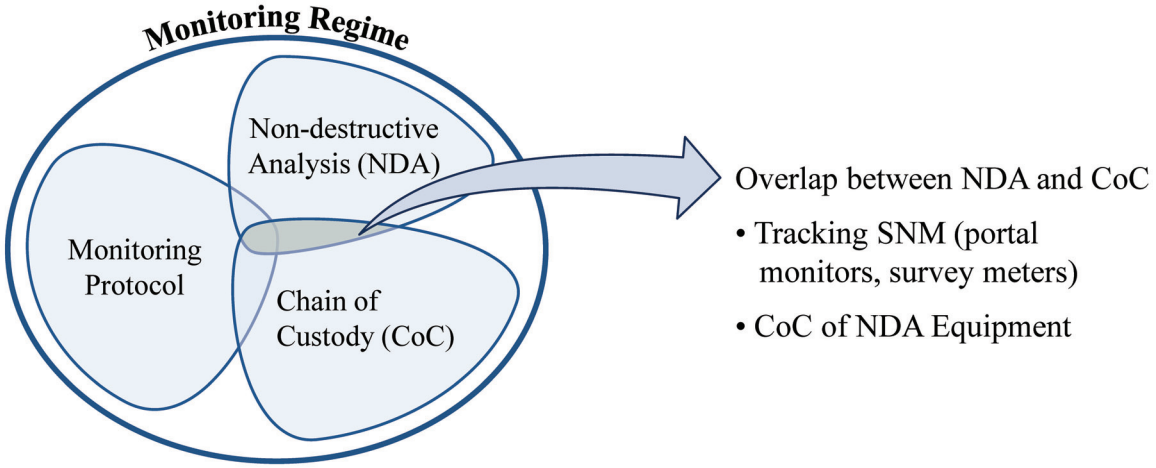

Figure 2. Breakdown of the Monitoring Regime and the Role of Portal Monitors
To a rough approximation, non-destructive analysis (NDA) is used to verify that the treaty limited item (TLI) is consistent with the attributes, and chain of custody (CoC) is used to verify that the TLI is processed (e.g. dismantled) in a manner consistent with declarations. The monitoring protocol is a combination of technical procedures and high-level rights, and provides an agreed upon structure for NDA and CoC activities. The real picture is naturally more complex. CoC supports verification of the TLI attributes, for example through CoC of NDA equipment, and NDA is needed for dismantlement verification, for example through the tracking of special nuclear material (SNM).

PORTAL MONITOR SYSTEM BUILT FOR ARMS CONTROL

A prototype portal monitor system consisting of two neutron-based portals and two gamma-ray based portals was built at LANL and used in a dismantlement exercise. The system utilized a Dragonball MiniGrand instrument board; originally designed at LANL for IAEA safeguards applications of portal monitors and now commercially available. Each neutron-based portal monitor contained four 36-inch He-3 tubes imbedded in polyethylene. Each gamma-ray based portal monitor contained two plastic scintillators and a single channel analyzer (SCA); also designed at LANL and now commercially available. Each portal monitor measures and records gross neutron or gamma-ray counts as a function of time.

The portal monitor system, pictured in Figures 3a-b, consisted of neutron and gamma-ray subsystems that were independent of each other. Only one portal monitor in each sub-system included a secondary tamper indicating enclosure and user controls, the second portal monitor in each system was controlled by the first. Figures 3c and 3d show the internals of the controlling gamma and neutron portal monitors, respectively.

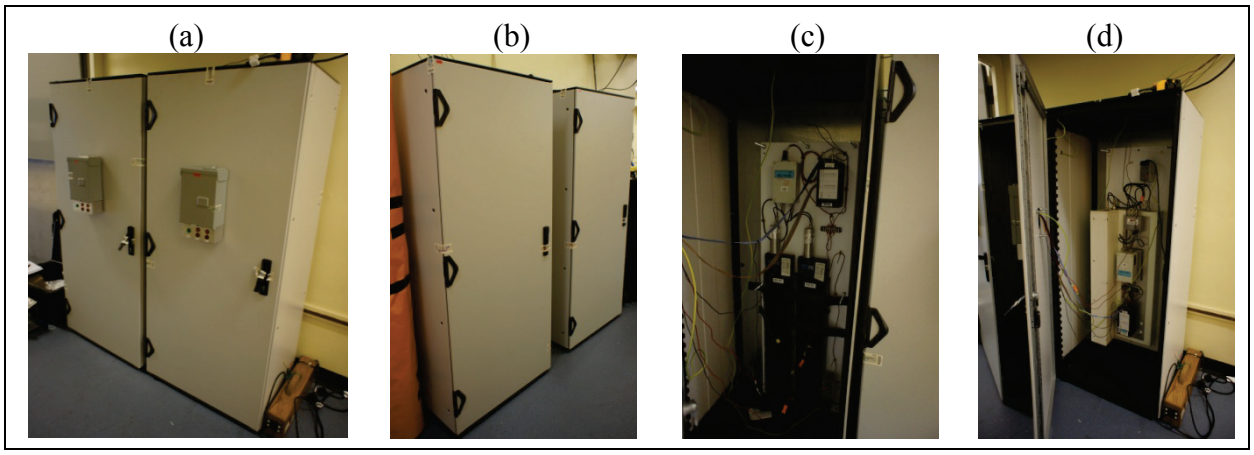

Figure 3. External/Internal views of the Portal Monitors used in the dismantlement exercise.
The portal monitor system consisted of neutron and gamma-ray subsystems that were independent of each other. The primary portal monitors in each sub-system (a) included a tamper indicating enclosure for the user controls, the secondary portal monitors in each system (b) were controlled by the primary. The gamma portal monitor is on the left and the neutron portal monitor is on the right in both (a) and (b). The internal structure of the controlling gamma portal (c) and controlling neutron portal (d) are also pictured.

The portal monitors were positioned in a hallway in the same order shown in Figures 3a and 3b, alternating gamma/neutron/gamma/neutron. Each pair of portal monitors was separated by about 6 feet. Figure 4 shows an example of portal monitor data which exemplifies one of the advantages of arranging the portal monitors in this configuration; the ability to deduce direction of motion.

Certain design choices were made to make the portal monitors more suitable for a treaty verification application. Design choices were driven by facility limitations as well as certification and system authentication requirements. Certification is the process by which the host party assures that equipment is safe to operate and protects sensitive information. An example of a design requirement based on certification concerns was the ability to inhibit data acquisition at pre-determined points during the monitoring visit. Accordingly, an inhibit control was added to the portal monitors which prevented acquisition of any data. An example of the data from all four portals is shown in Figure 4.

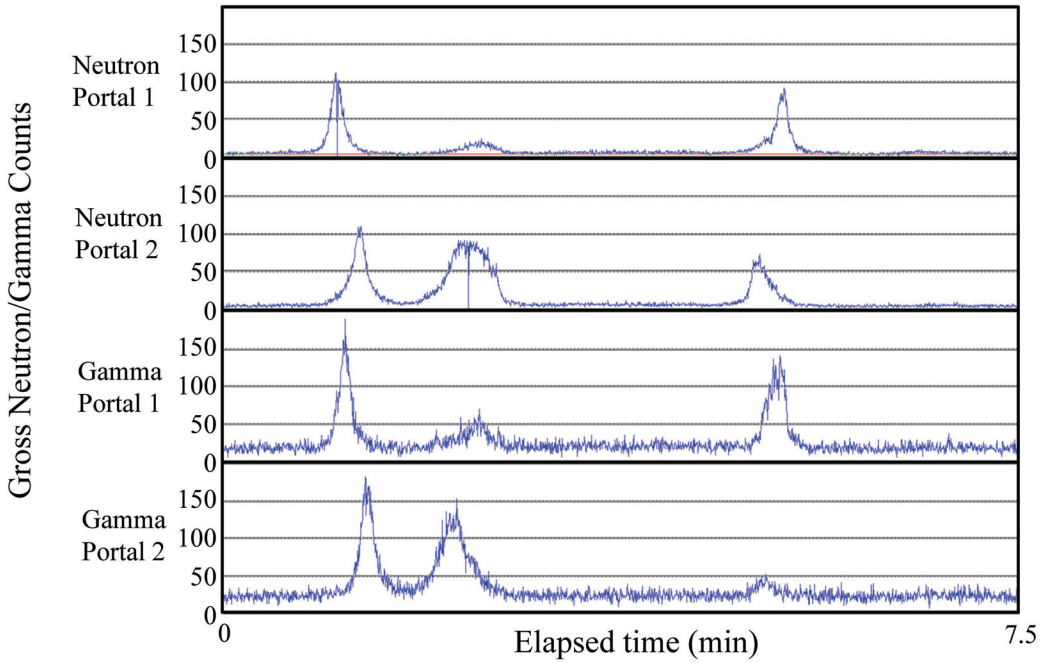

Figure 4. Example Data a Test Source passing by Portal Monitors
It was possible to deduce direction of motion using either the neutron or the gamma portal sub-system, although each portal in a sub-system was separated by only ~6 feet. E.g., the first peaks clearly appear in portal 1 prior to appearing in portal 2.

Authentication is the process by which the monitoring party gains confidence in the fidelity of the monitoring regime outcome. For the case of the portal monitors, authentication considerations include

- Design simplicity and minimal functionality to facilitate equipment inspections
- Simple communication between modules to facilitate inspection and potentially line filtering
- The ability to download data at the discretion of the monitors to allow for unplanned equipment functionality checks
- Protection of the portal monitor user controls from unauthorized access
- Protection of the portal monitor measurement equipment from tampering or any unauthorized access
- External state of health and alarm indicators to inform monitors of equipment status

Modifications and design choices that were made to the portal monitors to meet each of the authentication requirements are described below.

Simple Design
The portal monitor detectors and supporting instrumentation had a simple one-dimensional layout pre-arranged on a sled, which was mounted inside the portal monitor enclosures. In this way the physical system mirrored the system diagrams so that the monitor could visually inspect system layout quickly.

Minimal functionality
One instrument card (for ionization chambers) was removed from the MiniGrand to remove excess functionality. Minimizing functionality makes it easier for both the monitoring party and the host party to verify that the system is operating as designed, with no hidden or prohibited functionality.

Simple communication between modules
The neutron portal sub-system (consisting of two portal monitors) is completely independent from the gamma-ray portal sub-system (also consisting of two portal monitors). In each case, the two portal monitors in a sub-system were connected with two cables; a 12V power supply cable, and a BNC signal cable. For authentication purposes it is preferable that each type of communication is provided by a distinct cable so that the physical system mirrors system diagrams. In addition, it is easier to filter cables carrying only one type of information to prevent any additional information from being passed along the same cable.

The ability to download data at Monitor discretion
A very important monitoring technique is to build flexibility into equipment procedures so that it is impossible for the host to predict exactly when a monitor will opt to perform a task. One method of gaining confidence in the portal monitor is to extract data at any time at the monitor's discretion to assure that it is working correctly. Originally, the MiniGRAND instrumentation would continuously write data files to an SD card. Each data file contains information from one day, beginning and ending at midnight. Errors in the data file would occur if the portal monitors were not properly restarted after inserting the SD card. The file storage was modified so that portal monitor data could be retrieved at any time and so that the portal monitor did not need to be restarted while switching SD cards.

Protection of the Portal Monitor user controls
A sealable tamper indicating enclosure was designed to contain the controls for the power, inhibit and alarm reset, and the SD card interface. This mitigated the possibility of the portal monitors accidently or surreptitiously being disabled without knowledge of the monitoring party.

Protection of the measurement and acquisition equipment
The portal monitors were originally designed to be placed in Hoffman Boxes®, or other suitable tamper indicating enclosure. The need to prevent and detect tampering of the portal monitor falls under CoC of NDA equipment, which was noted in Figure 2 as one of the overlaps between CoC and NDA, along with portal monitors themselves. An appropriate TIE was not used during the

dismantlement exercise (and therefore is not pictured in Figure 1) due to cost and time constraints. The portal monitors were also designed to include a door switch which would record times that the door was opened and closed.

External state of health and alarm indicators

The monitors (the people) will be busy during any monitoring visit with several events competing for their attention. Therefore, easily visible state-of-health and alarm indications are very important. The controlling portal monitor of each sub-system had one green LED indicating that the controlling portal was receiving external power, two red LEDs indicating that the respective portal was currently alarming and two orange LEDs indicating that the corresponding portal alarmed previously, often called a latched alarm.

LESSONS LEARNED

The previous several paragraphs describe design criteria which were anticipated and built into the portal monitors prior to the dismantlement exercise. Each of these design criteria were important for maintaining confidence in the correct functioning of the portal monitors and the portal monitor data. However, while using the portal monitors in the dismantlement exercise, several additional design guidelines were emphasized. Some of these were anticipated, although perhaps not fully appreciated until using the portal monitors in a realistic context. The most important "lessons learned" were

- Mitigate any potential need to troubleshoot because it won't be possible
- Be prepared for noisy facility power and electrical grounding
- Plan for facility requirements, resources and limitations
- Make equipment reliable even during rushed and distracting conditions
- Minimize any data handling, including downloading, recording or reviewing

Each of these "lessons learned" are discussed in more detail below.

Inability to Troubleshoot Onsite

One of the practical difficulties introduced by the need to simultaneously maintain certification and authentication of equipment is the inability to perform any troubleshooting on site. Any attempts to open equipment or perform any non-standard equipment modifications that were not agreed upon in negotiations would result in the loss of host confidence, monitor confidence or both. Therefore, equipment should be extremely robust and utilize redundancy. It is recommended that equipment should be highly modular and individual modules should be designed to move into the facility intact. Reassembly comes with the significant risk of non-functional equipment, and even minor troubleshooting will not be possible. Whenever possible, adequate spares that have gone through the same authentication/certification processes, as the primary equipment should be available.

Prepare for Noisy Facility Power & Electrical Grounding

Equipment should be designed to handle facilities with noisy or fluctuating electrical power. In addition to problems associated with facility age, facilities are often running a large array of industrial equipment which can have a significant and fluctuating draw on facility power. In particular, fans and motors can introduce noise in the power supply. The availability of power

outlets can restrict equipment locations or lead to the use of long extension cords, which can also introduce noise. Making equipment self-sufficient with an uninterruptable power supply (UPS) is one option, but must take into account facility safety regulations. Use of a UPS would also reduce dependence on the location of outlets.

Electrical grounding is a common safety requirement for all industrial (including weapons) facilities. In some cases, the same grounding conductor is used for all equipment in the facility, making the ground itself particularly noisy. If grounds are not required for safety reasons, the equipment hardware should be floating to prevent feedback loops of grounding noise. During the dismantlement exercise, the signal input cable between the portal monitors in each subsystem was connected with a metal connector which became a potential source of noise/interference when placed on or near noisy grounds. Finally, radiofrequency (RF) fields in the vicinity of the detectors can introduce noise and interference. Insulating any exposed components, for example by wrapping the detector/photo-multiplier tube interface with aluminum tape, can mitigate noise from RF fields.

Plan for Facility Requirements, Resources and Limitations

The facility has a major effect on the final design of the equipment and it is impossible to construct measurement equipment for one facility with the assumption that it will be feasible in another facility. On the other hand, certain design characteristics, such as modularity, may help to make the equipment feasible for use in a wider range of circumstances. Even when equipment is being designed for a specific facility, many aspects of the facility may be sensitive and unavailable (at least in detail) to the monitoring party during equipment design. Basic facility characteristics such as allowable weight loadings, hallway and door sizes and resources for transporting large/heavy equipment must be considered during the design phase. Safety requirements can include grounding (as discussed above), support and stabilization requirements, and specifications of types of equipment enclosures and limitations to communication methods, to name a few examples, and have a fundamental impact on equipment design. Safety personnel generally do not care about signal quality and will require changes without regard to effect on functionality. It is frequently not possible to retro-fit equipment to meet safety requirements, which must be built into the original design. Equipment will be operated by facility personnel that are not necessarily trained in that type of equipment. Therefore, equipment should be fool-proof, both for safety and reliable operation of the equipment as designed. Connections should only fit in the correct location; batteries should only fit in the right direction, etc. Ideally, equipment should be built to require as few facility resources as possible. A lack of resource availability once onsite can slow down and inhibit monitoring tasks.

Reliability even during rushed and distracting conditions

Most weapons facilities have both stringent escorting requirements and personnel limits. The result can be relatively few monitors in the facility at one time and many more facility workers and escorts. Crowding around equipment can make it difficult to detect surreptitious movements either in real time or during surveillance video review. State of health and alarm indications should be extremely easy to see from a distance by people on the ground and in surveillance videos, even if there is a crowd around the equipment. Technical procedures should be kept simple so that they require a minimum amount of attention on the part of the monitor or facility worker to do correctly.

Minimization of data handling

The procedure for data transfer out of a facility can result in a delay of up to a day between events and reviewing the corresponding portal monitor data. It can also be time consuming to review all portal data, even with the built-in flags for identifying alarm points, especially with regard to finding corresponding points in the surveillance video. Some potential improvements to the portal monitor system for arms control include triggered data and an integrated portal-video system.

POTENTIAL NEED FOR AN INFORMATION BARRIER

In arms control, the host must be assured that all sensitive information is protected. To address this, information barriers (IBs) can be incorporated with measurement equipment to protect sensitive information. [8] Only agreed upon measurement results are allowed to pass through the IB, which may be a combination of physical enclosures, electromagnetic shielding and signal processing design.

Due to the design of these portal monitors, they are only capable of measuring gross neutron and gamma-ray count rates as a function of time. However, depending on the negotiations, the gross counts may be considered sensitive by the host party. In addition, the dismantlement exercise revealed the great amount of information implicit in the gross count rates. For example, it was possible to distinguish changes in neutron count rate resulting from the movement of people. Physically this is caused by changes in neutron moderation. With corresponding video surveillance of the area, precise timing of events evident in the portal monitor data could be reconstructed. Therefore, it is possible that an IB may be required for future deployment of portal monitors for treaty verification, depending on the negotiated agreements.

It is not clear how an IB should be implemented for portal monitor data. One option is to eliminate or restrict the downloading of data and to instead have monitors to review data onsite in real time. There may be additional benefits of having onsite data review, since it mitigates the time delay between events and their review and decreases the monitor's burden of data to be reviewed while off site.

ACKNOWLEDGEMENTS

The design, construction and testing of the portal monitors for an arms control scenario was a combined effort among Danielle Hauck, Duncan MacArthur, Robert Parker, Richard Williams, Michael Browne, and Aled Richings and was supported by the U.S. National Nuclear Security Administration's Office of Nuclear Verification (NA-243).

REFERENCES

[1] MacArthur, D., D. Langner, A. Livke, M. Smith, J. Thron and S. Razinkov (2010) The Attribute Measurement Technique, *Proceedings of the 51st Annual INMM Meeting, LA-UR-10-03195*

[2] Langner, D.G., R.P. Landry, S.-T. Hsue, D.W. MacArthur, D.R. Mayo, M.K. Smith, N.J. Nicholas, R. Whiteson, T.B. Gosnell, Z. Koenig, S.J. Luke, and J. Wolford (2001) Attribute Measurement Systems Prototypes And Equipment In The United States, *Proceedings of the 42nd INMM Annual Meeting. LA-UR 01-3610*

[3] Razinkov, S., M. Bulatov, S. Kondratov, A. Livke, D.W. MacArthur, D. Sivachev, J. Thron, S. Tsybryaev, A. V'yushin (2010) AVNG System Objectives and Concept, *Proceedings of the 51st INMM Annual Meeting. LA-UR* 10-2625

[4] Thron, J.L., D.S. Bracken, L.A. Carrillo, T.H. Elmont, N.A. Johansen, K.C. Frame, J.A. Gallegos, P.J. Karpius, D.W. MacArthur, J.M. Shergur, M.K. Smith, D.T. Vo and R.B. Williams (2007) Next Generation Attribute Measurement System, *Proceedings of the 48th INMM Annual Meeting. LA-UR* 07-3749

[5] Archer, D. (2011) The Third Generation Attribute Measurement System, *Proceedings of the the 53rd INMM Annual Meeting.*

[6] Elmont, T.H., D.G. Langner, D.W. MacArthur, D.R. Mayo, M.K. Smith, A. Modenov, A. Livke, M. Bulatov, A. Morkin, S. Razinkov, S.S. Safronov and S.J. Luke (2005) AVNG System Software - Attribute Verification System with Information Barriers for Mass Isotopics Measurements *Proceedings of the 46th INMM Annual Meeting. LA-UR 05-4502*

[7] The Joint DOE-DoD Authentication Task Force (2001) Guidelines for Authenticating Monitoring Systems.

[8] D.W. MacArthur and J.K. Wolford Jr. (2001) Information Barriers and Authentication, *Proceedings of the 42nd Annual INMM Meeting, LA-UR-01-3334*