Preliminary Results from the 2010 INMM International Containment and Surveillance Workshop

Frances Keel
Steve LaMontagne
National Nuclear Security Administration

Chris Pickett
Oak Ridge National Laboratory

Keith Tolk
Milagro Consulting LLC

Abstract

The Institute of Nuclear Materials Management held an international workshop, entitled "Containment & Surveillance: Concepts for the 21st Century," on June 6–11, 2010, at Oak National Laboratory, in Oak Ridge, Tennessee. The National Nuclear Security Administration Offices of Nonproliferation Research and Development and Nonproliferation and International Security sponsored the event. The workshop focused on determining concepts and needs for twenty-first century containment and surveillance (C/S) systems that support International Atomic Energy Agency (IAEA) safeguards, regional safeguards authorities (e.g., the Brazilian-Argentine Agency for Accounting and Control of Nuclear Materials and the European Atomic Energy Community), and future arms control agreements.

Panel discussions among subject matter experts and international practitioners provided the daily topical theme for the following areas of C/S: authentication, tagging, sealing, and containment verification and surveillance systems. Each panel discussion was followed by a question-and-answer session with the audience and an afternoon breakout session. The facilitated breakout sessions were used to compile and prioritize future needs.

Individuals attending the workshop included: C/S experts and practitioners, IAEA and arms control inspectors, technology providers, vendors, students, and other individuals with an interest in or desire to learn about future C/S system needs. The primary goal for the workshop was to produce a document that details the future research and development needs and priorities for C/S systems that support nuclear safeguards and arms control missions. This paper presents a preliminary compilation of the information obtained from breakout sessions at the workshop.

Introduction

"Containment & Surveillance: Concepts for the 21st Century," an Institute of Nuclear Materials Management international workshop sponsored by the National Nuclear Security Administration Office of Nonproliferation Research and Development (NA-22) and the Office of Nonproliferation and International Security (NA-24), was held on June 6–11, 2010, at Oak Ridge National Laboratory. Attending were 95 participants, each representing U.S. or foreign government agencies, universities, industry, or national laboratories (see Figure 1). The presenters, who are subject matter experts and practitioners in the topical areas of containment and surveillance (C/S), provided daily panel discussions on the issues and emerging trends in authentication, tagging, sealing, and containment verification and surveillance systems (Figure 2).

Figure 1. Photo of workshop attendees

The primary goal of the workshop was to supply information and to detail challenges that must be addressed to enable future C/S systems to improve the continuity of knowledge for materials and activities monitored by nuclear safeguards and arms control inspectors. Each morning, the workshop began with a series of talks in one of the four topical areas of containment and surveillance: authentication, tagging, sealing, and systems. The discussions were followed by question-and-answer sessions with the audience and an afternoon brainstorming session with smaller groups of attendees (facilitated by subject matter experts from U.S. national laboratories). This format was followed for the first four days of the workshop. On the morning of the fifth day, the workshop concluded with each breakout team presenting the efforts of their team to come up with twenty-first century concepts for C/S.

Figure 2: Morning panel discussion

This paper provides a preliminary overview of the discussions and reports generated by the participants of the workshop.

Authentication

The following definition of authentication was given to the participants:

> Authentication is the process by which the Monitoring Party gains appropriate confidence that the information reported by a monitoring system accurately reflects the true state of the monitored item.

The Authentication Task Force, a U.S. interagency group that was active in 2000–2001, developed this definition. In order to satisfy this definition of authentication, all aspects of the monitoring system must be trusted. Aspects include the hardware that comes from the manufacturer, the software and firmware used in the monitoring data generators and the data collection/processing system, and the security-critical aspects of the monitoring system, such as the cryptographic key management system.

There were many discussions of various aspects of authentication throughout the workshop. First, the design of the security-critical components must be such that authentication can be performed. Then, there must be some method for ensuring that no one can modify the equipment so that it gives false results. A method must be designed into the equipment to re-verify the authenticity of the equipment if there is a possibility

that an adversary might have had access to it. Discussions focused on how to accomplish these goals and what technologies might be developed. There were several new ideas put forward, which is the reason for having a diverse group of talented people working together.

Verification of the trustworthiness of software from outside vendors was identified as a major problem that requires further study.

The technology surrounding the cryptography used to add digital signatures to the data was also discussed. There are two approaches to calculating digital signatures. One uses the same key to both sign and verify the signature. Of course, anyone who can verify the signature can also counterfeit the data, so keeping the keys secret is extremely important. This results in a very difficult key management problem. The other approach uses different keys for the signing and verifying operations. This greatly simplifies key management, but the computing resources required in the seal or tag increase dramatically. This approach is therefore quite difficult in small devices with limited battery life. Unfortunately, the discussions gave no breakthroughs in this area but identified it as a target for future research and development.

Tagging and Identification Technology

Unique identifiers are very important attributes that safeguards and arms control inspectors must establish with assets of concern to ensure that C/S systems can sustain and maintain the appropriate level of continuity of knowledge with the asset. The standard definition for a tag is a device that provides a unique identifying attribute that can be used to facilitate the inventory process and to track assets of concern. Since many assets of interest do not have unique identifiers or any visually identifying attribute, inspectors typically have two choices: either take advantage of a unique feature (or features) of the containment or establish a unique identifier by securely attaching a tag to the asset and/or the containment. Most nuclear materials cannot easily be tagged. Therefore, the standard practice has been to containerize materials and externally tag the container.

Presentations at the workshop pointed to the need to establish unique intrinsic identifiers (tags) for new containers and to develop secure tag-attachment schemes for existing containers. Secure tag-attachment schemes point to the need to make tags into seals. Seals can be used as tags, but it is important to point out that tags cannot be seals.

It was also considered important that future tags be durable and capable of being read remotely with automated data entry equipment (to reduce human error from manual data entry and to support asset tracking). Recommendations were made for continued investigation of emerging radio-frequency (RF) technologies to address the need to support asset tracking and location monitoring. For example, ultra-wideband (UWB) technologies may solve some of the problems in the communication and security of these devices, and it was recommended that the role of UWB in tags and seals be studied further.

Radio-frequency identification (RFID) devices are now widely used in industry, but they have not been used in safeguards or arms control. The strengths and weaknesses of RFID technology were discussed, and some recommendations were made for addressing its shortcomings.

Sealing Technology

Seals are defined as devices that have unique identifiers with a non-erasable tamper-indicating feature (or features). Seals typically are applied at the interface of a container where normal access occurs. A seal's purpose is not to prevent access but only to record that it occurred. The presentations on sealing voiced a message that was repeated many times during the workshop as a need for "more tools in the toolbox." One of the speakers (who formerly worked at the International Atomic Energy Agency [IAEA]) noted " that when your only tool is a loop seal, every container appears to have a hasp." This statement summarized what many of the breakout sessions (see Figure 3) and attending experts concluded: more sealing options are needed and the options need to be tailored to the application.

Figure 3: Afternoon breakout session

In the previous section it was pointed out that a need exists for using seals as tags to facilitate inventory taking and asset tracking and to sustain continuity-of-knowledge monitoring for both safeguards and arms control applications. The basic theme for several talks presented at the workshop was a need to develop secure tamper-indicating attachment schemes for attaching tags to containers (or basically for turning tags into

seals). A parallel theme was also described as a need to make the containment the seal (i.e., the need to make asset containers into tamper-indicating enclosures [TIEs]).

Containment—Tamper-Indicating Enclosures for Equipment

Active monitoring of the integrity of TIEs will increase the confidence of the monitoring party that the equipment has not been tampered with while the inspectors or monitors have been absent. This increased confidence will allow longer intervals between monitoring visits and can free the inspectors/monitors to perform other duties during their limited time on site. Several technologies were discussed, including resistive membranes, ultrasonic/acoustic approaches, and monitoring the interior of the enclosure for changes in light level or RF characteristics.

There were also discussions about how to improve the efficiency of inspecting TIEs in the field. Several approaches were discussed, including random patterns applied to the surfaces for identification, ultrasonic inspection, and eddy-current sweeps to detect repaired penetrations.

Tamper-Indicating Enclosures for Material

One of the problems associated with monitoring material that is subject to a safeguards or arms control agreement is that the approved containers for the material were not designed for high-security sealing. In most cases, the host will not be willing to change the container to accommodate sealing because of the difficulty in getting the modified container certified for use. This problem was discussed, and the options appear to be either adding tamper-indicating features to all possible entry points into the container or putting the existing container into a TIE that can be sealed. In some cases, the TIE can be the room itself.

Conduit

There were several discussions about tamper-indicating conduit in the working groups — how to inspect it, how to monitor it, and how to avoid it. The IAEA currently uses tamper-indicating conduit to detect tampering with cables carrying unauthenticated analog signals. The conduit must be physically inspected to find indications of tampering attempts. This can be especially difficult in an operating facility because operations might have to be suspended and scaffolding might need to be erected to get to some sections of the conduit. It is also difficult to inspect conduit at wall penetrations and behind equipment that is installed after the conduit was put in place. Most of the brainstorming groups identified the inspection of tamper-indicating conduit as a problem that should be addressed, either by eliminating the need for the conduit, actively monitoring it for intrusion, or improving methods for inspection.

The most effective way of eliminating tamper-indicating conduit is to add authentication to the signal at the source. This is difficult for analog signals, and digitizing the signals at

the sensor can be difficult in high-radiation fields. However, with advances in electronics, these ideas could be pursued.

Another approach is to actively monitor the signal cables with technology such as time-domain reflectometry. This approach is currently being studied at the IAEA.

Other technologies that could be used to monitor the integrity of the conduit were discussed, including the use of acoustic waves and active fiber-optic wraps.

System Issues and Approaches

Defense in depth came up several times during the workshop, emphasizing the danger of depending on a single layer of security in monitoring equipment and scenarios. One innovative suggestion was to use information about facility characteristics, such as the pressure variations in a pipe, to add confidence that no changes have been made.

Data processing and interpretation is another area that received considerable discussion. The inspectors/monitors are being deluged with an amazing amount of data that must be turned into knowledge about the conditions at facilities. The more this process can be automated and turned over to computers, the more time the inspectors/monitors will have available to investigate anomalies and draw conclusions. A rules-based approach to automation was one method proposed for doing this.

Monitoring systems must also be thought about from a systems approach, rather than being thought of as a collection of discrete sensors. Modeling tools may be useful in helping systems designers optimize a system design. Risk-based approaches may also be useful in optimizing monitoring systems.

Joint use of equipment between the monitoring party and other agencies or the host is also recognized as a problem area because other parties must be considered to be potential adversaries. If joint use is going to be employed extensively in the future, the monitoring systems and equipment must be designed with that scenario in mind.

Cryptographic key management is another area that was discussed in the groups. There may be new approaches to the use of private or secret keys that minimize the risk of needing to reveal the keys.

Several people recommended making greater use of wireless technology in monitoring systems. Although there is some reluctance on the part of the operators to allow wireless transmissions because of security concerns or interference with other systems, the advantages of wireless communications make the technology attractive for future study.

Surveillance

The new surveillance system that is currently under development for the IAEA addresses many of the issues that were brought up in the discussion groups, but several problems and implementation questions remain.

- The camera cost is high. A range of cameras might be useful so that money is not wasted on features that are not necessary for specific applications, such as radiation tolerance.
- It needs to be determined whether cameras should be made smaller so that they are less intrusive and can be deployed more easily.
- Improvements are needed for low-light situations.
- The large volumes of data require extensive use of network, data processing, and personnel resources.
    - A better use of triggering for surveillance should be investigated.
    - A method for selecting, combining, and prioritizing images that allow inspectors to focus on those that are of the highest importance should be developed.
- The use of information barriers for imaging systems should be investigated to provide assurance to the monitored party that no sensitive information will be divulged.
    - The field of view of the camera could be limited,
    - optical methods could be used to blur sensitive areas of the scene,
    - the resolution of the camera could be limited, and
    - trusted processing could give pass/fail output instead of images.
- Methods for authenticating images/cameras should be reexamined.
- Methods for preventing spoofing at the physical level should be investigated. For example, a laser could be used to verify that nothing has been placed in front of the camera to spoof the image.
- Simplified cameras for arms control should be developed.

Effective twenty-first century surveillance will require efforts that look into system approaches that evaluate "plug and play" connectivity for emerging safeguards surveillance technology and that provide methods for effective utilization of information barriers. Rules-based event processing was one method discussed that offered a common system strategy for integrating layers of technology to support "in-depth" safeguards monitoring. Protecting sensitive information is an area that requires parallel efforts of the development of policy and technology. Future systems will also require improved methods for handling large amounts of sensor and image data. This includes the capture, transmission, and inspection of data.

Some Concluding Thoughts and Proposed Next Steps

Many of the attendees felt that there needs to be more communication between the customers and technology developers (especially between the IAEA and the national laboratories). Methods that improve the communication of both user needs and emerging technology must be developed and sustained if the needs of both twenty-first century safeguards and arms control are going to be met. Workshops such as this one help, but workshops that focus on specific technology areas or needs would also be useful.

Informal discussions, technology exchanges, laboratory visits, and distribution of reports articulating recent developments and needs would fill a communication void as well.

The time required for developing, testing, and deploying new systems and technologies is so long that the equipment can become obsolete before it is fully deployed. The development of replacement systems should begin immediately after the deployment of the current systems. This also reinforces earlier themes of both safeguards and arms control: that more tools are needed for the respective toolboxes and that long-term research and development needs to be sustained for these missions. The IAEA should publish and promulgate a procedure for describing the technology/system acceptance process for new safeguards technology.

Some of the near-term next steps for consideration would include the following:

- Conducting scenario- and technology-specific workshops/exercises, including
    - RFID issues, status, and future,
    - mock inspections, and
    - spent fuel dry storage monitoring.
- Forming international working groups (similar to the Tagging Laboratory Advisory Group) to work on specific issues such as tagging and sealing that provide annual reports.