SAND2012-0205 C

SAND2012-0205C

Seventh INMM/ESARDA Joint Workshop
Working Group 2: Future Directions for Safeguards and Verification Technology Research & Development

Co-chairs

Sergey Zykov

Director, Division of Scientific and Technical Services, Department of Safeguards, International Atomic Energy Agency, Vienna, Austria

Dianna Blair

Manager of International Safeguards and Technical Systems, Sandia National Laboratories,[1] *Albuquerque, NM, USA*

Introduction

The European Safeguards Research and Development Association (ESARDA), the International Safeguards Division (ISD) of the Institute of Nuclear Materials Management (INMM), the Atomic Energy and Alternative Energies Commission (CEA) of France, and the European Commission Joint Research Centre (JRC) co-organized the seventh INMM-ESARDA joint workshop *Future Directions for Nuclear Safeguards and Verification*, held in Aix-en-Provence, France, from 17–20 October 2011. The INMM/ESARDA joint workshop gathered experts, programme managers and policy makers from across the international community to discuss current issues in international safeguards and the non-proliferation arena. This paper summarizes discussions that took place within Working Group 2 of the joint workshop, *Future Directions for Safeguards and Verification Technology Research and Development.* The intent of this paper is to capture the major points that were discussed by the group, not to reiterate the presentations provided by participants. Papers contributed by individual presenters are included in the workshop proceedings.

Working Group 2 included approximately 35 participants. While this number varied slightly throughout the workshop due to intergroup migration there was, in general, consistent attendance. The group comprised representatives of technology providers, developers, users and regulatory bodies. This diverse assembly of stakeholders helped to provide the requisite context for understanding and framing the challenge of determining future directions for safeguards technology. The working group session comprised 21 presentations organized in three sections:

[1] *Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.*

1) The future for safeguards technology
2) The future for detecting undeclared nuclear activities
3) Future arms control verification technology.

In general, question and answers and group discussions took place following individual presentations. Where appropriate to common subject areas, discussion took place after a group of presentations. Feedback and discussion points were collected at key intervals.

The workshop organizers had posed four questions to Working Group 2:

1) What developments are needed in information, detection and monitoring technologies?
2) What verification technology and R&D are needed to deter the proliferation of nuclear weapons, by detecting early the misuse of nuclear material or technology?
3) How can progress be made in the detection of undeclared nuclear activities through environmental sampling, satellite imagery, open sources analysis and beyond?
4) How international verification could be applied to material released from nuclear weapons programmes.

Examination of these questions in the context of the topics presented (notably excluding the final question in view of the uniqueness of its scope), reveals that they can be distilled to one single, overarching concern, namely:

> *Which technology developments and R&D are needed to deter the proliferation of nuclear weapons, through early detection of the misuse of nuclear material or technologies?*

It is from the perspective of this overarching concern that we report the outcome of the Working Group 2 proceedings.

Background

The international safeguards arena is recognized by many who work in this field as being a highly complex environment. Safeguards conclusions, the final outcome of International Atomic Energy Agency (IAEA) verification activities, result from an analysis of all available and relevant information. Information gathering facilitates the analytical process applied in arriving at these safeguards conclusions, with technology playing a critical role in providing definitive empirical information, and also in processing and managing information. The challenge is to properly identify and place technology in the overall cycle of information collection, management, evaluation, utilization and credible knowledge generation.

IAEA safeguards, implemented through a series of interdependent verification activities, provide credible assurance to the global community as to the peaceful utilization of nuclear material and activities in States that have concluded Safeguards agreements. The overall goal of deterring the proliferation of nuclear weapons is thus supposed to be achieved through establishing an

unacceptable risk of detection for potential proliferators. Therefore, the future of safeguards technology and respective trends and priorities should be evaluated from the perspective of increasing this risk.

The Implementation of safeguards under standard Comprehensive Safeguards Agreements (CSA) and under CSAs with Additional Protocols (AP) presents different challenges in terms of how best to establish deterrence factors. In safeguards implemented under a CSA alone (often referred to as **traditional** safeguards), where facility inventories and operations are declared by the Operator and verified by the IAEA, the probability of detecting noncompliance may already be considered high enough to deter potential proliferators, while the Agency's ability to address adequately proliferation risks outside of the 'declared domain' is obviously limited. This former assertion is based on historical records of compliance and historical evidence relating to real proliferation 'cases' originating from undeclared activities, where the likelihood of detection is still far from the desired 'deterrence threshold'. Where an AP is in force, the IAEA has the potential to increase significantly the probability of detection of undeclared activities, not only through comprehensive analysis of information available from satellite imagery, open sources and international trade analysis (i.e. from information available through a network of external providers), but also through its own physical presence and the ability to apply appropriate techniques directly in locations of concern. Under AP implementation (referred to herein as **non-traditional** safeguards), where not just the accuracy but the completeness of a State's declarations may be verified directly, the risk of detection of undeclared activities must, therefore, also become sufficient to deter aspiring proliferators. Thus, the goal is to create a risk of detection comparable to that already achieved under traditional safeguards.

The challenges in terms of defining the direction of future R&D for safeguards and verification technology are therefore to achieve efficiencies in more traditional approaches, while at the same time increasing the risk of early detection of undeclared nuclear material and activities. It is recognized that future R&D will need to address both of these respective challenges.

Working Group Findings

For reporting purposes, the findings of the working group are organized according to the applicability of technologies to **traditional** or **non-traditional** safeguards, and, through categorization of these findings under the headings of *hardware, software and procedures* and *conceptual.* In the hardware category, technologies were distinguished also based on ownership of the data acquisition technology, i.e. whether equipment was envisaged to be operated by the IAEA, or by a network of third party technology holders with only the information gathered there being made available to the inspectorate(s).

Traditional Safeguards — Hardware

For traditional safeguards it was recognized that the hardware available at present is in general addressing adequately fundamental IAEA needs, and that further developments should therefore

focus mainly on improving efficiencies (i.e. increasing cost economies, reliability, maintainability and user-friendliness, keeping abreast of continual advancements in technologies and of the evolution of verification approaches). Specific technology areas that could benefit from continued development include:

- Non-destructive measurement systems (NDA), in particular, gamma-spectroscopy and neutron counting techniques.
- Containment and surveillance tools, such as tamper indicating seals, video-surveillance, surface identification methods, etc.
- Geophysical methods for Design Information Verification (DIV) and safeguarding of geological repositories, which are recognized as growing needs requiring expansion of their respective technological bases.
- New tools and methods for real-time monitoring could radically improve efficiencies in the area of traditional safeguards.

Furthermore, the Working Group acknowledged that a 'building block' (or modular) approach should be adopted towards technology development, enabling equipment to be upgraded efficiently as technologies advance.

Declarations provided by Operators and Member States are directly validated during verification missions. The information gathered is then analyzed for consistency. Except in the area of joint-use equipment, where special considerations relating to its use are applied, it is recognized that equipment and technology deployed by the IAEA in applying traditional safeguards should, as a rule, be IAEA-owned and operated; therefore, network providers of equipment are not anticipated in this area.

Some additional considerations were highlighted during the Working Group discussions. A distinction should be drawn between toolboxes that are needed to verify facility compliance under the CSA, and Complementary Access (CA) toolboxes utilized under AP provisions. Opportunities to improve the acceptance of new technologies by facility operators need to be identified. Due to the complexity of the various implementation scenarios, specific and comprehensive requirements are difficult to articulate, therefore a balance should be found between technology 'push' and 'demand pull' as technology advances are realized and international safeguards systems evolve. Evident and specific technical needs include, in particular, improving battery life/power usage; expanding the scope of underwater instrumentation; and, exploring further the feasibility of wireless communications.

Traditional Safeguards — Software and Procedures

The issue of data-processing architecture is recognized as an issue that increases in importance as the quantities and complexity of safeguards-relevant data continues to expand. Some specific concerns identified by Working Group 2 in this area related to data authentication, application

interfaces, standardization, mega data handling, and the archiving and accessing of historical records. Encryption key management was also identified as a significant concern.

Traditional — Conceptual

Human factors *must* be taken into consideration. All information that is collected will be subsequently analyzed by human beings; this fact should remain foremost as information is gathered, recorded, and transmitted. Based on the evolving safeguards paradigm, increasing collaboration is envisaged between safeguards inspectorates and operators. The appropriate methods and best approaches towards executing that collaboration need to be explored. Multiple and often diverse stakeholder requirements create discrete information challenges. Working Group 2 also recognized that, due to budgetary constraints, cost/benefit considerations will need to be taken into consideration in the evaluation of any new verification activities.

Non-traditional Safeguards — Hardware

As previously stated, it is recognized that the objectives, requirements and activities of a CA visit differ distinctly from those of a CSA inspection. Key attributes of the CA equipment made available to inspectors in the field are identified as automation, portability, versatility, and hands-free operation.

In pursuing its goal to detect undeclared activities, there is an acknowledgement that the IAEA has, and will continue to have, a growing reliance on data and information provided by third parties (including commercial information providers). In the area of satellite-based sensors, increased spatial resolution and broadened spectral range were identified as priorities. Workshop attendees were impressed in particular by the high revisit frequency already achieved by commercial satellite systems as well as by the availability of commercial hyper-spectral sensors and satellite based synthetic aperture radar (SAR) technology. The present lack of tools available to reduce the requisite skills for data interpretation was identified as an area of concern. Extending operational space to “get inside” buildings was mentioned as an additional objective for these types of sensors.

In the area of wide area surveillance, the development of LIDAR-like tools for atmospheric sensing was discussed from the perspective of both potential benefits and certain limitations.

The large numbers, and types, of samples that will result from increased environmental sampling are expected to require an improvement in the performance of instrumentation within the IAEA Network of Analytical Laboratories (NWAL). Next generation mass spectrometry systems, which enable the analysis of smaller samples (at femtogram levels) and improved processing time are needed. The area of micro-analysis, where techniques are needed to determine particle information, such as elemental composition, isotopic information, age, origin, and morphology was identified as being of particular interest. Presentations made to Working Group 2 and the

ensuing discussion revealed micro-analysis to be an evolving area where, although significant advances have been made, many challenges remain.

Non-traditional — Software and Procedures

Working Group 2 noted that the critical element in data and information analyses is the human brain. Limitations of the human brain therefore need to be considered when seeking to enhance the speed and quality of analyses. Approaches are needed that will automate information collection, organization, management and analysis, while optimizing opportunities for human insight. Emerging areas and new technologies, such as the world-wide community of voluntary information providers, open-source information, citizen sensors, citizen problem solvers, and crowd sourcing, represent opportunities that might be leveraged in the application of non-traditional safeguards. The applicability of open-source geospatial information to safeguards was recognized. For information derived from the Internet, extension of the language base for accessing and utilizing information and the ability to organize information in useful formats were viewed as important next steps. Validation of information and its rating for pertinence were seen as continual challenges.

The value of using open source software wherever practicable was recognized in that the approach followed in its development and deployment embraces standardization. Open source software has proven to exhibit a shelf life comparable, if not exceeding, commercial software packages.

In the area of image processing, current practices are time consuming and dependent upon experts. There are varying levels of automation; information extraction and interpretation remains challenging, and, change detection and pattern recognition require expert skills. Advances in software are needed to remove some or all of these inherent challenges.

In the growing area of forensics the identification of signatures and indicators is required, based on factors such as fuel cycle associations, geographic origin, age etc.

Non-traditional — Concepts

Recognizing the limitations imposed by the human brain in terms of information assessment and analysis, technologies are needed that will enable the more effective utilization of all information, regardless of its format and origin. There is a need to overcome the information silos that exist between the entities performing inspection, data collection, and analysis activities, to allow for the more effective and efficient use of all available information.

Working Group 2 noted that not all information gathered is useful in enabling the IAEA to reach safeguards conclusions and that simply increasing data volumes may not be the solution. Sometimes more is not better; it is just more, therefore efficiency in data collection should be a fundamental consideration as new software tools are developed.

Summary

An enormous amount of technical information was provided to Working Group 2 over the course of the workshop. A range of issues were covered, from specific technical concerns to high level concepts. Whereas it is evident that the contribution of technology remains crucial to maintaining the overall effectiveness of safeguards, further developments are needed with increased emphasis on the detection of undeclared activities. Such technologies will be made available resulting both from IAEA in-house capabilities and the activities of a network of external providers. Partnerships will remain central to achieving continued and successful progress.

Next steps

Working Group 2 recognized the value of promoting continuing dialogue, in a format such as that achieved through this workshop, where technology providers, developers, users, and regulators all participated in the discussion. Dialogue of this nature could be accomplished through future workshops, networks, and other engagements.