DEPARTMENT OF SAFEGUARDS WORKSHOP
ON
SAFEGUARDS TOOLS OF THE FUTURE

INTERNATIONAL ATOMIC ENERGY AGENCY
DEPARTMENT OF SAFEGUARDS

December 2005

"This report is produced under the auspices of the International Atomic Energy Agency. It is based on all information and knowledge available to the author(s) but does not necessarily reflect the policy expressed or implied by the IAEA or its Member States."

TABLE OF CONTENTS

1.0 Executive Summary

This document details the results of the "Safeguards Tools of the Future" workshop held in Newport, Rhode Island, USA from October 10 – 14, 2005. The International Atomic Energy Agency (IAEA), with the support of the U.S. Safeguards Support Programme, convened this meeting to set out a roadmap for identifying and developing new technologies to support inspectors in the field. The workshop brought together technical experts from government, academia, and private industry to explore technology trends and to identify the characteristics of technology that would be available in five to ten years to enable Agency safeguards inspectors to perform their jobs more effectively and efficiently.

Twenty-three people presented papers on new or future technologies that could improve inspection efficiency and effectiveness. The presentation topics included Sensors and Surveillance, Tracking and Navigation, Communications, Security, Computing, and Information Analysis. The presentations were as varied as virtual reality tools, geo-collaboration tools, wearable computers, "reachback" technology, statistical data mining, and geo-location devices that use inertial guidance when GPS signals are not available, such as in a building or underground. A video recording of the presentations is available on DVD from the Department of Safeguards or from the U.S. Safeguards Support Programme.

Dr. Shirley Jackson and Dr. Vinton Cerf were keynote speakers. In her keynote speech, Dr. Jackson, President of Rensselaer Polytechnic Institute and former chairperson of the U.S. Nuclear Regulatory Commission, highlighted the Agency's need to harness new technology to fulfill its missions. She emphasized, however, that technology alone is an incomplete solution and she cited the need for strong educational institutions to provide the Agency with staff who are educated in science and technology. In the second keynote speech, Dr. Vinton Cerf, Vice President of Google, Inc. and one of the inventors of the Internet, discussed the future of the Internet and how the convergence of widely varied applications on the Internet might affect the manner in which Safeguards inspectors perform their job, for better and for worse.

The workshop participants envision a world in which inspectors are able to make better decisions in the field with the assistance of technology that would provide them with improved data gathering and analysis tools and that would connect them in near real-time with Agency managers, safeguards experts, and Agency databases. These capabilities would be especially beneficial during complementary access inspections when access to up-to-the-minute information could affect the decisions that an inspector makes while he is onsite. Agency staff in Headquarters, Tokyo, or Toronto would be able to see inspection data in near-real time and could interact with inspectors in the field to ensure that safeguards data is gathered as efficiently as possible. The inspectors would also receive improved support both before and during inspections via an Operations Centre that would be staffed around the clock.

Within the next ten years, inspectors will be able to enter a facility and proceed to a single location where they could download data from all installed safeguards sensors. This would be accomplished via an internal network that would poll safeguards system sensors and store the data on a server that could be accessed easily by the inspector. A communications device would be configured to collect data from legacy systems, as well as new safeguards systems. The device would also have analytical tools, such as NDA, NDE, or environmental monitoring, to help the inspector decide if further inspection action would be required before the inspector leaves the site. The device would connect the inspector to IAEA Headquarters

to provide voice or data communication capability. The data network would allow the inspector to “push” information to Headquarters, thereby providing Agency managers the ability to evaluate data in near real time, and to “pull” information from Agency databases for further evaluation in the field. The ability to push and pull information would facilitate better and more timely decisions because the inspector would be able, while still onsite, to evaluate his inspection data within the context of other State related safeguards information. At Headquarters, databases would be integrated to provide seamless information flow. A common graphical user interface would facilitate the data mining so that the inspector would not have to be concerned with the arcane knowledge of where certain types of data are stored. The Headquarters network would have a security system with predetermined access rights so that individuals could see only the information for which they had a clearance and a need to know.

The workshop participants recommended several courses of action to assist the Agency in developing a technology strategy. The report authors grouped the recommendations according to the following categories: 1) Communications, 2) Data Processing, 3) Security, 4) Sensors and Surveillance and 5) Non-Technology Related Issues. The participants’ strongest recommendation is to establish an operations centre at Agency Headquarters. Although an operations centre is not a technology per se, it does provide a framework for implementing many of the technologies identified by the workshop participants.

Operations Centre Recommendation

The workshop participants identified the need for a Headquarters-based operations centre. The purpose of the operations centre is two-fold: to provide Agency staff a common operational picture (COP) of safeguards activities worldwide and to provide inspectors with a single point of access to Agency managers and subject matter experts who might be needed to support inspection or maintenance activities. The operations centre would provide Agency staff with command, control, communications, and intelligence sharing tools. Agency managers would use the operations centre to assess at a glace ongoing activities in the world of international safeguards. Inspectors could use the room to prepare for inspections, checking to see if equipment has been delivered or receiving the latest intelligence and safety briefings.

The operations centre would also benefit inspectors by providing a single point of access at Headquarters for solving emergent problems, answering inspection-related questions, and for exchanging information with other staff members to facilitate timely, well-informed decisions in the field. Inspectors could contact the operations centre staff via telephone, satellite link, or the Internet. The operations centre staff, in turn, would be able to reach key Agency managers, technicians, and subject matter experts quickly via the telecommunications system, thereby providing field personnel access to others who might provide assistance. This would enable the field personnel to resolve technical problems, make decisions, expedite clearances or authorizations, and solve emergent problems. The field personnel could work more confidently in the field knowing that they could access any type of expertise quickly.

Communications Recommendations:

- Upgrade network infrastructure to provide:
    - Indoor / Outdoor access while working onsite at a facility.
    - Security/authentication (Sandia National Laboratory, Section 5.4.3; Section 6.3).
    - Redundancy.

  - High speed (2-way) (Cisco, Section 5.3.1).
  - Portability.
  - Internet Protocol

- Near-Term
  - Satellite (Broadband Satellite Communications, Section 6.10,; Re-configurable Antennas, 6.5) / Current Cellular / Land line / WIFI (Sections 6.6)

- Long Term
  - Software Radio (Section 6.4) / Land Line

Data Processing Recommendations:

- Establish a common look and feel for interfaces to make access to all databases easy and user-friendly.
- Ensure the ISIS Re-engineering Project (IRP) is compatible with Agency's technology vision .
- Continue to invest in intelligent search engines, searchable content.
- Deploy software to overlay geo-tagged information from multiple sensors / GIS.
- Acquire data visualization and data fusion software.
- Evaluate use of virtual reality for inspection preparation and training. (LANL, Section 5.5.3)
- Deploy automated data reduction and analysis tools. (Object Recognition, Section 5.1.1)
- Evaluate statistical data-mining and other analysis tools for the identification of anomalies. (Carnegie Mellon University, Section 5.6.2)

Security Recommendations:

- Automate Authorization Access (Multi-Level Security Systems and Guards, Section 6.3)

Sensors and Surveillance Recommendations:

- Deploy an integrated multi-functional secure data-collection devices (e.g., wearable computer) that are compatible with legacy sensors. (Carnegie Mellon University, Section 5.5.1; XRF Technology, Section 5.1.4)
- Establish a central collection point at the facility where data from different sensors can be collected.
- Deploy autonomous sensors.
- Provide HQ access to on-site sensors.

Non-technology Issues: In the course of breakout sessions, the participants identified several issues that they considered important for the Agency to study, but which they deemed outside the scope of the workshop. These issues related to Agency policy or to issues outside the control of the organizations represented at the conference. The workshop participants believe that the Agency would benefit from studying these issues more thoroughly.

Personnel Issues**:**

1. The Agency should review their staffing levels and work distribution to ensure that the Department has sufficient numbers of people to perform the analysis of information.
2. The Agency should continue to provide training for its personnel so that they are able to maintain the knowledge and skill necessary to perform their jobs at the highest level.
3. If the Agency decides to implement an operations centre, the Agency should evaluate the need to operate the centre around the clock, seven days per week.
4. The Agency should investigate establishing a network of subject matter experts who would be available to answer questions posed by inspectors working in the field.

Policy Issues:

1. The Agency should develop the capability to share information, via a computer network, among Agency workgroups.
2. The Agency should evaluate the impact of empowering inspectors with greater connectivity. More actionable information in the hands of the inspector in the field in near-real time makes it possible for the inspector to act on that information before he or she leaves a site. This could yield a better understanding of the activities ongoing at a facility. It could also mean a cost saving because information can be gathered in fewer trips.
3. Board of Governors and Member State approval may be required before certain technologies could be implemented.

Management Issues:

1. The Agency should evaluate its decision making processes to determine if more decisions can be make by the inspector in the field.
2. The Agency should evaluate where data analysis will be performed: in the field using or at Headquarters.

2.0 Introduction

This document details the results of the “Safeguards Tools of the Future” workshop held in Newport, Rhode Island, USA from October 10 – 14, 2005. The International Atomic Energy Agency (IAEA), with the support of the U.S. Safeguards Support Programme, convened this meeting to set out a roadmap for identifying and developing new technologies to support inspectors in the field. The workshop brought together technical experts from government, academia, and private industry to explore technology trends and to identify the characteristics of technology that would be available in five to ten years to enable Agency safeguards inspectors to perform their jobs more effectively and efficiently.

The premise of the workshop was that Agency inspectors require new tools to collect data from safeguards monitoring systems and to exchange data and information with Agency Headquarters personnel in near-real time. Headquarters personnel would corroborate and analyse the data and provide the inspector information that he or she could use as the basis for further inspection action before the inspector left the facility. The focus of workshop discussions was on identifying the capabilities that would be required by Agency field and Headquarters personnel and on identifying technologies that could be implemented in the next five to ten years to provide Agency personnel with the tools necessary to realize the Agency’s vision. Workshop participants discussed technology trends, gathering sensor and other safeguards data, secure transmission between the field and Headquarters, data management systems, tracking systems, data visualization and presentation tools, and information security.

3.0 Workshop Overview

3.1 Workshop Methodology

There were three, interwoven parts to the workshop. The first part was a series of technical presentations that were designed to educate the workshop participants in subjects that were outside their area of expertise. This meant presentations on Agency safeguards for technical experts who were unfamiliar with the mission of the Department of Safeguards, and presentations on state-of-the-art and emerging technologies for Department of Safeguards personnel. The second part of the workshop was a forum on the challenges that Agency inspectors could face in the future and technologies that could be implemented to solve the identified challenges. The third part of the workshop was documenting the participant’s discussions and conclusions.

Workshop planners dedicated fifteen hours to formal presentations by Agency personnel and selected representatives of public and private institutions, referred to hereafter as the Technical Community. A synopsis of each technical presentation is provided in Section 5.0.

The workshop forum was conducted with the aid of two scenario-based exercises. The exercises provided a framework for structuring debates on different approaches for addressing the Agency’s technology needs. The scenarios were based on real-world inspection problems that inspectors could face while performing inspections with a complementary access. At the start of each exercise, participants were given an overview of the exercise process. Following the orientation presentation, the meeting participants were sorted into two working groups. Group assignment decisions were based on establishing broad technological expertise and diversity of opinion and culture in each working group. The working groups were divided into teams of about 20 people each and included representatives from the Agency and guest organizations.

The Agency tasked each group with analysing the scenario presented to them, developing a plan for solving the problem, identifying technologies that the Agency could use to assist them in implementing the solution, and making recommendations on how the Agency should proceed. The first scenario addressed inspection activities in the field during an inspection with a complementary access. The second scenario focussed on the activities at Headquarters that were necessary to support inspectors in the field who were equipped with a state-of-the-art communications devices. At the completion of each exercise, a representative from each group briefed the plenum on the results of their group's discussions.

The third and final phase of the workshop was dedicated to briefing the Agency on the Technical Community's recommendations and drafting a summary report.

A copy of the workshop agenda is included as Appendix 1.

3.2 Keynote Speakers

Dr. Shirley Jackson and Dr. Vinton Cerf were keynote speakers. In her keynote speech, Dr. Jackson, President of Rensselaer Polytechnic Institute and former chairperson of the U.S. Nuclear Regulatory Commission, highlighted the Agency's need to harness new technology to fulfill its missions. She emphasized, however, that technology alone is an incomplete solution and she cited the need for strong educational institutions to provide the Agency with staff who were educated in science and technology. In the second keynote speech, Dr. Vinton Cerf, Vice President of Google, Inc. and one of the inventors of the Internet, discussed the future of the Internet and how the convergence of widely varied applications on the Internet might affect the manner in which safeguards inspectors perform their job, for better and for worse.

4.0 Capabilities Required for a "Connected" Inspector

The workshop participants identified capabilities that they thought Agency inspectors would require in the future. The list of capabilities developed by the participants is not intended to be an exhaustive treatment of all capabilities required by future Agency inspectors. The participant's assessment was made within the context of the scenarios presented to them and was constrained by the time available for discussion and the expertise resident in the working group. The participants used the brainstorming process to identify capabilities that could be required to support a "connected" inspector. Afterwards, the participants focused on capabilities that could be satisfied with a technological solution. The list of capabilities is provided here to provide context for the technology solutions that are presented in Section 7.0

4.1 Sensors and Surveillance

- Ensure compatibility of existing equipment with new technologies.
- Comprehensive suite of globally integrated sensors.
- Integrated multi-functional secure data-collection device.
  - Interfaces with all new and legacy sensors (e.g, WiFi for new, serial for old)
- GPS/inertial/laser geo-location for geo-tagging other data.
- Ability to collect radiation data.
- Efficient and autonomous sensors.
- Voice recognition for text conversion / data input.
- Large storage capacity.
- Extensible
  - Imagery (multi-spectral)
  - Environmental real-time analysis

  - Facility penetrating sensors.

4.2 Communications

- Real-time collaboration with subject matter experts and Agency managers.
- Access from the field to information and expertise resident at Headquarters or at locations throughout the world.
- Capability to provide an inspector in the field with a response from Headquarters within approximately 4 hours of the original request.
- Ability to access/confirm declared facility operations using information from Headquarters and the field.
- Networking Infrastructure.
  - Secure, highly available, high-bandwidth communication.
  - Access to communications while inside facilities is desirable.
  - Single phone number staffed by a qualified Agency person with whom an inspector can speak at anytime of day.
  - Near real-time identification and access to information, SMEs, and analysts.
  - Collaboration tools to facilitate information exchange between inspectors and Headquarters personnel.
  - Analyse information provided by inspector.
  - Provide and display situational awareness [e.g., common operating picture/ (COP)].

4.3 Data Processing

- Central collection point at a facility where data are stored.
- Common look and feel of interfaces to make access to all databases easy and user-friendly.
  - Easy access to database information without having to look for it or to know where it is.
  - Should feel like a single user interface.
  - Query expert system and knowledge base.
- Imagery (e.g., pattern recognition, change analysis).
- On-site material analysis tools (DA, NDA, NDE).
- Spectrum analysis (e.g., isotope, metal).
- Ability to process data on-site as well as store / forward data to Headquarters.
- Data review and interpretation technologies to convert large amounts of data into useful information for real time decision making.
- Front-end analysis of data when generated.
- Automated state of health and integrity reports from installed systems.

4.4 Security

- De-compartmentalize databases and information resident at Headquarters.
- Provide for remote access to Headquarters information from the field.
- Capability to parse information based on access rights (roles).
- Headquarters access to onsite Sensors.

5.0 Technical Presentation Synopses

Twenty-three people presented papers on new or future technologies that could improve inspection efficiency and effectiveness. The presentation topics included Sensors and

Surveillance, Tracking and Navigation, Communications, Security, Computing, and Information Analysis. The presentations were as varied as virtual reality tools, geo-collaboration tools, wearable computers, “reachback” technology, statistical data mining, and geo-location devices that use inertial guidance when GPS signals are not available, such as in a building or underground. This section summarizes each presentation. A video recording of the presentations is available on DVD from the Department of Safeguards or from the U.S. Safeguards Support Programme.

5.1 Sensors and Surveillance

5.1.1 ***Smart Surveillance/People Vision (IBM Research)***

The IBM Smart Surveillance System is middleware for use in surveillance systems. It provides video-based behavioural analysis capabilities. The Smart Surveillance System Release 1 (S3-R1) comprises two components: the Smart Surveillance Engine (SSE), which provides front end video analysis capabilities; and Middleware for Large Scale Surveillance (MILS), which provides data management capabilities.

S3-R1 provides the following functionality.

1. *Web based Real Time Alerts,* including Motion Detection, Directional Motion, Abandoned Object, Object Removal and Camera Move/Blind.
2. *User Designed Alerts*: Specified using simple SQL like interface.
3. *Web based Event Search* using Object Type, Object Size, Object Speed, Object Location, Object Colour, Track Duration & Compound Queries
4. *Web based Event Statistics* including Distributions & Moments

The Smart Surveillance system utilizes the following technologies:

- *Object Detection* in the presence of distraction motion.
- *2D Object Tracking*: Multi-object tracking with occlusion resolution.
- *Object Classification*: View independent object classification.
- *3D Object Tracking*: Precise 3D location using standard cameras.
- *Multi-scale Tracking*: Automatic PTZ Camera control to track objects.
- *Multi-camera Handoff*: The ability to track an object across cameras.
- *Face Cataloguing*: Captures faces at large distances from the camera.
- *XML Metadata* Representation for an object and its motion attributes.
- *Extensible Engine Architecture* for plug and play video analytics.
- *Real Time Event Indexing*: Scene events are instantaneously available for searching in a distributed database environment.
- *Web service interfaces for Event Search & Retrieval*: support the rapid application development of customer specific applications.
- *Scalable Backend System*: COTS database technology allows for both distributed surveillance and scalability.

5.1.2 ***Position Orientation System, Land Survey (Applanix, Inc.)***

Position Orientation System, Land Survey (POS LS**)** is an all-terrain land positioning/ navigation system, housed in an ergonomic backpack. The combination of an Inertial Measurement Unit (IMU) and a Real Time Kinematic (RTK) Global Positioning System (GPS) receiver makes POS LS a robust positioning solution for land survey, optimized for pedestrian use. POS LS provides reliable position accuracy in areas where conventional optical or GPS survey are ineffective or impossible. The system monitors position quality continually and requests Zero Velocity Updates (ZUPTS) to limit error propagation, while automatically using any available GPS.

5.1.3 *Reachback Technology (MITRE Corp.)*

This presentation outlined the use of dust networks, wireless relay communications for RF challenged environments, and reachback communications. Dust networks are self-forming and self-healing with every node acting as a battery powered router. The distance between nodes is on the order of 10 - 20 meters indoors and greater than 100 meters outdoors. Each node can function as a relay and supports “data” collection. Each network mote can support multiple sensors, controllers, or actuators.

Wireless relay communications enable secure two-way voice, two-way data, or one-way low rate video communications among a small team and its field command element operating in an RF-challenged environment. MITRE has tested a prototype system in shipboard and subterranean (cave) environments.

The presenter concluded his presentation by saying that sensor networks are evolving to include self-forming behaviour, thereby making deployment of sensor networks in harsh environments easier. These ad hoc networks are an immature technology, except in highly specialized situations. A promising technology that is growing rapidly is very small aperture terminal (VSAT). It has the potential to provide high capacity reachback from virtually any location

5.1.4 *XRF Use for Controlled Materials Identification and Seal Authentication (Pacific Northwest National Laboratory)*

Portable XRF devices are able to assay the composition of material by detecting and analysing fluorescence radiation. Portable XRF instruments, which are commercially available, can be used to identify elements and alloys non-destructively and rapidly. This can be done for elements that are controlled by international export control agreements and those used in authentication of nuclear material safeguards seals. This technology could be used to identify materials of proliferation concern during complementary access inspections under Additional Protocol. It could also be used with elemental taggants in tag/seal applications.

5.1.5 *Nano-technology: Devices for the Terabit Communications Network (Bell Laboratories)*

This presentation described several of the underlying nano-technologies, such as MEMS, high speed electronics, quantum cascade lasers, IP opto-electronics, and SiOB. It also provided examples of applications for these technologies. Of interest to safeguards applications is a technology that is characterized as a “dog on a chip”. In essence, it is a computer chip that can be programmed to detect the presence of certain chemicals. The presentation also addressed the future of nano-technology.

5.2 Tracking and Navigation

5.2.1 *Real Time Tracking and Surveillance (Oak Ridge National Laboratory)*

Oak Ridge National Laboratory (ORNL) is developing a real time asset tracking and surveillance system that may become the technical equivalent of the “two person rule” for some domestic safeguards operations. The major efforts associated with this task are the integration and adaptation of commercial-off-the-shelf (COTS) active RF technologies into an unobtrusive system that provides real-time tracking of sensitive nuclear material assets and people who have access to them. The system design will provide up-to-the-minute information on the state of in-process materials while applying rules-based algorithms designed to provide immediate detection of theft or diversion.

5.2.2 *Mobile Information System for Safeguards Inspectors (European Union/Joint Research Center)*

The objective is to increase the efficiency of inspections by bringing decision capability to the field, rather than making decisions exclusively at headquarters. This is consistent with the new investigative character of inspections introduced by the Additional Protocol. It means that sensitive data must to be brought to the field and presented to the inspector in the context of current measurements.

The goal is to develop a GIS-based application to assist Safeguards inspectors in the on-site verification of declarations related to the Additional Protocol, as well as to supporting their local investigation capabilities. The idea is to make available during the inspection all relevant data and allow local decision-making by comparing declared and archived data with real-time data. Access to remote data would be made through secure, wireless connections (IPSec protocol) over heterogeneous networks (Wi-FI, Bluetooth, GPRS).

The system is easily connected to local, preferably wearable, acquisition devices. An inspector will wear the equivalent to a digital jacket, filled with small, low-power dedicated instruments, each one targeted to specific measurements. Examples: portable radiation meters, distance meters, portable gamma spectrometers, etc. With this capability, an inspector could request assistance from headquarters-based experts and expect to receive a timely response.

5.3 Communications

5.3.1 *The Future of Data Communications (Cisco)*

This presentation reviewed the expansion of the Internet from its earliest days through the present and projected a future vision of the Internet based on present-day trends. The presenter showed that the Internet is ubiquitous in countries in which the U.S. has economic or military ties. This is due to the early roots of the Internet as a Defence Department project. The regions that are not well covered are located primarily in Africa, the Middle East, and countries of the former Soviet Union. The clear technology trend lines are the deployment of National Research and Engineering Networks (NRENs); National Internet Exchanges (IXPs); national and consortium fiber rings; broadband to government agencies, schools, hospitals, and business; and undersea cable to developing countries. These trends are driven by business factors, education, and national programs to become more competitive. It is projected that large areas of Africa, the Middle East, and central Russia will not have fiber installed in the foreseeable future. The Internet will be shifted from IPv4 to IPv6 over the next decade.

The major backbones of the Internet in the next ten years will be telephone companies and regional research/educational consortia. It will run primarily IP communications protocol to transmit voice, video, and data. High capacity fiber will be used more commonly, with some use of optical cores. Wired and wireless internet will remain important components of future communications networks. GSM/3GPP will be used heavily for voice, but its use for data transmission is unclear due to capacity limits and business rules. Geo and Meo satellites will remain important for temporary and “on demand” communications needs, especially in Central Asia. Satellites will be edged out over time however as a primary communications media.

5.3.2 *Geo-Collaboration Technology for MoMoSat (Dialogis)*

This presentation provided an overview of Dialogis's product Mobile Monitoring over Satellite (MoMoSat.) MoMoSat is a map-based information management tool designed for worldwide mobile communications. The system is intended to meet the needs of a worldwide, mobile workforce, who works in teams, and who demand current and historical geo-information. These individuals must have the capability to communicate securely in real-time and must gather location-based multimedia information. The MoMoSat system provides the user with worldwide mobile access to maps, documents, and external databases. It also provides a spatial search for relevant, 'nearby' information and task management and monitoring. In the future, Dialogis plans to add the following functionality:

- redlining map views.
- automatic combination of GPS tracks and multimedia data.
- integration of sensor web data.

The presenter asserted that a geo-collaboration system can help safeguards inspectors to:

- structure and manage large amount of different information.
- verify state declaration, especially by
    - orienting the inspector on the inspected site.
    - suggesting locations for environmental sampling.
    - presenting information (on a map).
    - exploiting synergism between different information sources using the geographic coordinate.
- improve reliable and secure communication between inspectors and headquarters.

5.3.3 *HazMatCam (Idaho National Laboratory)*

The Hazmat Cam Wireless Video System was developed by the Idaho National Laboratory for use by National Guard Civil Support Teams during their mission of emergency response to incidents involving weapons of mass destruction. The Hazmat Cam Wireless Video System sends secure, real-time video from emergency responders on the ground in the hot zone to a command post a safe distance away. Developed to transmit live images from inside a potentially contaminated area, the system comprises a handheld wireless video camera, a receiver and viewing console, and an optional extension link allowing the command post to be placed up to five miles from danger. The system can connect to the internet and function like a "web cam" allowing experts with the proper authorization to view the real-time image from virtually anywhere around the world. It can be fully deployed by one person in a standalone configuration in less than 10 minutes. The on-scene camera transmits encrypted, low-frequency FM signals to a true diversity receiver with three antennas. This unique combination of encryption and transmission technologies delivers secure, clear, interference-free images to the command post under conditions where other wireless video systems fail. The lightweight camera is completely waterproof for quick and easy decontamination after use. The Hazmat Cam has been tested in a variety of different structures and environments and is now commercially produced under the name Visual First Responder.

5.4 Security

5.4.1 *Cyber Threats of the Future (Carnegie-Mellon University)*

This presentation described some of the attack strategies that computer hackers are launching against computer systems. The threats include the Scob Trojan attack, Command and Control Networks, Internet Extortion, Electronic Fraud, and a new generation of Trojan horses that listen for data packets with specific identifying characteristics, like a TCP window size of 55808. For the 55808 attack, the hackers are looking for information embedded in the packet header in order to detect sequence and port numbers which are likely to convey encrypted information about the destination (controller) IP and port to be used by the infected host for subsequent communication.

The presenter continued to say that the fundamental problem to be solved is one of system survivability. Computer systems must perform their mission in the presence of attacks, accidents, and failures. This can be accomplished by implementing security systems which provide confidentiality, authentication, integrity, access control, availability, and non-repudiation. Systems must also be redundant and diverse.

5.4.2 ***Malicious Insider Threat (MITRE Corp.)***

This paper summarizes a collaborative, six month ARDA NRRC challenge workshop to characterize and create analysis methods to counter sophisticated malicious insiders in the United States Intelligence Community. Based upon a careful study of past and projected cases, the team developed a generic model of malicious insider behaviors, distinguishing motives, (cyber and physical) actions, and associated observables. The paper outlined several prototype techniques developed to provide early warning of insider activity, including novel algorithms for structured analysis and data fusion. The presenter reported the assessment of their performance in an operational network against three distinct classes of human insiders (an analyst, application administrator, and system administrator), measuring timeliness and accuracy of detection.

5.4.3 ***Secure Remote Internet Access to Sensors and Seals (Sandia National Laboratory)***

This presentation described a Secure Remote Internet Access to Sensors and Seals system designed by Sandia National Laboratory. It defined a secure sensor platform (SSP) as an electronics platform that has been designed to be versatile for monitoring a wide variety of sensors, on an application-specific platform, and communicate the results to a host computer for analysis. The SSP would provide:

- An FM transceiver
- Secure translator Internet access
- Reduced power requirements and platform volume
- More robust communication protocol with sign and forward
- Intrinsic code verification (ICV) signature generation
- Collision avoidance for RF communication
- Fiber optic loop seal monitoring enhancements
- Data collection and analysis tools

The SSP could accommodate a variety of sensors, including: Loop Seals, temperature, motion, gamma spectrometry (Q306), conditioned analog signals, digital signals and controls.

5.5 Computing

5.5.1 ***Wearable Computer Applications (Carnegie Mellon University)***

The convergence of a variety of technologies makes possible a paradigm shift in information processing. Lightweight electronics, displays and wireless broadband communication make wearable computing technology feasible and cost-effective. Decades of research in computer science provides the technology for hands-off computing using speech and gesturing for input. Wearable computers can communicate seamlessly with sensors and other devices in a pervasive computing environment.

Wearable computers deal in information rather than programs, becoming tools in the user's environment much like a reference manual. The wearable computer provides portable access to information. Furthermore, the information can be automatically accumulated by the system as the user interacts with and modifies the environment thereby eliminating the costly and error-prone process of information acquisition. This research defines a new era of human-centric computing, focusing technologies on human needs, augmenting their capabilities and productivity, ushering in an age of context-aware computing and proactive help. The goal is to get the right information to the right person at the right time, providing just-in-time help.

Carnegie Mellon University has developed over two-dozen generations of wearable computers, each addressing a different class of applications. We have deployed several prototype systems in domains such as manufacturing (Electric Boat, Boeing) and operations/maintenance (U.S. Marines, Bombardier, Compaq). For example, the VuMan3, which was used by the U.S. Marines for vehicle inspection, and proceed with a taxonomy that captures lessons learned from several generations of our wearable computers in accessing remote information and experts. Another example is the MoCCA. It supports a group of geographically-distributed field service engineers. Its asynchronous capabilities for team problem-solving include audio bulletin boards and tips allowing collaboration between remote FSEs and their colleagues. A 40-50% performance improvement in task completion time was already measured compared to a standard help desk

5.5.2 ***Context Aware Computing (Carnegie Mellon University)***

Current research in context-aware computing allows mobile computers to exploit context to anticipate user needs using low cost sensors and machine learning algorithms. Context-aware software agents become a virtual assistant handling tasks according to the user needs and preferences that it has learned.

The presentation included a visionary scenario of a synthetic helper. This technology allows a computer model of a human expert to interact conversationally, provide advice, read procedures and answer questions from a human. Prototypes of this technology have been developed at Carnegie Mellon University.

5.5.3 ***Virtual Reality (Los Alamos National Laboratory)***

The IAEA is constantly faced with budget and scheduling issues that limit the amount of time that inspectors can spend at any given site. Valuable time is needed, and subsequently, budget is also needed, to support on-site training and familiarization of inspectors with the facilities that the Agency is responsible for monitoring. Virtual reality training environments could help to alleviate the cost incurred by the Agency in both time and money of training new inspectors. Virtual reality and “gaming” environments have become more sophisticated and realistic in their interfaces while becoming easier to develop and deploy as training aids. Virtual reality or gaming environments allow users to walk a space and become familiar with the placement of every room, instrument, and area of exclusion (i.e. humans not allowed in region or high radiation areas) within a given facility. Recent developments in gaming environments and the introduction of physics into the motion of the elements in the virtual environment can provide for a realistic walk-through and familiarization of a facility for a user without ever having to leave their desk.

5.5.4 *Auditable Sensor Networks for Remote Monitoring and Surveillance (Rensselaer Polytechnic Institute)*

The concepts proposed in this presentation assumed that the onsite presence of a human inspector is the most critical element of the safeguards system. From this perspective, the presenter proposed enhancement to the systems presently used by the Agency for unattended and remote monitoring. The enhancements included fully automated, remote surveillance and monitoring systems; security improvements to address stealth and insider adversaries, and new defence mechanisms such as redundancy (for reliability), and sensor polling for semantic security, verification, and auditability.

5.6 Information Analysis

5.6.1 *Geo-Spatially Enabled Technology (Canadian Support Program)*

This presentation provided an overview of geo-spatially enabled technology and identified technology trends to orient the group on the future of geo-spatial technology. The presentation addressed positioning and tracking technology, mobile computing, sensor webs, 3D and virtual reality, and integrated information portals. It provided a glimpse of the future by citing examples of how geo-spatial technology has already been integrated with other technologies such as wearable computers.

5.6.2 *Statistical Data Mining (Carnegie Mellon University)*

This presentation addressed the exploitation of large-scale transactional databases in order to help analysts and professionals who are responsible for the early detection of terror attacks. It discussed the statistical and computational issues from both the application’s "pull" end and the researcher’s "push" end.

Applications and case studies illustrated various statistical operations in support of human intelligence analysis. The presenter provided examples of statistically mining transactional data. The underlying technologies include group detection and tracking algorithms that fuse information about links between entities with other relational data. The presenter discussed extensions for dealing with groups that evolve over time, how to rank plausible collaborators, and how to score threat entities.

5.6.3 *Reachback Technologies (Lawrence Livermore National Laboratory)*

This presentation described Lawrence Livermore’s work on a network-centric communications and computing architecture that would support a variety of users, devices, and applications. The network would provide a flexible communication infrastructure to:

- Standardize on the IP protocol.
- Increase bandwidth to the field.
- Enhance reliability though multiple communication paths and redundancy.

- Leverage existing infrastructure and connectivity options.
- Improve usability (faster, easier set-up and use).
- Dedicated space segment and flat rate pricing model.

It would also provide a flexible information management capability to support client-server computing models, web portal models for centralized access to content, tools, workflow-based applications to support processes and protocols, and redundant servers with replication and fail-over between sites.

The benefits offered by this network include:

- Support Field Team to Home Station communication.
- Allow field personnel to interact with remote Subject Matter Experts.
- Allow field personnel to access headquarters-based resources (databases, documentation, modeling codes, etc.)
- Enable collaboration to enhance analysis and decision making.
- Provide information management tools to support a distributed workflow model.
- Support voice, data, and video communication.
- Ensure security of equipment, data, and communications.

6.0 Technologies Discussed During Breakout Sessions

6.1 Redundant Data/Networks

It is common for international organizations to have a redundant internet presence. The rational for redundancy provides numerous benefits. These include the ability to distribute the overall networking load to multiple points as well as the ability for real-time fail-over back up.

Infrastructure enhancement are often necessary to establish redundant systems within multiple physical locations. Each location needs to have access other locations, ideally via fast or moderately fast network connection. This can be done with either a dedicated connection from a wide area network provider (i.e., Sprint, AT&T, UUNET) or via a virtual private network tunnel between facilities. The hardware and storage space at each location must be equivalent, preferably with equivalent memory and processor power. Commercial software, such as Veritas, Oracle, DB2, MySql will perform various level of syncing between the systems.

The use of collocation providers can reduce the networking and administrator overhead for redundant systems. These collocation providers provide physical- and network-isolated hardware storage and can also provide some level of system support. The collocation providers provide the backbone network, including multiple internet access points.

6.2 Directory Based Information Access

Controlling access to information is one of the challenges presented by enabling integrated remote access to information and data resources. One model for controlling such access is authorization based on a directory infrastructure. A directory organizes resources (data files, folders, databases, servers, etc.) into a hierarchy of objects that specify access relationships between users, groups, administrative units. A directory also authenticates individual users and then assigns them to one or more groups. In this model, a user would first authenticate to a common directory server by providing identity information (username and an authenticator such as a password, a token value, a biometric value, etc.). After successful authentication, a user would be assigned to one or more groups, perhaps based on their roles within the

IAEA's business model or concept of operations. The directory can be configured to establish and enforce access rights to the various objects in the directory resource tree. For example, if a particular division within the IAEA is responsible for collecting a certain type of information and storing it in a database, the database and the department can be represented as objects in the directory and access based on the defined groups can be established.

The advantage of directory technology is that it is a powerful mechanism for structuring organizational resources and defining access to those resources based on users, groups, administrative units, and roles. If implemented correctly, a directory can accurately reflect both the organizational structure of the Agency, establish a common authentication capability, and provide a powerful mechanism for defining access to resources within the Agency. Another advantage is that an international standard for directory interoperability exists in the form of the Lightweight Directory Access Protocol (LDAP). The challenge to implementing directory based services and access control, however, is the need to do it across the entire organization if it is to be effective and the need to obtain the support of all the departments and divisions with the Agency in order to achieve the most effective implementation.

6.3 Multi-level Secure Systems and Guards

Multilevel security (MLS) has posed a challenge to the computer security community since the 1960s. MLS sounds like a mundane problem in access control: allow information to flow freely between recipients in a computing system who have appropriate security clearances while preventing leaks to unauthorized recipients. However, MLS systems incorporate two essential features: first, the system must enforce these restrictions regardless of the actions of system users or administrators, and second, MLS systems strive to enforce these restrictions with incredibly high reliability. The high costs associated with developing MLS products, combined with the limited size of the user community, have also prevented MLS capabilities from appearing in commercial products in any large scale (thus, not achieving commodity status and cost reduction). MLS systems come into play because multiple users typically need to access a given system. In the United States, the defense community usually describes a multi-user system as operating in a particular mode. For the purposes of this discussion, there are three important operating modes:

> *Dedicated mode* - all users currently on the system have permission to access any of the data on the system. In dedicated mode, the computer itself does not need any built-in access control mechanisms if locked doors or other physical mechanisms prevent unauthorized users from accessing it.
>
> *System high mode* - all users currently on the system have the right security clearance to access any data on the system, but not all users have a need to know all data. If users don't need to know some of the data, then the system must have mechanisms to restrict their access. This requires the typical file access mechanisms of typical multi-user systems. However, there is a long history of vulnerabilities on all systems where such access restrictions are violated.
>
> *Multilevel mode* - not all users currently on the system are cleared for all data stored on the system. The system must have an access control mechanism that enforces MLS restrictions. It must also have a mechanism to enforce multi-user file access restrictions. These systems tend to be very robust and have a good history of ensuring restriction policies.

Most systems (other than a personal desktop system) operate at the system high mode, which, for most, is “good enough”. If policy permits, this is the desired path to take to reduce cost and complexity. However, if even one access violation is not acceptable, the multilevel mode is the approach to take. It is this third mode that we are interested in where all users are not cleared for all data stored on this system. To support this concept, a trusted environment is needed. First the operating system must implement strict rules of separation (access restrictions) to ensure that access privileges are un-erringly enforced. An example of a trusted operating system is Trusted Solaris. Second, any applications (i.e., database applications) that have multiple levels of information must also enforce these rules. An example of a trusted application is Trusted Oracle. The term “trust” in this case implies the software has gone through a certification process to ensure that it meets minimum criteria. In addition to certification, the system also goes through an accreditation process to ensure that the degree of trust in the system has been adequately addressed. While there is a history of failed products in this realm (failed from a commercial perspective vice technical failure), the two primary areas that have produced some degree of commercial success are guards and trusted servers. Guards are basically a specialized version of a trusted server typically supporting two compartments or security classification levels. Guards provide a boundary protection between two networks operating at different classification levels where information between the two networks needs to be passed in agreed-to manner. The combination of guards and trusted servers could be used in a future IAEA environment to compartmentalized information as privacy or security requirements dictate while, at the same time, permitting selected information to pass into a common operating environment (to create a common operational picture, for example). This would be synonymous with maintaining country separation while having a “coalition” view of the community.

6.4 Software Defined Radios

Software-Defined Radio (SDR) is a rapidly evolving technology that is generating widespread interest in the telecommunication industry. During the last few years, analog radio systems are being replaced by digital radio systems for various radio applications in military, civilian and commercial spaces. In addition, programmable hardware modules are increasingly being used in digital radio systems at different functional levels. SDR technology aims to take advantage of these programmable hardware modules to build an open architecture software based radio system. SDR technology facilitates implementation of some of the functional modules in a radio system such as modulation/demodulation, signal generation, coding and link-layer protocols in software. This helps in building re-configurable software radio systems where dynamic selection of parameters for each of the above-mentioned functional modules is possible. A complete hardware based radio system has limited utility since parameters for each of the functional modules are fixed. A radio system built using SDR technology extends the utility of the system for a wide range of applications that use different link-layer protocols and modulation/demodulation techniques (be it WiFi, cell phone, or very small aperture terminal [VSAT]). The commercial wireless communication (cell phone) industry is currently facing problems due to constant evolution of link-layer protocol standards (2.5G, 3G, and 4G), existence of incompatible wireless network technologies in different countries inhibiting deployment of global roaming facilities and problems in rolling-out new services/features due to wide-spread presence of legacy subscriber handsets. SDR technology shows promise in solving these problems by implementing the radio functionality as software modules running on a generic hardware platform. Further, multiple software modules implementing different standards can be present in the radio system. The system can take up different personalities depending on the software module being used. Also, the software modules that implement new services/features can be downloaded over-the-air onto the handsets. This kind of flexibility offered by SDR systems helps in dealing with problems due to differing standards and issues related to deployment of new services/features. SDR is a promising technology for IAEA to consider due to the potential diverse environment that the inspector will be facing with regards to communications technology inherent in country. It minimizes the suite of equipment that will need to be available while provide dynamic configurability to meet the needs of that specific situation. It also has strong potential to reduce cost in that one platform can perform the task on many devices. While some SDR products are available now, this technology is most likely (from the IAEA viewpoint) a long term (5 to 10 year forecast) technology. However, cell phone technology is well poised to use this technology in the near term.

6.5 Re-configurable Antennas

Having a dynamically configurable radio would be of limited value if the corresponding antenna cannot stay in step with any changes. Reconfigurable (smart) antenna technology is considered by many to be the last technology frontier in antennas that has the potential of leading to large increases in systems performance. Smart antenna systems combine multiple antenna elements with signal processing to optimize the radiation pattern in response to the signal environment. Switched beam arrays and adaptive array antennas are widely used for this purpose. When applied to satellite communications, smart antennas can increase coverage and capacity, improve link quality, decrease size and weight, lower power consumption, and help with direction finding of any jamming or RF threatening sources. Unlike fixed antennas, which can only radiate in one pattern, reconfigurable antennas have the ability to radiate multiple, different patterns through adjustment of their physical configuration. Another example of a reconfigurable antenna involves the introduction of MEMS switches (micro-relays) in electronically steerable antenna. MEMS technology permits physical connection/disconnection of sections of the antenna conductive structure relative to each other and relative to other electromagnetic tuning structure. This flexibility offers benefits for modern radar and telecommunication systems by permitting deliberate alterations in antenna performance to accommodate changes in mission, environment; tolerance to defects and faults and enabling new algorithmic approaches that extend complementary techniques such as software radio and direct digital synthesis. Consequently, new types of devices and architectures are being developed which can enable the realization of steerable antennas that can operate successfully over a large bandwidth. SDR in combination with a reconfigurable antenna provides the highest flexibility to support a system that can potentially operate globally given the same platform.

6.6 WiMAX Technology

WiMAX technology might be available in areas where satellite coverage is not. WiMAX, which stands for Worldwide Interoperability for Microwave Access (a form of broadband wireless access), is based on the IEEE 802.16 standard for wireless metropolitan-area networks (MANs). Global deployment of the technology is expected over the next three to five years, driven by WiMAX's ability to deliver affordable "Last Mile" broadband Internet services. Many of the companies entering the WiMAX market include those that have dominated the WLAN arena. The WiMAX Forum provides a good overview of the company’s participating globally in this technology and the technology’s state of progress. In a typical 20-MHz channel bandwidth deployment scenario, WiMAX Forum certified products will support downlink data rates of 65 Mbps at close range to 16 Mbps at distances of 9 to 10 km, which is enough bandwidth and transmission range to deliver high-speed simultaneous access to voice, data, and video services to hundreds of businesses or thousands of residences. WiMAX's extended range is driving a significant market opportunity and, thus, looks well poised to continue forward. In addition, it's proving useful in delivering broadband services to rural areas where it's cost-prohibitive to install landline infrastructure. Due to the fact that an inspection site can potentially be anywhere, it is advantageous for IAEA to have a range of broadband connectivity options. In combination with VSAT technology, WiMAX can provide high capacity reachback technology for the field inspector. Because WiMAX is also an RF radio, it is technically conceivable that VSAT, WiFi, WiMAX, and cell phone devices may all merge into a single configurable device. It should be noted, however that market forces will make this unlikely.

6.7 Communications Architecture

Routing of communications and data between field inspectors, the operations centre and experts off-site will require several different types of communications links. Communications between the field inspector and the operations centre could use cell phone, landline, mobile satellite terminal, and satellite phone. The link between the operations centre and off-site experts would most likely use existing telecom and data networks.

6.8 Broadband Inspector Concept

This concept would provide inspectors the capability to communicate instantaneously with experts in Vienna and to access web-based data, live video streaming, and safeguards information. Due to the highly mobile nature of field inspectors, some form of mobile broadband infrastructure would have to be taken into the field. Each inspector could be considered a node in the broadband network and could serve to relay packets of data over a large distance. The IAEA inspector presently does not have this ability. If inspectors were to utilize this technology as it is implemented today, they will need to bring several small battery powered nodes to the field or be able to link directly to satellite. Most likely, a combination of both techniques would be necessary to maintain the connection while indoors or under dense tree coverage.

6.9 International Internet Service Provider (ISP) (iPass)

iPass is a worldwide network of internet service providers that have subscribed to a common connection scheme. This service provides local dial-in telephone numbers to an ISP worldwide. The user connects to a local internet provider using their home ISP user credentials. This enhances the speed and reduces the cost for internet access. iPass provides international wireless access from ‘hot-spots’ world wide. These hot-spots include locations like T-mobile, Wayport, and others. iPass also supports non-802.11 connections in countries like Japan, where other forms of wireless (PHS) are more common.

6.10 Portable Broadband Satellite Technology

Portable broadband VSAT (Very Small Aperture Terminal) satellite access from the field is a currently available technology and one that is continually improving in terms of smaller size, lighter weight, faster data rates, and ease of use. Broadband VSAT technology can be used by an inspector in the field to provide a continuous communications connection to IAEA Headquarters or to other support locations. It therefore can serve effectively as an unattended communications gateway during an inspection that can be used continuously or intermittently to transmit and receive voice, video, and data traffic. The increase in bandwidth provided by broadband VSAT can enable new types of applications and interactions with remote experts and resources, such as videoconferencing, audio conferencing, white boarding, streaming video, high resolution image transfer, and real-time sensor data transfer from the inspection site to Vienna.

Portable VSAT terminals now can be purchased with motorized, automated antenna alignment systems that make them easier for a single individual to set up and use. Such systems can now reach speeds up to 2Mbps and are packaged in one or two pieces of wheeled luggage cases that can be checked or carried onto airlines during travel.

The primary advantage of this technology is that it provides a portable, continuous, high-bandwidth connection for the inspectors in the field that can be established from virtually anywhere in the world. Only extreme northern or southern latitudes would not be covered. Satellite is the best form of universal communications when existing infrastructure or availability of other forms of communications at inspection sites cannot be provided or is unknown.

Potential issues and challenges associated with this technology are the following: 1) difficulty operating in high wind conditions (> 20 mph sustained) that can affect antenna pointing accuracy; 2) power requirements that currently exceed practical portable battery capacity; and 3) the need an unobstructed view of the satellite. Approaches to mitigating these potential issues would include: 1) finding a wind sheltered area to locate the terminal during high wind conditions; 2) finding an AC power outlet at the site to power the portable unit or using a rental vehicle as the DC power source; and 3) moving the portable unit as necessary to avoid obstructions that interfere with the view to the satellite.

6.11 Modular Flexible Sensor Communication Methods

To allow a single device access to multiple sensors which have a variety of communication protocols requires both a hardware and a software solution. Facilities worldwide contain a number of technologies used in data collection. These systems have been deployed over many years and are based on a number of technologies. While active efforts are under way to standardize on a single communication scheme, it will be a number of years before all sensors have been replaced; therefore there will be a continued need to support collection from legacy systems for a number of years. Legacy sensors communicate using such technologies as serial: RS232 and RS485, TCP/IP over Ethernet, and multiple RF frequencies, as well as others.

In the long term, a software radio will likely provide the ability to configure a single system to interact with multiple radio devices. These devices may include 802.11, Bluetooth and other short range transmission systems. In the short term, the use of multiple radios will be required.

Hardware exists to allow RS232 and RS485 to be connected to a system over USB or to allow RS232 or RS485 to be connected to an Ethernet port. A USB/Ethernet device also exists. The use of these solutions will allow a single device with either a USB or Ethernet port to connect to any serial device. Ethernet based sensors can also be connected directly or via the USB port. The software drivers for these serial to USB or Ethernet allow the common serial protocols to be transmitted to the computer in a manner that is transparent to the computer. This would allow for the current data collection software to continue to be used. However, ideally, a single piece of software would be created to allow for all collection to be centralized.

Technology Needs: Similarities Between IAEA Inspectors and Emergency First Responders

Emergency responders and IAEA inspectors share many goals in completing their work. Some of these common goals include:

- Increase safety of inspector/responder.
- Shorten time needed to perform inspection/assessment.
- Reduce the need to return to facility/target.
- Reduce the size and weight of carried equipment.
- More reliable communications.
- These common goals result in common technology needs.

The IAEA inspectors may be able to utilize many of the new technologies under development for emergency responders. Some of these technologies are:

- Lightweight radioisotope identification devices (including neutron emitters).
- New smart dosimeters.
- Portable, wireless LAN nodes.
- Real-time video feeds (both ways)

Using new technology already developed for the emergency response community is much more cost effective for the IAEA.

Another point to consider is standardization of equipment. Many standards are currently in place for emergency response equipment. It will be very beneficial to the IAEA in terms of equipment interoperability if they adopt existing standards whenever possible for new equipment.

6.12 Automated Data Reduction And Analysis

The goal of this technology would be to provide algorithms that could provide fast reduction and analyses of data from multiple sources in the field. This would facilitate inspector decision making in the field.

6.13 Virtual Reality

Due to recent advancements in computer gaming technology, it has become easier to make virtual environments that look very close if not identical to the environment that they are trying to emulate. We believe that the IAEA could use this projected virtual environment to train IAEA inspectors, and also to familiarize them with the environment that they are going to be inspecting.

There are many ways for this technology to be utilized. One is the aforementioned familiarization of the facilities that they will be inspecting. Using a virtual walkthrough of the site, they can know what to expect, and identify possible places where they should be sure to look at closely. If an accurate simulation has been created, then the inspector can load the map onto his laptop that he takes into the field, and can do a virtual walkthrough of the facility as he is doing a real walkthrough of the facility, and can take note of anything that has changed. Also, the virtual facility can be used to train future inspectors how to properly conduct inspections. Instead of flying inspectors out to training sites located elsewhere in the world, they can sit instead in front of a computer and learn via an interactive simulation. Another use would be to allow the inspector to link up with a knowledgeable expert who is located in another country or back at the IAEA, and help them go through the facility simultaneously, and identify any suspicious items.

One of the more valuable aspects of these virtual facilities is that real-world data can be fed into the virtual world. This would allow inspectors an even better look at where they are inspecting, provide a real-time way of analysing data, and also a way of communicating with headquarters instantly. The simulation can also be used as a virtual meeting place. Many people can join the same simulation from anywhere in the world and they can all share information and communicate easily.

6.14 Voice Transcription

This technology would facilitate data entry. The technology would need to be reliable and work in noisy environments.

6.15 Wearable (Low Power) Computer

The purpose of this technology is to provide mobile computing options and devices in the field that would improve timely data acquisition and analyses. Procedures, technical information, and data storage for portable devices could be consolidated to this system.

7.0 Conclusions and Recommendations

The workshop participants recommended several courses of action to assist the Agency in developing a technology strategy. The report authors grouped the recommendations according to the following categories: 1) Communications, 2) Data Processing, 3) Security, 4) Sensors and Surveillance and 5) Non-Technology Related Recommendations. Within each category, the recommendations are listed along with issues that the participants thought the Agency should investigate because they could impact the proposed technological solution or because they were particularly noteworthy in some way. The participants strongest recommendation is to establish an operations centre at Agency Headquarters. Although an operations centre is not a technology per se, it does provide a framework for implementing many of the technologies identified by the workshop participants. The concept of an operations centre is addressed in section 7.5

7.1 Communications

Communications improvement can be characterized as technology that provides inspectors with reliable, high speed data, secure data communication channels to enable the inspectors to exchange safeguards data between the field and Headquarters. The inspectors clearly desire the ability to communicate from within a facility, but they recognize that this is not only a technical problem, but also a political problem.

7.1.1 ***Communications Upgrade Recommendations***

- Upgrade Network Infrastructure to provide:
  - Indoor / Outdoor access while onsite on an inspection.
  - Security/authentication .
  - Redundancy.
  - High speed (2-way).
  - Portability.
  - Internet Protocol.
- Near-Term
  - Satellite / Current Cellular / Land line / WIFI
- Long Term
  - Software Radio / Land Line.

7.1.2 ***Communications Issues***

- RF limitations within Facilities.
  - Interference.
  - Safety.
  - Legal
- Limited bandwidth.
- Lack of direct landline.
- Lack of cellular/satellite coverage.
- Size.
- Limited resources will constrain new technology deployment/application.

7.2 Data Processing

Data are valuable, but can be overwhelming when presented in its raw form. Safeguards data exists in the form of sensor data, images, facility declarations, satellite images, among others. It is necessary to convert this raw data into a useable form to enable the user/inspector to interpret it. Some methods include the use of meta-data to enhance data queries. This allows the user to be provided only specific information. Other methods include using process models to filter the reported information to identify the reports which differ from the expected process. Data can be correlated spatially and temporally and presented as such. Through improved data processing, it is possible to reduce the inspector's information overload and thereby to allow them to make better assessments.

7.2.1 ***Data Processing Recommendations***

- Establish a common look and feel for interfaces to make access to all databases easy and user-friendly.
- Ensure the ISIS Re-engineering Project (IRP) is compatible with Agency's technology vision .
- Continue to invest in Intelligent search engines and searchable content.
- Deploy software to overlay geo-tagged information from multiple sensors / GIS.
- Acquire data visualization and data fusion software.
- Evaluate use of virtual reality for inspection preparation and training.
- Deploy automated data reduction and analysis tools.
- Evaluate statistical data-mining and other analysis tools for the identification of anomalies.

7.2.2 ***Data Processing Issues***

- Integrate databases and information (seamless sharing by end user)
- Security strategy
  - Role-based access control.
  - State may not allow certain site information or unattended/remote monitoring data to be transmitted off-site.
  - Balance between security of information and availability of information .
  - Certain data is restricted from being more-widely distributed and available (satellite imagery data.
- Limited resources will constrain new technology deployment/application.
  - Meta-data tagging.

- Limited resources will constrain acquisition of new technology.
- No significant internal research and development budget .
    - Research and development prototype laboratories are not available.
    - No model for relationship between IAEA and private sector partners
- Member State approval of new technology may be required for complementary access.
- Is the inspector the final analyst or merely one source of data collection for a larger state-level analysis?
- Operational Efficiencies
    - Inspector may want to review the on-site automatic analysis of URM and surveillance data even if it says nothing happened—double check.
    - Technology not always the solution
    - Technology should be adapted to reality (miniaturization, integration, etc.)

7.3 Sensors and Surveillance

7.3.1 ***Data Collection Recommendations***

- Deploy an integrated multi-functional secure data-collection device (e.g., wearable computer)
    - Ensure compatibility of existing equipment with new technologies
- Establish a central collection point at the facility where data from different sensors can be collected
- Deploy autonomous sensors
- Provide HQ access to on-site sensors.

7.4 Security

- Automate Authorization Access.

7.5 Operations Centre

The purpose of the operations centre is two-fold: to provide Agency staff a common operational picture (COP) of safeguards activities worldwide and to provide inspectors with a single point of access at Headquarters to Agency managers and subject matter experts who might be needed to support inspection or maintenance activities. The operations centre would provide Agency staff with command, control, communications, and intelligence sharing tools. Agency managers would use the operations centre to assess at a glace ongoing activities in the world of international safeguards. Inspectors could use the room to prepare for inspections, checking to see if equipment has been delivered or receiving the latest intelligence and safety briefings.

The operations centre would benefit inspectors by providing a single point of access at Headquarters for solving emergent problems, answering inspection-related questions, and for exchanging information with other staff members to facilitate timely, well-informed decisions in the field. Inspectors could contact the operations centre staff via telephone, satellite link, or the Internet. The operations centre staff, in turn, would be able to reach key Agency managers, technicians, and subject matter experts quickly via the telecommunications system, thereby providing inspectors access to others who might provide assistance. This would enable inspectors to resolve technical problems, make decisions, expedite clearances or authorizations, and solve emergent problems more quickly and efficiently than is possible today. Inspectors could work more confidently in the field knowing that they could access any type of expertise quickly. Since the communication channels would provide two-way communications, it would be possible for Agency Headquarters staff to contact inspectors in the field. This would provide Headquarters personnel a mechanism to transmit information that might be important for an inspector to have before he or she departs a site.

The configuration of the operations centre is dependent on the scope of the support that the Agency personnel require, the available budget, and space constraints at the Vienna International Centre. One possible configuration would be to equip the room with several flat panel displays, telecommunications equipment, large working tables, and computer workstations with access to the Agency's network. The centre would be staffed whenever there are Agency personnel working in the field. For the purposes of this discussion, it will be assumed to operate 24 hours per day, 7 days per week. In practice, this may not always be the case.

The flat panel displays would shows information of interest to Agency managers and staff. This information might include:

- Graphical presentations of the location of all Agency field personnel.
- Graphical presentations of the location of installed equipment or equipment in transit (position information provided via RF technology).
- State of Health information from unattended monitoring systems.
- Remote monitoring equipment data.
- Operational status of Member States facilities.
- Headline news of importance to the Agency.
- Intelligence briefings from SGIT.
- Planned inspection activities.
- Satellite imagery information.

The challenges facing the Department when establishing an operations centre would be:

1. MCM approval.
2. Financial support from Member States to procure equipment.
3. Specifying the collaboration tools that might be used.
4. Review decision-making process: how can it be made more effective and efficient given the new technology?
5. Implications of new technology on Agency culture/policies/procedures.
6. Operations centre staffing.
7. Need to create an international Subject Matter Expert network.

The operations centre could be implement in phases over several years. This would reduce the budget risk and would allow the Agency learn from their early implementation experience.

7.5.1 ***Recommendations:***

- Establish single access point and point of contact that inspectors can use to anytime from anywhere in the world to contact the Agency Headquarters staff.
- Establish near real-time identification and access to Information, SMEs, and analysts.
- Implement Collaboration Tools.
- Conduct near real-time analysis of information while inspector is on site.
- Provide and display common operating picture (COP).
- Decision-makers or delegates must be on-call, reachable, and empowered.

7.5.2 ***Operations Centre Issues***

- Security Strategy
  - State may not allow certain site information or safeguards data to be transmitted off-site.
  - Balance between security of information and availability of information.
  - Certain data is restricted from being more-widely distributed and available (satellite imagery data).
  - No link to Member States export control programs.

- Decision making
  - Inspector does not have the authority to decide to do a complementary inspection while on site.
  - Inspector needs more authority to make decisions in the field when he gets improved information channels to headquarters.
  - Decision-makers and experts must be on-call and reachable.
  - Support Network.
  - Organize and acquire resources to provide 24/7 capability.
  - Develop and maintain a list of subject-matter experts (use of SW to identify experts by information usage).
  - A single POC for inspectors is not consistent with current IAEA practices.

7.6 Non-Technology Issues that the Agency Should Evaluate

In the course of breakout sessions, the participants identified several issues that they considered important for the Agency to study, but which they deemed outside the scope of the workshop. These issues related to Agency policy or to issues outside the control of the organizations represented at the conference. The workshop participants believe that the Agency would benefit from studying these issues more thoroughly.

Personnel Issues:

1. The Agency should review their staffing levels and work distribution to ensure that the Department has sufficient numbers of people to perform the job of information analysis.
2. The Agency should continue to provide training for its personnel so that they have can maintain the knowledge and skill necessary to perform their jobs at the highest level.
3. If the Agency decides to implement an operations centre, the Agency should evaluate the need to operate the centre around the clock, seven days per week.
4. The Agency should investigate establishing a network of subject matter experts who could be available to answer questions of inspectors in the field.

Policy Issues:

1. The Agency should develop the capability to share information, via a computer network, among Agency workgroups. Presently, sharing information is constrained by diverse security approaches in Safeguards divisions
2. The Agency should evaluate the impact of empowering field personnel with greater connectivity. More information in the hands of the inspector in the field in near-real time makes it possible for the inspector to act on that information before he or she leaves a site. This could yield a better understanding of the activities ongoing at a

facility. It could also mean a cost saving because information can be gathered in fewer trips.

3. Board of Governors and Member State approval may be required before certain technologies could be implemented.

Management Issues:

1. The Agency should evaluate its decision making processes to determine if more decisions can be make by the inspector in the field.
2. The Agency should evaluate where data analysis will be performed: either in the field using software installed on the new hand held device or at Headquarters.

Appendix 1

Safeguards Tools of the Future Workshop Agenda

Agenda for "Safeguards Tools of the Future" Workshop

October 10-14, 2005

Monday: October 10th, 2005

8:00 – 9:00	Registration, coffee and refreshments	
9:00 – 9:15	Welcoming Remarks	S. Pepper
9:15 – 10:15	Keynote Speaker	Dr. Shirley Ann Jackson, Rensselaer Polytechnic Institute
10:15 – 11:15	Keynote Speaker	Dr. Vinton Cerf, Google
11:15 – 11:30	IAEA Overview and Workshop Goals	N. Khlebnikov, IAEA, Director Safeguards Technical Services
11:30 – 12:15	Lunch	
12:15 – 1:30	IAEA Presentations	M. Aparo, SGTS R. Gaetano, SGIT J. Barton, SGIT
1:30 – 2:00	Real Time Tracking & Surveillance	C. Pickett, Oak Ridge National Laboratory
2:00 – 2:30	Nanotechnologies: Devices for the Terabit Communications Network	D. Bishop, Bell Laboratories
2:30 – 3:00	Cyber Threats of the Future	M. Linder Carnegie Mellon University
3:00 – 3:30	Malicious Insider Threat	M. Maybury MITRE Corp.
3:30 – 4:00	Geo-Spatially Enabled Technology	V. Tao, GeoTango, and Q.S. Truong, Canadian Support Program
4:00 – 4:30	Position Orientation System, Land Survey	J. Gillett, Applanix
4:30 – 5:00	The Future of Data Communications	F. Baker, Cisco
5:00 – 5:05	Closing Remarks	
6:00 – 7:30	Harbour Cruise	

Tuesday: October 11th, 2005

8:30 – 9:00	Secure Remote Internet Access to Sensors and Seals	J. Coombs, Sandia National Laboratories
9:00 – 9:30	Smart Surveillance/People Vision	A. Hampapur, IBM Research
9:30 – 10:00	Geo-Collaboration Technology for MoMoSat	D. Schmidt Dialogis
10:00 – 10:30	Reachback Technology	G. Nakamoto MITRE Corp.
10:30 – 11:00	Mobile Information Systems for Safeguards Inspectors	V. Sequeira European Union-Joint Research Centre
11:00 – 11:30	Future Technology –Future Threats	K. Silva Verisign
11:30 – 12:00	Compact Systems for the Location and Identification of Radionuclides	T. Twomey, ORTEC
12:00 – 12:45	Lunch	
12:45 – 1:15	Brief Scenario #1	C. Carroll, Sonalysts, Inc.
1:15 – 5:15	Scenario #1	ALL
5:15	Finish for Day	

Wednesday: October 12th, 2005

8:30 – 9:30	Recap Scenario #1/Prepare Briefing	
9:30 – 10:00	Wearable Computer Applications	A. Smailagic Carnegie Mellon University
10:00 – 10:30	Context Aware Computing	D. Siewiorek Carnegie Mellon University
10:30 – 11:00	Statistical Data Mining	A. Dubrawski and A. Moore Carnegie Mellon University
11:00 – 12:00	Brief Results of Scenario #1	Group Representatives
12:00 – 1:00	Lunch	
1:00 – 1:30	Brief Scenario #2	C. Carroll
1:30 – 5:30	Scenario #2	ALL
5:30	Finish for Day	

Thursday: October 13th, 2005

8:40 – 9:40	Recap Scenario #2 /Prepare Brief	
9:40 – 10:40	Brief Scenario #2	
10:40 – 11:00	Coffee	
11:00 – 12:00	Consolidate Findings	
12:00 – 1:00	Lunch	
1:00 – 1:30	XRF Use for Controlled Materials Identification and Seal Authentication	T. Blackburn Pacific Northwest National Laboratory
1:30 – 2:00	Virtual Reality for Facility Training	K. Michel Los Alamos National Laboratory
2:00 – 2:30	HazMat Cam	K. Young Idaho National Laboratory
2:30 – 3:00	Pervasive Computing and Wireless Networks	B. Yener Rensselaer Polytechnic Institute
3:00 – 3:30	Reachback Technologies	K. Masica Lawrence Livermore National Laboratory
3:30 – 4:30	Time for General Discussion	ALL
4:30	Finish for Day	

Friday: October 14th, 2005

9:00 – 10:00	Week Summary	Participants Representatives
10:00 – 10:15	Questions and Answers	ALL
10:15 – 10:30	Coffee	
10:30 – 11:30	Agency Response	Dr. N. Khlebnikov
11:30 – 12:00	Closing Remarks	S. Pepper
1200	Finish	