EXECUTIVE SUMMARY

The Workshop, Standardization and Integration of Unattended and Remote Monitoring Systems, held at Brookhaven National Laboratory on October 15-17, 2002, brought together representatives of the International Atomic Energy Agency (IAEA), International Safeguards Project Office (ISPO), and Member State Support Programs (MSSP) and their contractors to resolve long-term issues about the efficacy of the IAEA's safeguards and surveillance systems. Khlebnikov hoped that new ideas would emerge on the choice, improvement, and miniaturization of equipment, life-cycle studies, and use of off-the-shelf products that could lower the costs of project management, training, procurement, and the need for large inventories, and also help developers of equipment.

In opening, Aparo remarked that this workshop follows the 1998 and1999 meetings on unattended monitoring systems aimed at standardizing equipment; he reviewed the ensuing draft document on requirements, and the essential guidelines that the IAEA developed covering general requirements, and those for hardware, software, and data. A more detailed review was needed, especially of potential replacements for the now unsupported Windows NT4.0 operating system, and of such modifications of unattended equipment that would significantly extend the interval between inspectors' visits. Schanfein asked for page-by-page comments on the guidelines. Lively discussions centered first on efficient access to, and stable operation of, the equipment, on its power consumption and supply, retention of operation during power failures, and accelerated aging and life cycle studies of components versus systems. Later, the speakers and participants explored the configuration of collect computers and their storage capacity, data generators (sensors), data filtering and compression, and trusted time clocks. Throughout the debate, the IAEA focused on the need to simplify the tasks of inspectors and technicians at the sites, while precluding unauthorized access to data. Under the heading of Networking, three speakers discussed auxiliary communication devices: the advantages of the Ethernet (O'Gara); its application in a reactor facility and its security features compared with those of a serial interface (Caskey); and data communication standards (Capel). During the following day, Martelle concluded this topic with presentations on future directions in, and tests of, storage media. Wednesday focused on the IAEA's requirements for Authentication and Encryption and the guidelines for implementation (Tolk), followed by Neumann's introduction to cryptographic principles and demonstration of real-life equipment (electronic optical sealing system). Next, Capel, O'Gara, and M. Stein expressed their views of the merits of various public- and secret-key systems and their management. Again, the audience offered several alternatives, some of which were robustly contested. In the afternoon, Schanfein and Jansen described several candidate server operating systems to replace Windows NT 4.0. Khlebnikov encouraged developers to explore "intelligent" sensors, consider those used in other monitoring applications, and consider creative technological solutions to current and emerging safeguards needs.

Schanfein and Parker led Thursday's sessions on the IAEA's standardization of components and development of flexible multi-instrument software for collecting and reviewing data. The need to consult with, and write drivers for, developers was emphasized. Gonçalves detailed the installation and operation of a new unattended monitoring system for the characterization and verification of fresh fuel assemblies. Aparo moved on to consider the complexities of competition versus sole supplier in procurements for the IAEA, whilst Kadner's presentation highlighted the problems faced by suppliers.

The final review of the workshop's results, led by Aparo, emerged as a very interactive and enthusiastic conversation involving all participants. The following conclusions were reached:

1. Networking. Ethernet, with the TCP/IP protocol, is considered the best way to communicate and connect the data generators and the collect computer. The Agency will continue to implement this system, but will still support ILON for special cases and during a transition period until Ethernet connectivity and ILON functionality (e.g., triggering and time synchronization) are fully supported in current safeguards instruments.
2. Operating Systems (OS). The Agency is considering migrating from Windows NT to embedded Windows XP for the short term. They will closely examine the possibility of other topologies not based on a central data collect computer with a mainstream OS. Candidates for such an approach could be based on "zero administration servers" (SUN) with a simple user interface and removable media, for the long term.
3. Encryption and Authentication. A top priority is to define a single standard for cipher schemes that is applicable to small battery driven instruments as well as to large mainframes (review stations).
4. State of Health. This is a growing concern as the Agency expands the implementation of remote monitoring systems. A standardized approach in data format, message content and review must be vigorously pursued now to prepare for the future.
5. Integrated Review Software. The Agency hoped the vendor would define the interface by the end of 2002, though this may not occur. Methods to assure the quality of imported data should be explored.
6. Monitoring. It is likely that Virtual Private Networks (VPN) would be adopted.
7. Procurement. Critical components have been procured to protect the IAEA against their unavailability.

Workshop on Standardization and Integration of Unattended and Remote Monitoring Systems

Workshop Summary

Susan Pepper, Head, ISPO, welcomed participants to Brookhaven National Laboratory (BNL), and Ralph James, Associate Laboratory Director for Energy, Environment and National Security, expressed his hopes that the meeting would generate the essential building blocks to resolve safeguards for surveillance systems, and promised BNL's cooperation in providing new technical ideas. Then Nikolai Khlebnikov, Director, Division of Safeguards Technical Services, IAEA, briefly discussed the Agency's efforts to establish standard requirements and protocols for current and new support equipment, such that they would greatly facilitate project management, including improving components, miniaturizing systems, and adapting commercial products, while simultaneously reducing the life cycle costs. He pointed to the Agency's ongoing achievements in replacing analog cameras with digital ones, and looked to participants for new ideas for the future.

Background

As background, Max Aparo offered his Review of the Results of the Workshop on Integration of Safeguards Equipment, a report of a meeting that took place in Niagara Falls, Ontario, in 1999. The intent of that workshop and a previous one held in 1998 in Albuquerque was to resolve issues of standardizing equipment and reducing inventories, while lowering the costs of procurement, development, and training. The first workshop revised standards so that they conformed to industrial ones; the second meeting offered recommendations for unattended and remote monitoring (RM) and data security. The objective of the present workshop was to review and agree upon those guidelines. The major needs include replacing the now-unsupported Windows NT 4.0, using Ethernet and TCP/IP to interconnect instruments versus ILON and RS465; deciding whether each data generator should have a data buffer; and, selecting removable storage devices so that inspectors can readily retrieve data from the collect computer, or from data generators should the computer fail. The Agency wants better guidelines for data security, key management, and types of algorithms (symmetric or asymmetric) while limiting vulnerabilities. They also want to extend the interval between inspectors' visits to sites, which necessitates higher standards of operation and reliability of equipment.

Mark Schanfein opened a discussion of the IAEA's draft Essential Guidelines and User Requirements for Safeguards Unattended and Remote Monitoring System, a multi-authored comprehensive document containing generic guidelines. He reviewed the requirements individually, garnering comments on each one, and on particular terminology and phrases, such as the definition of "minimum" power requirements (#3.5). For example, the Agency does not specify to vendors the minimum power consumption of instruments, in order not to limit possible design approaches. However, the IAEA normally specifies the time the instrument is required to survive without mains power. Similarly, specifications are required on the radiation sensitivity of equipment. The vendors suggested that some of the requirements were ambiguous due to

terminology; in many cases the word "should" was replaced by "shall." Another example of apparent ambiguity in phrasing was the words “where practical” in guideline #3.7 requiring all equipment to use an adjusting power supply. Cameras, all DC powered, can have such an adjusting supply, but this is inapplicable where supplies are AC.

Some requirements received little comment, but for others, there was a lengthy discussion, as for the general requirement, #4.1, that systems should undergo accelerated testing equivalent to ten years. Mike Farnitano confirmed that the vendors would test them under defined conditions. Several participants speculated that ten years might be too long as manufacturers often supported equipment for only five to seven years. Todd Main questioned its applicability to systems versus components; Schanfein replied that the Agency addresses components, or the critical components of a system. Aparo, Robert Parker, and Michael Ralph revisited and generally agreed with the guidelines (#4.4 & #4.5) for a PC-based operating system (OS), communicating via the Ethernet using the TCP/IP protocol with a 100-day storage capacity (#4.6). Susan Caskey suggested that the data generator should store data in such a way that it cannot be edited; Jim Jansen opined that an architectural description of the collector system might be valuable. The IAEA staff, Parker, Peter Button, and Guy Martelle compared the merits of a trusted time source against one that drifted, particularly when parts of a system become inoperative for a long time (#4.8).

Hardware requirements (#5.1-12) were thoroughly considered; Guenther Neumann suggested employing electronic means, rather than visual inspections, to detect welds. Orderly shutdown of the collect computer and data generators (#5.7) is essential in power failures, so batteries should last at least three hours under reduced operation. The question arose as to when systems should shut down: at a facility-power failure, or near the end of the batteries’ life? The IAEA requires that shutdown occur immediately after the former. Caskey believes that security concerns should be part of the guidelines for a removable storage device; later, Martelle suggested that removable media should display a green and red light, indicating that it was safe, or not, for the inspector to remove the disk. Caskey also noted that the security of Ethernet TCP/IP connectivity is less than that of FTP encryption. Other suggestions for the guidelines on hardware and software were that a watchdog should be installed; Neumann pointed out the difficulties, especially for software, but said it could be done. The watchdog, rather than individual software, should reboot the computer after a shutdown (#5.13).

The discussion moved to guidelines on data requirements and those for state-of-health (SOH). New requirements are needed for the authentication and encryption of trigger signals because the trigger’s threshold could be altered maliciously. In Aparo’s and Parker’s opinions, the trigger should not be differentiated from other messages; however, data might be transmitted randomly so that the trigger cannot be distinguished. More research is required here. A discussion of third-party vulnerability analyses under Information Security Requirements (#9) started a debate about ways to prevent anyone from knowing the operational state of a device, and about sharing data with member states when the state requires protection against unauthorized access. Certified algorithms seem to be the answer, except for special cases. The problem was raised of verifying the

integrity and security of data on a hard disk, along with the potential for other security breaches when the Agency ships data generators, seals, cameras and the like to member states – where they may wait for months before coming under the Agency's control. Few suggestions were made on the guidelines for engineering drawings, design specifications, the component list, and documentation, other than they should be more specific (#11). Similarly, more specificity was needed on procedures for installations, operations, and procurement, and training manuals. The many ideas discussed in this session were elaborated over the following days.

Networking

Aparo introduced Networking with a simple schematic of the system architecture in which Ethernet with the TCP/IP protocol connects the surveillance systems and the radiation-data collect computer. So far, the IAEA's Ethernet requirement is not established at any data generators in the field. Present connections are based on serial line or ILON networks. Aparo outlined the IAEA's explorations of several data generators having Ethernet with the TCP/IP protocol capability, and the search for an external device to convert legacy connections and protocols to Ethernet with TCP/IP protocol. Issues include whether Ethernet with the TCP/IP protocol is the correct choice, considering its cool reception from developers, and what features of TCP/IP should be implemented.

Ed O'Gara discussed his findings on Specification for the Auxiliary Communication Device (ACD), including those for power, ports, memory, and size, made from a market survey of off-the-shelf systems and components. The ACD is intended to provide a standard converter to allow all IAEA data collectors to communicate via Ethernet while maintaining ILON functionality. The rationale directing his library and Internet survey was the IAEA's search for a device to retrofit data generators, so they could communicate via Ethernet. O'Gara did not consider custom designs because of their high costs and limited flexibility. No commercially available ACD device had both low power consumption and a small footprint, but he demonstrated how commercial off-the-shelf (COTS) components could be "snapped together" into a suitable device without requiring additional circuit design. Possible solutions were based on the PC 104 alone or with standards. Those based on VME, cPCI, and STD were too large and consumed too much power. He ranked CPU boards (by their specified wattage). Those with the best processor, the ZF x 86 Failsafe, used by the military over wide ranges of temperatures, are no longer supported by the manufacturer. However, a consortium was formed to continue the ZF x 86 line. O'Gara also rated power supply boards, and digital input/output (DIO) boards. His surveys encompassed only hardware, but software could be added for encryption.

Caskey described the Application of Wireless Ethernet Inside a Reactor Facility, reflecting the Agency's considerations on using radio communications in power plants, rather than facing the high costs of installing cables. She described the three-layered, radio-based 802.11 box that is widely employed internationally and similar to Ethernet. The Media Access Control Protocol, in layer 2, carries Collision Avoidance and can use Request to Send/Clear to prevent collisions with other transmissions. Its spread spectrum

allows frequency hopping and direct sequence, though the data throughput is not very high; it can be readily and cheaply upgraded for international frequencies. Caskey detailed the applicability, security, and performance of the IR-based 802.11 in offices, using a diffuse light beam between buildings, direct point-to point, and its one-mile range with a laser beam. Transmissions through different types of wall are being explored. A possible drawback to radio communication is that the frequencies might affect the operation of other plant equipment, such as cranes. She went on to describe the pros and cons of cellular-, satellite-, and serial-wireless communications, and considered the increasingly popular Personal Area Network (PAN) to provide wireless connections between devices within a room or house. Although most wireless options allow some encryption module, the algorithms are untrustworthy; incorporating Virtual Private Networks (VPN), with a media access control (MAC) address will ensure the connection is as secure as a hardwired one. Caskey suggested that using wireless made sense for several applications within a nuclear facility. Participants stated that earlier reluctance to do so was based largely upon its potential to interfere with other vital equipment, and the requirements for safety certification.

Tony Capel spoke on Data Communication Standards for Safeguards Information, for use within the monitored facility, pointing out that he had examined standards for external networking in a previous paper, which recommended the use of IP-based wide area networking and IPSec. He discussed the interconnections required for a facility with nuclear measuring devices, cameras, seals, sensor/switches linked to the data store, communications, and power management system ("data collect computer"). He described the evolution of interconnection standards in five major industries, showing how today serial interface standards dominate, having overtaken parallel interface standards both in speed and cost effectiveness (except in very limited applications). He identified the major serial interface standards and indicated that Ethernet was the most popular. He then discussed the use of the Ethernet as a general-purpose interface standard (i.e. in local interconnection applications) to connect computers to instruments. He pointed out that originally the Ethernet standard defined a non-deterministic protocol where timely access to communicate was not guaranteed, and thus it was considered unsuitable for many industrial applications. This drawback can be avoided by using "switches" rather than "hubs" and by using point-to-point full duplex (FDX) connections. Capel discussed the normal 100-meter distance limit of Ethernet, and how it can be extended to many kilometers by using fiber optic, asymmetric and symmetric digital subscriber lines, wireless and other means. He also discussed the use of shared infrastructures and new "structured wiring systems" (and standards), along with Virtual Local Area Network (VLAN) and Secure Virtual Private Network (SVPN) technology. He emphasized that "real time" operation of Ethernet interconnections requires the use of deterministic "switches" (not "hubs"). Aparo appreciated the real-time connection that the system afforded, its low costs, and the ability to recover errors over the Ethernet.

In a related paper, Caskey discussed Network Security: Ethernet versus Serial Interface. She described the hardware and software components of an Ethernet local area network, its six-sectional frame (preamble, destination and source addresses, type, data, and frame check), and the functions of each. All frames are broadcast to all systems on the network,

and they all start to read the frames but stop if the destination address is not theirs. While it is not an efficient system, it is cheap, and includes a collision detect protocol; after a collision, a system must wait a random period before re-transmitting. She described its signaling component, the physical medium of cables and hubs and switches, and the high-level protocols. Serial networking has both a physical cabling layer and the networking protocol. Caskey considered six types of serial communication, the layers they would reside in, and whether they were synchronous or asynchronous. She compared the mode of operation, total number of drivers/receivers, and the maximum length of cable and data for RS 232, 422, and 485.

Caskey turned to the dependence of security on proper installation, configuration, and management, wherein lies the bulk of security risks. Backdoors are unprotected access points into the network; sniffing and spoofing are specific problems. Both Ethernet-based and serial-based communications are open to both. A hub-based Ethernet network cannot easily detect sniffing nor the presence of a new system, though both problems are radically reduced in a switched network with a smart switch. Sniffing also is problematic with serial communication using RS 485 and 422, but not for RS 232, which allows only two systems on the network. While the latter, therefore, is the easiest to secure, it is limited in its bandwidth and operating distance. Spoofing the Ethernet can only be done at the IP layer by a knowledgeable hacker, although a user can spoof another's IP address, causing loss of service between computer and misdirection of packages. Spoofing serial communication can only occur at the network layer because there is no unique identifier; however, a network run on the serial bus is susceptible.

Ed O'Gara concluded the session with Converting from ILON to Ethernet. ILON, standing for Intelligent Local Node, is a LonWorks transceiver, a control networking standard that was developed as a fair instrument bus with many topology options. By contrast, Ethernet, the world's most popular local area network, was not specifically designed for instruments. It was designed for light industries, although it often is used in heavy industrial environments. He listed the wide variety of options offered by both ILON and Ethernet for particular needs, including various data rates and transmission media. He then illustrated the topologies of both (excluding wireless). Ethernet is referred to as a contention-based technology because multiple stations contend for the same transmission window; messages might collide without collision-detect protocols based on the binary exponential back-off algorithm that is inherently unfair. Thus, stations experiencing few collisions generally do not have to wait as long to transmit as those with several failed attempts; however, switches can rectify this unfairness. ILON similarly is a contention-based technology, but its collision probability is much lower than Ethernet's. Further, priority slots can be assigned. The systems have other common traits; both are cheap, use CSMA (Carrier Sense Multiple Access), allow one repeater in a domain, and require a router to covert from one medium to another. The differences are that Ethernet has shorter segments, it lacks free topology, it does not have a priority-setting mechanism, and it requires at least one additional hardware component. On the positive side, it is non-proprietary, its switches prevent collisions, and it can accommodate VLANS to add an additional layer of security. Furthermore, Ethernet-based devices can be built from COTS components, are not limited to 48-bit

authentication, and they can encompass removable storage features, and mass storage, while ILONs require custom DIOs. O'Gara thought that the IAEA might well consider converting from ILON to Ethernet because of these advantages, coupled with its wide availability. However, adding switches will be a top priority.

Data Security

In the next session on data security, Keith Tolk surveyed the problems of authentication and encryption, algorithms, and key lengths and certification in his presentation IAEA Authentication and Encryption Requirements and Guidance, and of public versus secret keys file formats and data structure. The IAEA requirements state that data from unattended equipment must be cryptographically authenticated before transmission outside a Sealed Tamper Indicating Enclosure (STIE); moving between Agency computers, the data's integrity can be protected by certified VPN technology. This technology also satisfies encryption requirements to prevent disclosure of information to a third party. Tolk discussed the allowable National Instititute of Standards and Technology (NIST) - certified authentication algorithms, either Hash (SHA-1, or higher), or instead, digital signatures; the preferred one among the latter is Elliptic Curve DSA that can be run on a minimal processor. The choices for encryption are AES or 3DES with an RSA envelope, and RSA only for very short messages. Within a facility, low-power devices may use AES and 3DES when they cannot use RSA.

Other specified protocols Tolk described were key agreement, public key distribution, and a way to verify the integrity of firmware by comparing the firmware in a field device with that of a trusted processor. He outlined the IAEA's plans to follow NIST's guidelines for key sizes that will be fully applicable in 2015; particularly, the present minimum size of 80 bits will be replaced by one of 120 bits. The IAEA requirement that security-systems should pass a third-party vulnerability assessment (VA) is not yet fully enforced. Certified commercial equipment may be used without a VA provided that it is employed exactly as specified.

Under guidelines for implementation, Tolk spoke of the value of flexibility in supporting several algorithms so that the Agency can both rectify hacked systems and react to new products and future developments in cryptography. The IAEA prefers public keys to secret ones. The former allow verification at any location without exposing private signing keys; they need not be protected from disclosure, only substitution. Secret keys require that any computer verifying authenticity must have access to the signing key, i.e., they must be a security critical device and pass a VA. His discussion of implementation goals emphasized the Agency's desire to standardize their approach to data security – for example, with a single utility for verifying authentication signature, a single utility for decrypting files, and standard file formats, all of which would necessarily incorporate specific structural elements. He reiterated the Agency's preference for commercial equipment whenever possible.

Guenther Neumann followed with an introduction to cryptographic principles and demonstrations on the Electronic Optical Sealing System (EOSS), and the Color Video

Server (CVS) that encompass Aquila's prototypal CVS connected to a converter to the Ethernet. The EOSS system, based upon firing a light pulse into a fiber-optic cable, includes authorization, authentication, and encryption. The system is hard to tamper with, and the information is unreadable for those lacking the correct key. An illustration showed how the sender's plain text successively is encrypted and then decrypted for the receiver under a cipher-blocking chaining process. Authentication relies on HASH function-based MAC. Neumann showed the challenge response protocol for authorization that is restricted to dedicated individuals. He compared secret key cryptosystems and public/private key cryptosystems. Regardless of the cryptosystem being used, he proposed adopting a Key Manager. A sample Key Manager, which was used by the EOSS and the CVS having different cryptosystems, was demonstrated. Such an arrangement simplifies the interface at the inspectors' computers.

Tony Capel presented his analysis of the IAEA's requirements for security in RM and identified candidate standards based on the use of asymmetric cryptography in Data Security Standards for Safeguards Information. His first slide showed a straightforward view of the physical and operational RM environment. He then summarized basic key management for public key (asymmetric) cryptography, wherein an asymmetric key generator is used to generate private and public keys with the private key kept secret and the public key inserted into a certificate. He indicated that most certificates today follow the X509 Version 3 format and a Certificate Authority, part of a Public Key Infrastructure (PKI), would create and sign the certificate. Certificate Authority and PKI software is available from Entrust, and Microsoft bundles this software in their Windows Server products. Capel summarized IAEA requirements for authentication and confidentiality protection. Authentication requirements are primarily Agency driven and needed over the complete data lifecycle, while confidentiality requirements are primarily member state driven, needed "hop-by-hop" and depend on the data's physical location. He noted that the corresponding security mechanisms also differ significantly, with authentication being technically and operationally simpler to implement (but potentially requiring higher assurance levels). He suggested that authentication be implemented above the Application Layer (of the ISO model) and that confidentiality protection should be implemented on a "hop-by-hop" basis, for example using file encryption or IPSec. He then identified the Cryptographic Message Syntax (CMS, RFC3369) standard, a subset of which is widely supported in Windows, as a candidate standard to provide authentication protection. He also suggested RFC3126 for long-term protection. His final slide provided an authentication example using CMS. In his example, the private (secret) key is created, securely stored (subject to zeroization) and erased at the end of its life, within the source instrument. The debate afterwards centered on whether the higher electrical power requirements of asymmetric cryptography algorithms compared with symmetrical ones would preclude its use in field applications requiring low power, e.g. EOSS. Keith Tolk suggested that elliptical curve asymmetric algorithms might have sufficiently low power requirements, but more investigation is needed.

Ed O'Gara began his presentation on Elliptic Curve Cryptography (ECC) by summarizing public-key cryptography systems, including the well-used DSS, RSA, ECC, and the newest ones, NTRU and Braid Group. Public-key systems, introduced in 1976 by

Diffie and Hellman, use a public encryption key (for confidentiality) and a private decryption key (for authentication), the latter being very secure and hard for a third part to determine. The key maker keeps the private key, while the public key is given to those with whom the key maker will communicate. Digital signatures use a private key to encrypt part of a message, such as the checksum at the end.

O'Gara pointed to the advantages of RSA; it is a widely accepted standard algorithm that is robust and has withstood the test of time. Its disadvantages are that encryption and decryption are slow and computationally intensive, and large keys are required. It is considered secure with 1024 bit RSA key, and 168 bit symmetric key. ECC, a public key/digital signature system, is being used increasingly in mobile phones, Smartcards, and Personal Digital Assistants, and the Agency might well find it valuable for digital signatures of images and for digital envelopes. It is a sturdy standards-based system, widely favored in these limited environments, and can be used for encryption and authentication. As yet, it is not as well tested as RSA, its encrypted message is twice the size of the originating one, and security is based on chosen underlying fields for which no standards exist. NTRU, based on polynomial rings, was only patented in 2000 and still is under review by the Institute of Electrical and Electronics Engineers. It has a small probability of failure, and appears to be an order-of-magnitude faster than ECC although its keys are correspondingly bigger. The newer braid group system, based on infinite non-communicative groups arising from geometric braids, holds promise, but there has been little research on breaking the braids. O'Gara believes that for the same security, ECC is much more efficient than RSA, and speculated whether the computational savings could justify the IAEA's moving from RSA to ECC. Alternatively, they could wait until the two new systems are widely assessed before choosing a new public-key system.

The following paper, Key Management, presented by Marius Stein opined that the most difficult problem in key management is the fact that users break most security systems. Competent ciphers are not easily broken, but keys are compromised by weaknesses in procedures, protocols, and management. Attacking the latter facet can be the most rewarding because it is easy to do, and everything is revealed. Common ways to obtain information from people is to use undue influence, or to earn, and break, their trust. Stein looked at threat models, and weighed the value of recovering a key against generating a new one. He believes that key management often fails because it is treated as an add-on, rather than being embedded in the secure system. He detailed six minimal requirements for key management, and questioned the reliability of citizens of the "host country" who are IAEA employees. In other words, is the fox guarding the chicken coop?

Removable Storage Media

Aparo began the afternoon session on storage media with a précis of Removable Data Storage Media for unattended and remote monitoring stations. So far, the Agency has used Jaz and MO-disks at collect computers, and flash cards at data generators. The unavailability of Jaz drives and new requirements for larger capacity (from three months to a year) are driving the search for new reliable low-unit-cost media that meet the inspectors' needs.

Martelle continued with two presentations, Future Directions of Storage Media, and Testing of Different Removable Media. Assuming that versions of Windows operating systems would be used, he considered three options, in each case with different drives or cards: Windows NT 4.0 OS - three drives, and two PC cards; Win2000 - one drive and two cards: and, WinXP - one drive and two cards. For each scenario, he spelled out the system's specifications, computer issues, and usability issues (focusing on the inspectors' tasks). He then described his tests of the functionality and survivability of the 40GB IBM Travelstar in a USB enclosure under extreme versions of the conditions expected when hand-carried by inspectors from a site to IAEA headquarters. Travelstar passed all criteria without a problem or loss of data except once, during a "hot swap" with Win2000. This problem did not occur with WinXP. Nevertheless, this problem is not drastic because only a copy is lost, and the original information remains on the hard drive at the site. Routines could be established to ensure that the data are completely and properly transferred. Martelle now is testing a "Hawk" digital video recorder, a small temporary device that will run for three months on two AA batteries and support two cameras.

Server Operating System

Schanfein next discussed the Agency's Search for an Operating System for UMS Data Collect Computer, motivated by Microsoft's withdrawal of support for NT. From a comprehensive survey of inspectors, he verified the pressing need to lessen their burden from error messages in Windows OS, and from their difficulties with removable storage media, exacerbated by operational constraints at the field sites. ORNL is making a formal evaluation to select a robust cost-effective model that will support networked systems, system redundancies, the UPS interface, the DCC operating system, and SOH. The Agency's preferences are the following: 1) embed the OS and boot up to UMS software; 2) have well-defined access levels between inspector and technicians; 3) allow access to the OS and setup levels only for SGTS; 4) include FLASH disk bootable system; and, 5) ensure remote system management. The new system should tolerate abrupt shutdowns caused by power disruptions. Data collect computers should support hot swappable devices, Ethernet local networks, and have capabilities for large redundant storage, remote dial-up, and time synchronization.

The final presentation in the session, Jim Jansen's Evaluation & Recommendation of Operating Systems – E.131.01, reported the findings of an ORNL evaluation of candidate OSs for the IAEA. Cooperating with the Agency's staff, ten focal requirements for an overall architecture were defined, reviewed, and revised. Then, in a seven-step process, proposals from eighteen venders were solicited by letter, rated, and ranked. Ten of them were examined further. Four proposals were "essentially compliant": Venturcom Windows Embedded XP with RTX5; LynuxWorks BlueCat Linux; LynuxWorks LynxOS 4; and, Red Hat Linux 7.2. They ranged from highly embedded, very small kernel ones to full-featured systems with large kernels and many additional layers. All had TCP/IP protocol stacks and could add drivers; all had real-time and near-real-time features for multiple tasking. Jansen discussed the lessons-learned through this process, suggesting that revisiting the requirements and weighting them will dictate the Agency's selection of an OS. He also suggested that the Agency compare the advantages of storing data on the collect computer (CC), or on the CC on removable RAID disks (since

removal methods limit the choice of OSs). He questioned the value of real-time requirements that reduce options further. The ORNL review's best choices were Microsoft's Embedded XP OS and Red Hat Linux's OS. They will elaborate a field-simulation package to test them.

A variety of questions followed, from the costs of the new OSs versus reconfiguring present ones; some participants spoke strongly for the economic advantages of going with flexible mainstream COTS, despite their short lifetime, over custom-made systems. The suggestion was explored of using industrial collect-and-store systems that are not computer-based – though this might be difficult for inspectors. The quality of digital pictures from the cameras was raised, and whether they should record scene change only. Participants agreed upon the value of the IAEA's systematic approach to evaluating and testing new technologies.

Standardization

Schanfein opened the sessions on standardization and data transmission by describing the IAEA Standard Components List, a formal catalog essential to the Agency because their limited resources determines the inventory of spares they hold, and restricts the types. Eight categories are available to developers, the first being IAEA-configured standard cabinets with tamper-indicating features, now supplied locally by Schmidberger, also the contractor for the standard power distribution panel. Schanfein gave specifications for the others: power distribution, power supplies, and uninterruptible power supplies, batteries, computers, watchdog, and detector cables. On September 30, ORNL began a two-phase program to first develop equipment-specific performance requirements, and then to establish test regimes and process emulators with test loads based on the maximum capacity of each component. ORNL initially will determine the functional and environmental parameters for the equipment (UPS, batteries, power supply, and charger), before sending the revised document to the Agency. Test regimes will be based on UPS requirements, IAEA qualification protocols, and a broad spectrum of international standards. The IAEA proposes to minimize the support required for implementing equipment by having standardized systems with basic building blocks, by using COTS components, and by having a realistic spares inventory. Long-term training support will be a recurring need. Aparo confirmed that the Agency's procurement section has been notified of these standards and is notified of updates to them. However, if developers offer an innovative non-standard solution to a problem it will be carefully considered, though the Agency must focus first on short-term resolutions.

Parker next considered standardization of software, commonly used for three to four years, so that it conforms to any new data-generator system. His reports, Modular Multi-instrument Collect Software, and Modular Integrated Review Software focused on research at Los Alamos National Laboratory that was based upon restructuring of the software of the Integrated Review Software (IRS). The unattended and remote monitoring (UNARM) system is assembled monolithically, and accordingly, it is difficult for vendors to develop software to integrate new types of instruments into it. Therefore, the objective was to enable vendors to support such multi-instrument collect (MIC) systems. He stressed the importance of being fully knowledgeable about the functions,

configuration, and interactions of MIC components: the MIC main dialog, the communication support objects, and instrument support objects. Under a three-phase plan, using MICGM conversion methodology (1) the architectural requirements and framework for partitioning MIC were defined, (2) the interface design is being specified and finalized, and prototypic samples of software code provided to developers, and, (3) the acceptance test document and MIC user's manual will be updated. Initial development of MICGM is underway. The following discussion affirmed that the information would be available for developers, but the IAEA will specify the standardized component list – opening it for reviews by others would seriously delay the process. Similarly, writing drivers for developers or having them do so would hinder progress.

Parker described his work on breaking up the cumbersome text files of the IRS, and grouping them into manageable interfaces. He compared the five large independent pieces of the current system with the ultimate IRS software that will be developed over three stages. Notably, the latter incorporates radiation review (with time-align capability), a review manager with a generic facility configuration manager, and a well-defined interface module. It also has plug and play capabilities and consistent graphic configuration. Hence, it should afford a fast response to customers needs, and fully support new technology and software principles. Specifications for several components are complete, and design of others has started.

Under Unattended Measurement Station João Gonçalves described a system developed for Euratom Safeguards aiming at the full verification of the output of LEU fuel-fabrication plants, full validation of the operator's declaration on fuel elements, compatibility between safeguards verification and operator's management, and a reduction in safeguards costs while maintaining high standards. Plant operations should be little disturbed. Further, some of the requirements are: 100 days' unattended operation, automated association of nuclear material accountancy measurements with the identification of each fuel element, and data evaluation by the system with later validation by the inspector. He detailed the principles of operation, including the NDA measurements and the automated 3D identification system, and then described infield testing in Italy and Sweden, and the permanent installation of a UMS at FBFC, France, and its clone at the Joint Research Centre. In the second part, he described how the plant operator would operate the UMS. Gonçalves discussed the UMS architecture, very much in line with the workshop discussions, and covered many technical aspects, including OSs, communications, access control, start-up, power failure, security, and performance checks. The use of laser barriers to detect intrusions as well as protect Safeguards computers was mentioned. He dealt at length with system integration, a difficult problem that might be mitigated by using standard components and transforming the sensors into easily replaceable modules with well-defined interfaces (equivalent to the "smart sensor" concept). He favorably compared unattended safeguards against conventional ones, particularly in that the former unites the two separate worlds of the plant operator and the Agency; indeed, the design of the UMS is agreed upon with the plant's operator. Gonçalves stressed that the UMS is not a general-purpose instrument but must be customized for each installation. Responding to questions, Gonçalves believes that

software can be incorporated to generate third-party reports and for quality assurance. To validate data, and the state-of-health of the system, he also thinks that adding modules is feasible because of the UMS's design. He also highlighted the simplicity of operations. At the end of the fresh fuel assembly line, each fuel element is transported into the UMS, before being stored in the plant's storage area. The plant operator checks that the fuel element is well positioned inside the UMS and, starts the system. The UMS measures the fuel element for 30 minutes. The operator can then remove it. The data are securely stored so that only inspectors can access it. He stated that a remote data transmission system would be useful, considering that an inspector may wish to re-check a specific fuel element, and this may not be compatible with a 100-day inspection interval. Indeed, at this time, the element in question may have been already shipped and inside a reactor. Negotiations with plant operators for establishing the remote transmission of Safeguards data are in progress.

Aparo next considered Equipment Procurement Issues: Competition versus Sole Source Supply. Development and procurement are constrained by economics, politics, and technology. Thus, the market for instruments is small, probably only a hundred units per year. Politically, extrabudgetary funds may influence the choice of developer or vendor, while technological restrictions revolve around the uniqueness of safeguards equipment. Goods are procured through a Basic Supplier Agreement (BSA) negotiated directly. The BSA reduces delay within the Agency, while ensuring a fixed price for several years. Hence, sole-source procurement is the choice for authorized equipment. However, Aparo holds that competition between suppliers, and the selection of one of them, maintains the variety of suppliers and so must be part of the developmental process. Competition ensures cost-effectiveness, and the exploration of different technical solutions.

COTS equipment meets many of the IAEA's requirements, e.g., for multi-channel analyzers, so they can test and select the best for their purposes and then require changes in hardware and software. Thus, developmental and procurement costs are lowered, and the reliability and performance record of the equipment is known. Alternatively, the Agency can cost-effectively examine different perspectives by initiating parallel development by member states. The disadvantages are the high development costs to member states, their reluctance to invest monies without an assured outcome, and the prolonged period of development and testing. These drawbacks can be limited in several ways: by requesting proposals/prototypes from contractors and indicating the number of units required; limiting development time, and then arranging collaborations; or, specifying the general design and leaving the details to the developers. Other options are for the IAEA to develop an in-house development capability, to issue a manufacturing drawing, or to issue an open tender for manufacturing developed equipment. A central crucial issue is that now, because of third-party development, the Agency does not have intellectual property rights, and hence, cannot use cheaper alternate suppliers.

Steve Kadner spoke for vendors in his Equipment Procurement Issues: Supplier Point of View. He gave details of Aquila's worldwide operations, their support to the IAEA and their unique buyer-seller relationship in the safeguards business, and the highly specialized niche market relying heavily on MSSPs. The current short lifetime of

safeguards equipment entrains long and costly redesign due to the obsolescence of parts, the rushed placement of systems in the field, and the lack of communication and needs identification. He stressed the advantages of having a longtime approach and lifecycle support from one vendor familiar with the Agency's policies and procedures, and a reputation for swiftly executing their orders. Aquila has proposed a cost/benefit study to the U.S. Support Program of different long-term solutions to support a 15-year lifecycle.

Data Transmission

The last session concentrated on Data Transmission, beginning with IAEA Remote Monitoring. Aparo stated that 57 digital surveillance systems with RM capability are presently installed. Forty of these systems transmit their data through a remote link. He listed the communication media in each country. The susceptibility of the camera modules to single event upsets was rectified with a firmware revision, the incompatibility of COTS components for SDIS was solved by reconfiguring and simplifying the system, and so the reliability of RM has improved since the beginning of 2002. Some problems remain, including lack of ISDN compatibility between some countries, and the unreliability of the PSTN lines in others. A major development in RM is scene change detection that can reduce by 90% the amount of non-safeguards significant data, and hence, the costs of its communication and storage. VPNs offer solutions to security concerns. He outlined security improvements for sharing data with State Systems of Accounting and Control that may necessitate data filtering before information is copied or transmitted to the State's authority. Verification of the authenticity of the VACOSS seal data formerly relied on the inspector downloading the data directly from each seal during visits. Now, the DCM14 camera remotely interrogates the VACOSS at remote monitoring (RM) stations, and the seal data are embedded in the images. An upgraded version of GARS verifies the authenticity of the seal data.

Schanfein addressed the next challenge, State of Health Data. The Agency's objectives are to verify, from files in Vienna or field offices, that the systems are operational, to respond rapidly to failures, to support preventive/predictive maintenance, and to review some critical indicators daily and others weekly. Presently, there is no standard approach to filter the large volume of SOH data to a level that allows handling without technical expertise for data assessment and dedicated resources for daily reviews (a problem that will increase as remote monitoring is used in more installations). As a result each developer reports SOH information in their own way and this makes it difficult for the IAEA to assess the various messages. Schanfein considered the text and graphic output from one facility with eighteen DCM14 Cameras, seven SDIS units, and four GRAND3s and showed examples of the complex log files. His slides illustrated the enormity of the task and detailed the Agency's need for an automated review program, ideally one that could be run overnight. He discussed the role of the developers and the IAEA in evolving a future SOH platform, emphasizing again the Agency's pressing need for it. Participants suggested that the Agency might glean ideas from a comparable situation, namely the remote monitoring of the SOH of radiation detectors in nuclear power plants.

In the final presentation of the session, Heidi Smartt described Virtual Private Networks in which connectivity is established on a shared public infrastructure, e.g., the Internet,

with the same policies and performance as a private network. VPNs add security to a network by encryption and authentication, yet they are flexible (multiple sites can be connected to a center) and very cost-effective – they can pay for themselves within a year. Security is added at the network layer by IPSec protocols and key management, or Internet Key Exchange (IKE). Alternatively, security associations can be added manually by entering, and keeping track of, multiple large prime numbers. Smartt discussed the issues of configuration, export control, and placement of the VPN in front of a firewall, behind it, or in parallel with it. She prefers a VPN/firewall combination in which the VPN handles only encrypted traffic and the firewall handles the rest. Other aspects discussed included hardware configuration, common criteria certified products, and FIPS 140 certification. Finally, Smartt gave details of SNL's attempts to install a VPN between the laboratory and JNC, Japan, the subsequent troubleshooting, and eventual success.