ISPO-423

Proceedings from the

WORKSHOP ON INTERNATIONAL DATA COMMUNICATIONS

Sponsored by the U.S. Support Program to IAEA Safeguards
Held on behalf of the International Atomic Energy Agency

October 18-20, 1999

UNITED STATES MEMBER STATE SUPPORT PROGRAM TO IAEA SAFEGUARDS

DEPARTMENT OF ENERGY
DEPARTMENT OF STATE
NUCLEAR REGULATORY COMMISSION
DEPARTMENT OF DEFENSE

Prepared By

Avril D. Woodhead
Brookhaven National Laboratory
Upton, New York 11973

January 18, 2000

Proceedings From the

WORKSHOP ON INTERNATIONAL DATA COMMUNICATIONS

October 18 – 20, 1999

Sponsored by the U.S. Support Program to IAEA Safeguards

Held on behalf of the International Atomic Energy Agency

Host: Michael Farnitano, International Safeguards Project Office/USSP and Brookhaven National Laboratory

Facilitator: Massimo Aparo, Head, IAEA Section for Equipment Development and Support

Table of Contents

1.0 ORIGINAL AGENDA

Monday 18 Oct.	09:00 - 09:30	Introduction	Opening of the Workshop and participant introductions	Host – **Michael Farnitano**
	09:30 - 10:00	IAEA Communication Requirements for Remote Monitoring	Overview of the IAEA remote monitoring development and implementation efforts	IAEA – **Max Aparo**
	10:00 - 11:00	"	Overview of IAEA Technical Requirements and Challenges to Global Communications, Risk Scenarios for Networks.	IAEA – **Jim Regula**
	11:00 - 11:30	UN Satellite Network	UN satellite network To include: technology overview, components, configuration, protocols, data throughputs, applications, limitations, availability, reliability establishment and operation costs, experience, etc.	Rep. of the UN satellite network system **(New York Representative)**
	11:30 - 12:00	Discussion	Q/A participants and IAEA	Chaired by Host
	Lunch			
	14:00 - 14:30	Available Technologies All presentations in this session to cover: Technology overview, components, configuration capabilities for national and international networks, protocols, data throughputs, applications, limitations, availability, reliability establishment and operation costs	PSTN/ISDN	PSTN technology provider / vendor ATT and Aquila Technologies
	14:30 – 15:00	"	Frame Relay	ISDN technology provider ATT and Aquila Technologies
	15:00 - 15:30	"	Advanced (next generation) cellular telephone for data transmission	FINSP Tapani Honkamaa (STUK)
	15:30 - 16:00	"	Secure Internet	LANL Len Burcyk
	16:30 - 17:00	"	INMARSAT	INMARSAT technology provider COMSAT Craig Poyner
	17:00 - 17:30	"	VSAT	VSAT technology provider Hughes Aerospace
	18:30 – 20:30	Reception	Social Event	Home of Michael and Doreen Farnitano

Tuesday 19 Oct.	09:00 - 09:30	Security	Applicable risk scenarios for IAEA safeguards equipment	IAEA – **Julian Whichello**
	09:30 - 10:00	"	Applicable information security technologies	SNL - Keith Tolk
	10:00 - 10:30	"	Export Controls on Strong Encryption	**US Commerce Dept. – Kathleen Kenyen**
	10:30 - 12:00	Service Providers All presentations in this session to cover: available technologies, required components, configuration capabilities for national and international networks, protocols, data throughputs, applications, limitations, availability, reliability establishment and operation costs, contracts, maintenance	Applicable services offered	**HOT to Start** **ATT** **Aquila Technologies** **MCI WorldCom**
	Lunch			
	14:00 - 14:30	Service Provider Experience	Regional infrastructure difficulties	**SAIC, Service Providers**
	14:30 - 17:30	Forum on Service Providers and IAEA	Communications requirements (present and future) and support needed by the IAEA for remote monitoring	Forum chaired by IAEA
		"	Logistical challenges applicable to specific technologies	Forum chaired by IAEA
		"	Service provider cooperation	Forum chaired by the IAEA
Wednesday 20 Oct.	09:00 – 10:00	Management Issues	Management of Communication Infastructure Migration into the future	**Canadian Safeguards Support Program – Tony Capel (Comgate)**
	10:00 - 11:00	Future Technologies	Migration path to new and future technologies and ensuring that currently adopted system are capability of providing compatibility with future technologies.	Forum chaired by IAEA
	11:00 - 12:00	Concluding Statements		All / IAEA / Host
	Lunch			
	14:00 - 17:00	Review the outcome of the workshop	Prepare draft note consolidating the options with recommendations	IAEA, USSP, CSSP, Host, Others?

2.0 LIST OF ATTENDEES

Participant	Affiliation	Phone Number	Email Address
Michael Farnitano	USSP/ISPO	516-344-8085	Farnitano@bnl.gov
A.D. Woodhead	BNL	516-344-3482	Adw@bnl.gov
Susan Pepper	ISPO/BNL	516-344-5979	Pepper@bnl.gov
Tapani Honkamaa	STUK	358-9-759881	Tapani.honkamaa@stuk.fi
Heidi Smartt	SNL	505-844-3798	Hasmart@sandia.gov
Michael Goebel	HOT/HNS	44-1908-319-101	M_goebel@hnsltd.hns.com
Nick Leake	HOT/HNS	44-1908-319-101	N_leake@hnsltd.hns.com
Jim Regula	IAEA	43-1-2600-22262	J.Regula@IAEA.org
Les Epel	USSP/BNL	516-344-2920	Epel@bnl.gov
Duncan Gardiner	IAEA	43-1-2600-21989	D.Gardiner@iaea.org
Lester Martin	AT&T	732-420-4289	LRMartin@att.com
Shameel Talcott	Aquila	505-828-9100	Talcott@aquilagroup.com
Kaluba Chitumbo	IAEA	43-1-2600-22200	K.Chitumbo@iaea.org
Guy Martelle	IAEA	43-1-2600-21909	G.Martelle@iaea.org
Steve Kadner	Aquila	1-505-828-9100	Kadner@aquilagroup.com
Ed Hogan-Bassey	DISTCOM	1-703-924-1840	Hoganeb@bellatlantic.net
Joe Hennegan	DISTCOM	1-703-924-1840	USMAR13@bigplanet.com
Len Burczyk	Los Alamos	505-665-4273	Lburczyk@lanl.gov
Craig Poyner	COMSAT Mobile	301-214-3219	Craig@poyner@comsat.com
Steve Azevedo	LLNL/DOE	925-422-8538	Az3@llnl.gov
Kathleen Kenyon	DOC/BXA	202-482-5546	Kkenyon@bxa.doc.gov
Paul Lewis	AECB	613-995-2585	Lewis.p@atomcon.gc.ca
Trevor Fischbach	MCI Worldcom	201-804-6789	Trevor.fischbach@wcom.com
Tom Mantone	MCI Worldcom	732-603-6312	Thomas.A.Mantone@wcom.com
Todd Main	DOD Nuclear Treaty Programs	703-588-1983	Mainjt@acq.osd.mil
Bill O'Connor	DOE NN-44	202-586-4867	William.o'connor@hq.doe.gov
James Busse	DOE NN-44	202-586-1700	James.Busse@hq.doe.gov
John McCoy	PNNL	509-372-6156	John.mccoy@pnl.gov
Ajita Ratnatunga	IAEA	43-1-2600-26275	A.Ratnatunga@iaea.org
Huri Fraley	SNL	505-844-0161	Hfraley@sandia.gov
Keith Tolk	SNL	505-845-9014	Kmtolk@sandia.gov
Gene Bosler	LANL	505-6655-9111	Gbosler@lanl.gov
Don Marcopulos	Constellation Technology	727-547-0600	Dmarco@contech.com

Participant	Affiliation	Phone Number	Email Address
Peter Chiaro, Jr.	ORNL	423-576-4598	Chiaropjjr@ornl.gov
Fernend Sorel	Europ.Com.JRC Ispra	39-0332-789411	Fernand.sorel@jrc.it
Julian Whichello	IAEA/SGTS	43-1-2600-21867	j.whichello@iaea.org
Massimo Aparo	IAEA/SGTS	43-1-2600-21844	m.aparo@iaea.org
Andrew Werth	Hughes	301-428-5768	Awerth@hns.com
David Jupin	Hughes	301-601-7225	Djupin@hns.com
Tony Capel	Comgate/AECB	613-235-4778	Capel@comgate.com
Yakshey Malla	United Nations	212-963-2270	Malla@un.org
Ron Smith	CSE	613-991-7203	Rjsmith@its.cse.DND.CA
Bernie Wishard	NRC	301-415-6852	BEW@nrc.gov
W.E. Farrell	SAIC	858-826-2645	Farrell@gso.saic.com
Peter Taylor	AHT Concert	914-923-1763	Pete.Taylor@CONCERT.COM
Reinhard Messner	AECB	613-995-3096	Messner.r@atomcon.gc.ca
Nikolai Khlebnikov	IAEA	43 1 2600 21840	N.Khlebnikov@iaea.org
Joseph Carelli	BNL-ISPO-Vienna	43 1 31339 743547	Carelli@bnl.gov
Lisa Owens	SSTS	202-647-9730	OwensLi@acda.gov
Mark Sitko	MCI	Not available	Not available
David Bot	BOT Engineering	716-842-1033 Ext. 101	Davidbot@Cgocable.net

3.0 INTRODUCTION

The intent of this Workshop, sponsored by the U.S. Program of Technical Assistance to IAEA Safeguards (POTAS), was to bring together representatives of the International Atomic Agency's (IAEA's) Department of Safeguards with communications experts from industry to discuss the Agency's requirements for remote monitoring. The Department of Safeguards is charged with assuring the international community that the signatories of the Non-Proliferation Treaty and other agreements are complying with the commitments designed to safeguard nuclear material used for peaceful purposes. Presently, the Agency is exploring methods to upgrade their communications with remote monitoring sites, and is looking to the member states for help. The U.S. Support Program considered that this exchange of information, experiences, and opinions would greatly assist the Agency in meeting their present and future challenges in establishing and maintaining effective global data communication ability. The Workshop made significant strides toward achieving this goal.

The meeting ran for two-and-a-half days of intense discussion. On the first two days, IAEA staff began by explaining the Agency's particular requirements, which was followed by presentations from several leading-edge communications vendors who described their systems' capabilities and explained how they could meet the Agency's special demands. The Workshop concluded with a forum led by the Facilitator during which the participants gave their opinions on the advantages and drawbacks of the various solutions offered. A wrap-up session conducted by the host organization consolidated these views, and, in some cases, offered practical aids.

The speakers kindly sent copies of the overheads of their presentations. To read them, go to http://www.ispo.bnl.gov. Electronic or paper copies can also be obtained by contacting Michael Farnitano at the International Safeguards Project Office, Brookhaven National Laboratory, 12 S. Upton Road, Building 475B, Upton, New York, 11973-5000, Tel: 631-344-8085, Fax: 631-344-5344 or at Email Farnitano@bnl.gov.

4.0 MEETING PRESENTATIONS

4.1 Overview of the IAEA's remote monitoring development and implementation efforts: Massimo Aparo (Head, IAEA Section for equipment development and support)

Massimo Aparo opened the meeting by describing the Policy for Remote Monitoring for Safeguarding Nuclear Facilities (RM). The Agency began this work in 1996, and completed it in December 1998. This policy defined the framework on which to establish remote monitoring. It defined the types of safeguards; the needs for security, authenticity, and confidentiality of data; the types of inspections to be made (announced and unannounced); the ways to share data; and, the requirements for operating and accounting data. Procedures were set up for each facility, first for light-water reactors (LWRs), and then for nuclear-storage facilities. Mr. Aparo described the initial field tests designed to demonstrate the capability of RM and the associated equipment at the Mixed-Oxide (MOX) fuel storage in Switzerland. Tests at seven sites are completed (United States of America, Switzerland, Republic of South Africa, Japan, Republic of Korea, Sweden, and Finland). Phase 1 development was finalized at a

storage site in Germany, and three sites are under development (in Canada, Argentina, and Japan). The systems installed are for both surveillance and radiation monitoring. IAEA retains the old system of monitoring for six months after installing the new one.

The IAEA has planned 31 new sites for Server Digital Image Surveillance (SDIS) in 14 countries for 1999–2000. The member states will be involved in the development work, and IAEA's technical departments will assess the reliability of the systems. Much effort in remote monitoring focuses on demonstrating the cost-effectiveness of the selected systems, and whether they can be implemented with IAEA-authorized instruments or commercial equipment. Field and laboratory tests ensure that the equipment meets its performance criteria, and encompasses issues of safety, security, and environmental problems. Mr. Aparo delineated some characteristics of the RM systems that are essential for the Agency. They must be connected to a PC/server running with a Microsoft Windows NT operating system; the remote equipment must be standardized, which is essential in lowering the heavy costs of training maintenance technicians; and, the instruments must have a large storage capacity with fixed hard drives, in case communication with Vienna is lost. Furthermore, data should be authenticated at the source, and encrypted in the server so it remains confidential.

Mr. Aparo described the RM equipment being tested. The SDIS system has a flexible communications interface, and connections for up to three digital cameras on each of two serial ports. The camera can store 30,000 images, and contains batteries in case power is lost. The system is secure and access is controlled; data are encrypted in the camera and the server. The Digital Multi-Camera Optical Surveillance (DMSO) system is based on similar principles but has up to 32 cameras, each with an isolated communication line. Furthermore, the distance from the camera to the console can be up to 1,200 meters, depending on its cable. The digital camera, the system's basic building block, digitizes the data, encrypts it, and compresses it. Both systems allow the data to be retrieved on-site. He next detailed the features of the digital cameras and also those of the seals (the updated Variable Coding Seal System, VACOSS). He mentioned a new technology that detects scene changes. Data are stored on a 500-megabyte flash card, up to 3,000 images, or about three-month's information. The next step in its development will be to increase both the number of images and the times they are taken using a larger card. A small battery ensures that the system will operate for three days without a main supply. An inspector can set the intervals between taking the pictures, and the camera can be connected to other devices telling it when to operate. Mr. Aparo also briefly discussed how the General Advanced Review Station (GARS) Software in Vienna reviews incoming secure data, and showed the configuration of the System Building in the Department of Safeguards, and the data-flow scheme.

The Department of Safeguards prepared a RM implementation plan after reviewing the RM field results. Assuming that member states agree and their facilities are readied, up to 35 sites per year will be established at an annual cost of $1.5 million. Equipment was procured for those expected to be set up in 1999. However, installation work has been limited by the lack of skilled technicians. The estimated yearly cost of supporting a SDIS in a BWR is $16,000 (1camera, 2 seals), and for a PWR, it is $22,000 (2 cameras, 5 seals); these values include the capital cost, depreciation, and recurrent costs over 5 years. The volume of data generated for an SDIS with 3 cameras is about 17Mbytes/day. Aparo noted that using scene-change detection

might reduce by up to 90% the number of redundant scenes and those of no significance to safeguards, realizing a large savings in the expense of transmission and storage. IAEA is constructing a large Remote Monitoring Test Facility in Vienna to receive equipment, send it out, and test it, and to train technicians and inspectors.

Mr. Aparo concluded that remote monitoring can greatly strengthen safeguards, particularly because inspectors may no longer have to go to a site (thereby also lowering their exposure to radiation), and also because RM can serve as an effective complementary measure for unannounced and random inspections. However, he stressed that the Agency is striving to lower its communications costs and they need help in defining a cost-effective network and exploring unattended radiation monitoring RM systems. Additional technical help is needed in installing them.

4.2 Overview of IAEA's technical requirements and challenges to global communications: Jim Regula (IAEA)

Jim Regula began with several graphics depicting the entire operation of collecting, encrypting, and sending data from remote stations to a hub station, then transmitting the information to the IAEA Safeguards Office, Vienna for the inspectors' review, analysis, and eventual archiving. Member states can dial in to the hub station to retrieve their share of the data; alternatively, they can dial the main server in Vienna that then will dial-out the information to them, although he warned that the latter mode of access might raise a security problem in future. Today, there are nine facilities with servers in seven countries, on four continents, transferring 115 megabytes daily via three types of data links. The sites are in various environments and have from 1 to 12 cameras, so the volume of material sent to Vienna depends upon how frequently pictures are taken. Data are not sent in real time; rather they are sent out at once each day, hence the entire sequence of transmission from a remote site via the hub may take up to 24 hours to reach Vienna. Mr. Regula expects the volume of data to double or triple in the next few years, raising urgent problems about how to control it and keep it secure.

Mr. Regula next described the pros and cons of the three current data connections: Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN), and Frame Relay. PSTN, used in Barsebaeck, and SWE Regional Office Data Access Nodes (DANs) is simple to install, readily available, but is slow, noisy, and subject to retries. ISDN, used at sites in Goesgen and Muhleberg, Switzerland, and from Koeberg to Pelindaba, RSA, is much faster (400-5000 bytes/sec) but its drawbacks are that local PTTs can loose or change the configurations. Further, its availability is limited. Frame relay, employed at regional offices in Tokyo and Toronto, and in Pelindaba, RSA, has proved a reliable permanent connection that serves small offices very well. Consequently, RM can piggyback on existing services. The disadvantages of frame relay lie in the expense of international services, and also the SGIT must provide hardware encryption. Mr. Regula illustrated his points by showing several maps of current RM links. The speaker next discussed several communications tools, especially the RMS Explorer. Its values are that it specifies the state of health of each camera, and counts all the incoming images, raising a flag if some are missing. Further, it allows inspectors to access specific files at specific sites via their Microsoft connection. This system has demonstrated its

worth at the nine sites, but Mr. Regula cautioned in predicting its performance at large numbers of sites planned. He then briefly discussed the modes of communicating data to member states, and highlighted the particular needs for securing data in a Low Enrichment Uranium Facility, as are now under consideration for the PFPF in Japan.

The speaker summed up his points with a look at the challenges facing the Agency in selecting a reliable, secure, and economical mode of remote communication. He recommended testing a Virtual Private Network (VPN) wherein data would be encrypted with every connection authenticated at each server and the data then sent via the Internet and through a firewall to the SG-Ring in Vienna; this method would appear to be a safe, cost-effective way. For remote sites lacking a communications infrastructure, a useful evaluation might be of transmitting data via satellite, on demand. He proposed optimization of RM by using TCP/IP and multicast connections that could increase the capacity for data collection by 20%, although security might be compromised. He appositely closed by drawing attention to the 25 proposed new sites for 2000 (with 121 cameras), the associated risk scenarios, and suggestions to mitigate them.

4.3 Requirements for remote monitoring in Iraq: Guy Martelle (IAEA)

The third representative for the Agency, Guy Martelle spoke about the unexampled needs of remote monitoring in Iraq. In the harsh environment of that developing country, the telephone lines still are of poor quality, the electrical power supply is undependable, and there may be tampering with, and damage to, the equipment installed at the power plants. There are limited capabilities for communication via a satellite as the subtended angle is low, although this means was used previously to transmit data.

Many of the nuclear sites in Iraq are around Baghdad, frequently within 20 – 30 kilometers of the city center; some plants are involved in manufacturing weapons, and producing uranium. Other key facilities are near the border with Syria. Before 1998, the IAEA had six remote monitoring sites in primary production facilities. However, the data were collected every three minutes, and so the volume of information to be sent to Vienna was enormous, the equivalent of that from, perhaps, 60 facilities. Furthermore, the information had to be scrutinized closely each day to ensure that nuclear material had not been diverted. Many of Iraq's nuclear facilities were crippled during the war with Iraq. UNSCOM had been monitoring more than 20 other plants, collecting more data than did the Agency; some 5 to 10 of these sites may still be standing (mostly within 20 km of the city).

There is a 100-meter tower for telephone communication near Baghdad's center that was not destroyed in the war. However, its antenna is not fully functional.

Mr. Martelle described the considerations that have to be taken into account, and some solutions, for setting up RM stations in Iraq: viz. the need to use heavy encryption, low-profile equipment, and to be as unobtrusive as possible.

4.4 United Nations Satellite Network: Yacksey Malla (United Nations)

Having had an outline of the Agency's requirements for remote communication, the meeting then learnt of the successes of the active satellite communication system used by the United Nations. As Yacksey Malla explained, the hub of the U.N. global satellite network is centered in New York, and communications from there to Geneva and to the many offices (between 135 – 140) around much of the world rely upon time-leases on five commercial satellites. Presently, the United Nations has no stations and few operations in the pacific region; the Indian Ocean satellite covers about 20% of that area. In the rest of the world, the U.N establishes facilities with satellite dishes to receive satellite bands, and maintains them at an annual cost of $5 million. At outposts where such communications are restricted, telephones and fax machines are employed (set up by Hughes Corporation). The U.N. relies wholly on commercial systems and does not develop any themselves. He discussed two systems in particular that had proved valuable; the CISCO 3810 Voice Data/Video network that is used extensively worldwide, and the CISCO 3810/1GX network currently in place in Kosovo. He described the complex ring of communicators in the U.N. Building itself that reaches out to regional offices throughout the world.

The United Nations Division of Communications encounters problems similar to those confronted by the Agency. Thus, communications often must be set up in places where the Internet connections are sketchy, and where there is no local expertise and help. Most of their ground stations consist of a large trailer and a large satellite dish. The U.N. relies upon about 400 experts from New York and their other established missions, who then go out to these remote sites to set up satellite dishes. The costs of communicating by satellite are reasonable, and the U.N. has excess capacity available. Mr. Malla explained that the World Bank contracts out their installation work in politically stable areas, for example, to MCI (the United Nations does not use MCI). However, the World Bank wanted to set up a lot of facilities in a short time, so they leased severs from the U.N. at cost. The IAEA also might consider using this excess capacity. He mentioned that the present trend in the United Nations was to move to digital connections.

The speaker pointed out that although the need for security exists for the United Nations, and they encrypt data in bulk, much of their information is non-sensitive. Hence, their security requirements are not as critical as are those of the Agency, so that they can more freely use commercial products.

5.0 GENERAL DISCUSSION:

Mr. Aparo opened the general discussion at the end of the morning's presentations. He reiterated the Agency's requirements; one dial-in session per day with the remote sites from a regional hub to transfer data, the volume of which would depend upon the number of cameras at the site, and then transmission of the information at a non-peak period to Vienna. IAEA's plans to upgrade the system were explained. Sensors would download the information into a main "sensor box" which would encrypt it. The regional hub office would call this box daily at times when the cost of communication is lowest and download the data. If contact cannot be established on any particular night, then the data from two nights would be taken at once.

Accessing the station each day is not a requirement in most cases: information for up to three months can be stored at the remote site, and this volume can be retrieved by one call, if necessary.

The IAEA would use frame-relay transfer during the day for e-mail traffic, and during off-peak periods for moving the data from the regional hub to Vienna. This use of "downtime" periods reduces costs. Indeed, in some countries, the costs of moving data from the remote stations to the regional station are greater than the expenses of transfer from the hub to Vienna, such that the former transfer may only take place once a week. In other countries, such as Canada, the regional offices are quite near the central one, and local phone calls are free. The use of RF (radio frequency) communications was brought up, but the idea was somewhat negated by the difficulty in stalling the system and obtaining the required radio frequencies (although it was agreed to be a good way to verify seals). Satellite dishes might be used – but then they would have to be installed inside buildings so that they were not stolen. Mr. Aparo pointed out that, with all these caveats in mind, the Agency tries to "patch together" the least expensive methods of communication for a particular RM, though not to the detriment of efficiency and security. Usually, a large regional server can store the information collected over 15 to 18 months, even though it still is regularly transmitted to Vienna (an excellent backup system). However, he noted that, in essence, the regional hub is just a gateway, and under the right conditions, it could be bypassed and the data sent directly from the station to Vienna.

Ideas were exchanged about the problems in maintaining the remote stations. The IAEA's technical staff is not trained in maintenance and is otherwise fully engaged, so that, generally, the Agency must rely upon consultants and factory support. The IAEA also has the responsibility to set up connections for the commercial systems that they use in the regional offices, and to reconfigure and establish backups for them. While the vendors usually carry out this service locally, they do not do so for international connections. Mr. Aparo foresees that the Agency will have too few staff in coming years to cope with any glitches that occur. The discussion turned to the scope of future remote systems. Again, the scope was circumscribed by costs. As discussed earlier, the tasks are very site-specific, and, in particular, the costs of transferring the data might limit remote monitoring. Eventually, the IAEA might have to choose between having fewer stations with excellent systems, or having more stations with equipment that is less than optimal. Consequently, Mr. Aparo reiterated the importance of having remote stations that, among other benefits, relieved IAEA from having to send inspectors into the field every two or three months. But to do this, ways must be found to secure the extra technical support that the IAEA requires.

6.0 MEETING PRESENTATIONS

6.1 Networking solutions for the 21st century: Lester Martin (AT&T)

After the morning's overview of the Agency's requirements for remote monitoring, the afternoon session focused upon the services offered by various technology companies.

Lester Martin, representing AT&T, opened the session by discussing their new high-speed packages, and how they could readily move the rapidly expanding volume of the

Agency's data through the system. He briefly touched upon those business drivers apposite to the IAEA, such as the need for global expansion, the exploding bandwidth requirements, and technical support and management of new applications. AT&T's challenges also include maintaining network secrecy, and increasing the network's global reach. He spent some time describing voice services and their evolution: voice networks, such as 4ESS and 5ESS, might well be used to transmit data overnight after hanging up the telephone. He recommended the asynchronous transfer mode (ATM), a high-speed transfer network, which combines several services while maintaining a permanent connection (he noted, however, that the voice-over package is hard, exhibiting echoes, jitters, and latency defects).

Mr. Martin explained AT&T's progress in leveraging existing technologies to create virtual private networks that combine the reliability, security, and predictability of private networks with the flexibility, openness, and ubiquity of public lines. AT&T's key word here was "any": any speed (56 kbps to 155Mbps): anywhere; any service interconnection; anytime; any system to any system. He noted that over a thousand connections with Vienna could be established on such a network, but with more, then switched virtual circuits would be required that would make timely connections and then drop them. The system's architecture would also incorporate alternate paths to ensure its reliability.

He next discussed the distinctive features of AT&T's frame relays, suggesting that the IAEA might use these permanent circuits but share ports of access and egress. Sharing is valuable when there is congestion from the volume of traffic because much more power is available. The ATM-based platform behind the network also reduces delays in transmission. Frame relay is configured to rapidly recover from disasters – if the hub site is compromised, then there is backup capability at another site, and traffic is diverted to it. The company offers network management services, and takes responsibility for ensuring that the packets reach their destination.

Mr. Martin described the advantages to the Agency of using the faster IP enabled frame relay system wherein the locations are not tied together, but rather, the data go from one location to another omitting the nodes. Switching is based upon routers at the edges of the network. He then summarized the service classifications, attributes, and essential features of ATMs, and the various access options offered. Finally, he touched upon the bandwidth budget which combines voice compression (4:1), statistical mixing, and silence suppression to provide dynamic bandwidth allocation and doubles the capacity for transmitting data.

6.2 The potential of 3G mobile telecommunication technology in remote monitoring: Tapani Honkamaa (STUK- Radiation & Nuclear Safety Authority, Finland)

Tapani Honkamaa started by outlining the history of mobile telephones up to their present state (2nd generation, with a bandwidth of 9.6 to 14.4 kb/s) at which they show promise for providing services applicable to remote monitoring in nuclear safeguards. With the expectation of the third generation of systems in 2002, they offer an effective, reliable, secure, and economical way to pass data from the sensors to headquarters. The new systems will have a bandwidth of 2MB/s, enough to transmit a video signal, and will include full Internet services, the "last mile link" to the data network. The latter attribute is especially important because the

costs of local collection and sending data via these cellular phones is low, but prices escalate when international borders are crossed; transmitting over the Internet lowers this cost. Furthermore, because the system uses commercial components they will always be available, at a low price, with reliable connections, and built-in security (conversations cannot now be picked up by scanners).

There are drawbacks to them, the most important being that it is unclear whether eventually there will be enough bandwidth for all users since radio frequencies are a limited natural resource. Also, cellular phones cannot be used inside reactors, and will require repeaters linked to the outside.

Mr. Honkamaa pointed out that despite these disadvantages, cellular phones provide new possibilities for the Agency's remote monitoring program. They might be satisfactory for real-time video or surveillance cameras, for real-time alarms from seals and limit switches, and in monitoring and tracking transportation (their new positioning data can pinpoint locations to within a few meters). He cautioned the Agency to evaluate new technologies carefully, and suggested that, since their requirements are very strict and might hinder the use of new systems, the requirements themselves should also be evaluated.

6.3 Hughes Network Systems: David Jupin (Hughes Aerospace)

Hughes Network Systems is the largest provider of VSAT (very small aperture terminal) technologies in the world, and, in his presentation, Mr. Jupin listed the ways in which this mode of communication might serve the IAEA. VSAT is a well-established technology (over 200,000 HNS VSATs deployed worldwide) in which a small dish or antenna outside a building receives satellite signals and passes them to a box inside the building that acts as a multiplexer. Transmission is via geosynchronous satellites (i.e., satellites high above the equator), so that a tracking antenna is not needed. It is a ubiquitous and adaptable system, with uniform services and sophisticated networking capabilities regardless of the location, and it has a multifaceted architecture. Multi-Mbps data services for video, voice, e-mail and so forth can be provided, even in remote areas. VSATs already have a strong international presence. A strong feature for the IAEA's applications is that the system can bypass local communication services. This is especially important in countries where the telecommunications infrastructure is not reliable.

The system utilizes a time division multiplex (TDM) transmission from a central hub whereby all remote stations listen to the transmission via the satellite but decode only the data addressed to their specific site. Such limited access is assured because the system encapsulates the data sent to a particular station within its own packet; accordingly, the system knows where the data are going, and, should a packet be lost, it transmits the data again. The return links to the hub are shared in a time division multiple access (TDMA) mode. Here each earth station transmits short "bursts" of data, that are interleaved in time with the other stations. For each outbound link (data rates of 128 or 512 Kbps) up to 32 inbound links can be supported (data rates of 64, 128 and 256 Kbps). The system utilizes three access methods to efficiently handle different types of data. These include "aloha", "transaction reservation" and "stream". Traffic from a station can also be prioritized on a session by session basis; for example, voice could

take priority over other less time sensitive data. The access methods and prioritization allow the remote stations to be very flexibly configured to meet the customer's specifications.

Much attention is given to data security, and especially to the vulnerability of TCP/IP transmissions. Each remote station must be "commissioned" by the hub before it receives a download of its executable software thus ensuring that only authorized stations have access within the network. Among other measures, HNS utilizes it own proprietary transmission protocol within the system. Proprietary compression and spoofing algorithms can also be enabled on a session by session basis, which increases the data security. Finally, either the purchaser or HNS can encrypt the information. Hughes offers a software-based cryptic algorithm, and automatic key generation. Each transmission session can be uniquely encrypted and inbound and outbound sessions are separately enabled. However, encrypted data cannot be compressed.

For extra reliability, the system supports terrestrial backup via automatic dial backup. Dial up connections, ISDN or frame relay can be used as the alternate path. If a satellite connection should fail, the remote terminal can automatically establish a terrestrial link to the hub and information is redirected over this link.

Hughes Network Systems is capable of providing a worldwide service tailored to meet IAEA's needs including designing the network, performing the program management, installing and maintaining the equipment, providing the space segment, and taking care of all the required permits and specific regulations of a particular country. Mr. Jupin mentioned the company's recent success in contracting with the Comprehensive Test Ban Treaty Organization (CTBTO) to implement a worldwide communication network for monitoring and verification. The turnkey contract to implement and provide the worldwide service is valued at approximately $70M over a five-year period.

The audience questioned the costs of setting up sites. Mr. Jupin replied that the typically the company first asks the customer about specific requirements, surveys representative sites, runs pilot tests to establish the volume and types of traffic, and then provides a quote. He calculated, very roughly, that perhaps $128,000 per year would be sufficient to provide service to 40 sites in Europe transmitting at 5 Kbytes/s.

However, as Mr Aparo noted, the IAEA has not yet completed their scenarios. They now use NetBEUI that is costly over international routes, and perhaps want to consider using TCP/IP methods. He repeated the concerns about security; hackers can penetrate the system's kernel in the latter, but not in the former. However, this drawback might be overcome with the encryption measures presented, and by adding firewalls.

6.4 COMSAT mobile services: Craig Poyner (COMSAT Corporation)

COMSAT (Commercial Satellite Communications) was created as a not-for-profit organization by the Satellite Act of 1962. The United States was a signatory to the organization regulating the International Mobile Satellite (Inmarsat) and the International Telecommunications Satellite (INTELSAT): as a signatory, The United States owned and

funded the organization, oversaw its management, and provided services. This summer, the organization was privatized and the signatories have become investors. Transmission services can be bought from them. Mr. Poyner described the system, its connectivity at sea, on land, and in the air, and the ways in which it might closely befit the IAEA's configurations for remote stations. Fixed dishes, and portable ones on trucks, vessels, and aircraft receive signals from the satellites and send them out on private and public networks. Satellite coverage encompasses two regions in the Atlantic, one in the Indian Ocean, and one in the Pacific region, with subdivided spot-beam coverage over land areas within these global beams. Government user operations have been manifold, including peacekeeping missions, military operations, disaster relief, law enforcement, and arms control, reporting and verification. Its established benefits are that the system is secure, it can support voice calls, and send telex, fax, data, and e-mail messages or video images. The terminals can be small ones, such as the Planet 1 mini-M terminal used on planes and for tracking vehicles; however, analog terminals are still used in some marine applications. Various levels of service are offered. Inmarsat-A meets the demand for remote interactive stations: voice quality is excellent although the service is analog, facsimile and data service is digital, and will be available at 9.6kbps by year-end, as will high speed data transfer at 56/64 kbps (asynchronously using the Internet protocol). A 36-inch directional dish is required. The system's structure is compatible with several security devices. Inmart-B, -C, and –M, all digital services, offer different speeds and combinations of voice type, quality, antenna type and dimensions: each is specially suited to its use in a different environment. Inmart-C, with its small fixed antenna, and weighing only 5lbs can send facsimiles but not receive them.

The speaker introduced COMSAT Mobile-ISND that offers the most portable high-speed data services in the world: he considers that it satisfies demands for accessing remote information and fully supports remote stations. He mentioned several manufacturers of the new superior M4 terminals; for example, the Nera World Communicator that weighs less than 10 lbs., and can accommodate up to eight handsets, and the STN ATLAS Netlink that operates at 64kbit/min for $8.

6.5 Leveraging emerging authentication and encryption technologies from the Internet and E-commerce industries for secure data communications: Leonard G. Burczyk (Los Alamos National Laboratory)

The second day of the meeting followed the pattern of the first day, starting with descriptive narratives of the Agency's requirements, with several ensuing presentations by vendors of communication systems. Mr. Burczyk began the session by introducing the Space Data Systems Group to which he belongs, and briefly describing their mission, which covers software development, data handling and exchange, and research on satellite turn-on and early orbits. He explored the impact of the recent major changes in U.S. export controls that allow the export of any encryption commodity of any key length, after a technical review, to commercial firms and other non-government end-users in any country except the seven state supporters of terrorism.

The IAEA are vitally concerned in keeping their data secure, and because of these changes, Mr. Burczyk foresees a surge of research into security issues. He discussed two important technologies: Secure Sockets Layer (SSL 3.0), and X.509 Digital Certificates. The

SSL is an open, nonproprietary and economical protocol that is making headway as an encryption standard. It sits between the transfer and application layers in a network so that it is both flexible and independent of the physical architecture of the network. It is becoming the preferred choice in TCP/IP applications both to ensure the privacy of data packages sent across the Internet, and ascertain that they reach the right person. SSL encompasses authentication and encryption both at the server and recipient, and, thereby, its integrity. Public- and secret-key cryptography is used.

The digital certificate is a small application and digital file that is readily available over the Internet or can be obtained from a Certificate Authority (CA). It is used to generate an encryption key-pair (no two keys are ever identical, so that a key can identify its owner). Thus, the sender encrypts the information with a public key, and with it validates the receiver's identity and then dispatches the data. The receiver, with the corresponding private key, is the only one who can decrypt it. Public keys are distributed freely to anyone who wishes to exchange secure information with the person at the source, but private keys are not. Generally, digital certificates are used with a SSL. The speaker listed the Internet sites where such certificates are available (at a modest cost), reminding the audience to establish a hierarchical system for key management within an institute.

Mr. Burczyk described three places wherein to apply SSLs and certificates: within the facility's TCP/IP private intranet; within the private intranet of the international data center where information from the facility is analyzed and kept; and, within the selected data communications mechanism that transfers the facility's data to the international center. He discussed the successful implementation of this scheme by United Parcel Services and at Los Alamos on very small, resource-limited devices with embedded TCP/IP data acquisition abilities. He briefly surveyed emWARE a cost-effective device for managing remote equipment via Internet technology, which is being used increasingly by industry and then closed with an overview of space-based Internet connectivity.

In answering the questions that followed, Mr. Burczyk emphasized that the IAEA should be their own certification authority. The value of this system is that it is inexpensive, yet very adaptable to the IAEA's needs.

6.6 Applicable Risk Scenarios for IAEA Safeguards Equipment and Networks; Security Issues: J. Whichello (IAEA)

Mr. Whichello listed the many equipment systems that fall under the security umbrella: surveillance; seals; instruments for nuclear detection and measurement; sensors; process equipment jointly used by several operators; computer systems and networks; and, review software. To put these items into context, he showed a slide of the IAEA's remote monitoring (RM) model. Facilities may have hundreds of sensors, tens of seals, and up to ten cameras. Information from the sensors is sent to a hub office, and eventually to Vienna. Articles 14b and 15 of the RM model require the Agency to maintain a stringent regime to ensure the confidentiality of the material and also that of any commercial, technological and industrial secrets to which they may be privy. Also, they must encrypt the data for transmission and authenticate it. Agreements on security must be reached between the Agency and member states

when data is to be shared. As Mr. Whichello pointed out, these strict stipulations mean that basic systems must be fail-safe, correctly specified, designed, and built, properly maintained and fully documented (the latter often is neglected).

He next discussed the major risks to security extending over the network from the sensors to the equipment in Vienna. The former case might involve tampering with the front of the camera's lens, and the latter jamming the IAEA's computers. The Agency mitigates these threats with a variety of countermeasures including the design of equipment, sealing critical devices with electronic seals that can be monitored, and "zeroing" security-critical information when an attack is detected. He listed the many procedures implemented, the access controls, and the trusted systems. In answer to specific questions, he said that the IAEA's security measures were strong enough to withstand an attack comparable to one that could be mounted by a national authority. Systems are audited and monitored daily by the Agency, and if security was breached, they would backtrack to pinpoint its occurrence and contact the operator in the field. Hackers attempting to penetrate the internal system in Vienna would need to know the password, which is closely tied into the needed level of security of the information; much critical data is designated "read only". In their worst-case scenarios, the IAEA also takes into account that the threat may come from people within the Agency itself, and accordingly, different divisions and sections can access only different parts of the information; the Agency designates a particular person for key management. For sharing data with member states who must dial in to the internal network in Vienna, the Agency ensures that the member's computer is outside this ring, sets up barriers, air-gaps, and both parties change their passwords daily. In a series of detailed overheads, Mr. Whichello discussed the elements of the vulnerability assessments of safeguards equipment systems that are completed, in progress, or are proposed. Member states help by sending experts for this work. In future, the Agency would like to standardize these assessments and certify equipment by internationally accepted norms. They seek help in undertaking this, and look to the member states for advice and assistance in procuring secure systems. They plan to produce a document with security guidelines covering, among other parameters, the certification requirements, the development phase, and interfacing with the Agency's safeguards network.

6.7 International security technologies: Keith Tolk (Sandia National Laboratory)

Keith Tolk discussed several aspects of security within an unattended monitoring system, including its architecture, methods of authentication and encryption, and then offered his observations and recommendations to the Agency. His first slide showed a simple unattended monitoring system, with a series of sensors and cameras, and a data collection and communication system. Here, the possibility of a threat to security is high because the host country has unlimited access for months. To obtain the data securely, the sensors must be encased in tamper-sensitive enclosures, and their links to the data collection equipment authenticated cryptographically. Due to power constraints, this authentication is often accomplished using low-power microcontrollers running custom algorithms. Although certified algorithms would be preferred, they often require more computing power than is available on these devices. Any nuclear detection devices might similarly be enclosed.

Because of the high threat level, information should be encrypted and authenticated at the sensors within the tamper-proof containment before it is sent out. Mr. Tolk suggested using both private-key and public-key technologies. Encryption prevents the disclosure of sensitive information to unauthorized people, and the host country may require that sensitive information be encrypted at the site so that it is not disclosed to terrorists. Such information might include the type, amount, and location of material at the facility, the facility's layout, and domestic safeguards. In addition, at a weapons-manufacturing plant, the host may not wish to disclose the type and quantity of material in nuclear weapon component storage containers, the isotopic content of its weapons-grade material, and information about containers that are not under IAEA safeguards. Strong complications can arise should the host insist on reviewing the information before it is passed to the IAEA because the data then may be difficult to authenticate.

Sensitive information which the Agency and host might share might include the amount and location of weapons-usable material, the amount and type of material in particular containers, the seal numbers on tamper-indicating devices, and the number and type of the host country's safeguards. The IAEA may also be aware of information that the host considers classified, such as the number of guards in a given area, the weapons they carry, and how quickly they respond to an incident.

The IAEA, on the other hand, may wish to prevent the host country knowing some information. This might cover the failure of any sensors, detailed measurements of quantities of materials that could allow the host to alter their declarations to hide a diversion (for example, if the host was cognizant of the error bars on non-destructive assays, material could be diverted). They also may wish to keep secret the detection thresholds and sensitivity of surveillance equipment (it need not go through the host's computers). Mr. Tolk suggested that the IAEA would approve, through their vulnerability assessments, the security measures needed to prevent disclosure of such information to the host, and to also prevent them from modifying the data. Similarly, the host country would approve security mechanisms for their sensitive information. He warned that the approval process might be complex.

Alternatives to encryption at the site were explored. For example, physical protection could be chosen; the inspector might collect a floppy disk from the plant or review the data at the plant.

Implementing encryption or authentication algorithms directly in hardware is problematic, because the Agency and the host cannot verify the integrity of implementation. Vulnerabilities can be built into the algorithms that could leak vital information, such as information about the key. This can be done in a manner that will still allow the device to pass NIST certification.

Mr. Tolk observed that several security technologies may be required at a single site, and that no single solution would suffice for all sites. He recommended using certified cryptographic packages when practical. He thought that the party that has approval authority should select the type of information security employed, and that those responsible for protecting the data should specify the strength of the security measures.

6.8 Export controls on strong encryption: Kathleen Kenyon (US Commerce Department)

Ms. Kenyon began by defining encryption, or Ciphertext, as the use of software or hardware to scramble data or wire/electronic communications using mathematical formulas or algorithms. It is used to ensure the privacy, authenticity, and integrity of the information, and to guarantee that it cannot be repudiated. For reasons of national security and foreign policy, all types of encryption commodities developed in the United States are controlled by the U.S. Commerce Department, and are subject to Export Administration Regulations (EAR). Ms. Kenyon discussed the exemptions to these controls and how to obtain a classification so those particular items can be exported to other countries, except the seven countries that harbor terrorists. Ms. Kenyon pointed out that within a month or so these regulations would be relaxed; the easing of export controls will help the United States to retain its commercial "edge" in the field. The new strategy will maintain the balance between privacy, commercial interests, public safety, and national security. She then considered the regulations that had previously governed the international export of encrypted mass-market software, items used as tools of trade, those used for exhibitions and demonstrations, and those for personal use abroad by U.S. citizens and foreign nationals. The complexities of the license review process were described, and the time that each stage of the process might require (up to 70 days in all). The process may be further escalated for requests that are denied by the interagency review (in which the National Security Agency, the FBI, and the Department of Defense participate). In such cases, the exemption request may go to the desk of the Secretary of Defense, and even up to the President. Guidance on the process, and answers to questions about the recent changes can be found on the Internet at http://www.bxa.doc.gov/Encryption/q&a99.htm.

New, simplified export control guidelines were established on September 16, 1999. Items for export will receive a one-time review to ascertain that they do not pose a threat to national security. After satisfactory review, "retail" encrypted materials may be exported globally to individuals, commercial firms, and non-governmental agencies (except for the seven terrorist states). Such materials are products that do not require substantial support for their installation, and are primarily designed for individual use. There are no end-use restrictions, and the post-export reporting system was considerably streamlined, and based upon business models. These new guidelines essentially implement the Wassenaar Arrangement harmonizing export controls between 33 countries. Updates scheduled for December 31, 1999 will retain a process that allows government to carefully review the export and re-export of strongly encrypted items to foreign governments and military organizations.

These new policies will not have a great impact on the IAEA. The Agency controls its encryption devices at all times, and the Agency's end-users operate under individual licenses. The Agency already has a license for 1024 bit key exchange that was granted by the Congress. However, the IAEA wants to use U.S. encryption equipment in Russia, and this may be difficult. In reply to a question about this, Ms. Kenyon suggested that the IAEA could press for legislation in Congress to overcome this problem. Possibly safeguards materials could be considered separately from encryption devices.

There were several other questions from the audience. One again concerned whether the controls on the export of other security techniques, such as hardware and tamper devices, would be relaxed. This has not yet been decided. The speaker thought that other countries would follow the lead of the United States in relaxing export controls, most probably the European Union and, possibly, Canada; other countries may not.

6.9 A technology primer in support of nuclear safeguards: Mark Sitko (MCI)

The Tuesday afternoon session, a series of presentations by representatives of major communication service providers, covered the latest technologies that might resolve some of the Agency's problems. The first talk, given by Mr. Sitko of MCI, discussed the solutions available in using Frame Relay methods, Virtual Private Networks (VPNs), and Very Small Aperture Terminals (VSATs). He assumed that to support the collection of data, the Agency would require 64Kbs of transmission, including freeze frame video and other monitoring equipment, with dial-up once a day to a hub station, and that the hubs would transmit the data overnight to Vienna. MCI would seek to establish a standard architecture throughout the system that is scalable and manageable. He also assumed that there might be between 8 and 10 hubs (although the Agency has not yet specified this). In establishing the network, MCI would need to know whether the Agency had plans to increase bandwidth, and also have details of the required security arrangements.

MCI can provide a frame relay network with a variable package-length service. Logical paths would be defined in a closed network, or could be on-demand. Such a network would be secure, as it is closed, and a high-speed frame relay could be established if more data are to be transmitted. The network can interface with ATM and the Internet via Microsoft's Gateways. In several slides, he gave details of the available port speeds, access options, and global coverage; presently, coverage is not optimal in Africa, but it is pending in Russia, South America, and Austria. He moved on to MCI's VPN service, a logical shared network that is defined on a broader physical network infrastructure, such as the Internet. Again, this is a secure network because the data stays on the network's backbone. Access to the Internet is provided through a common access loop. Although this system has not yet attained the quality desired, for example, traffic cannot be prioritized, it might be an alternative to frame relay for hub stations. The cost is based upon usage, so that the location of the hubs is immaterial (indeed, hubs could be eliminated in this particular environment). Presently the system is operational in 18 countries.

MCI's VSAT has a shared hub and uses Hughes VSAT, with a maximum transmission rate of 128Kb/s; other dish providers are also used. Data is transmitted by frame relay over satellites, and then is integrated with terrestrial frames. MCI is developing the system in South America, and other places where it is difficult to establish communications. MCI also offers private lines for communications, but notes that they are not as fault-tolerant as is frame relay. They have three excellent levels of managed services for large and small customers, and have in-country expertise for maintenance and repair.

Mr. Sitko ended his talk with some recommendations to the Agency for obtaining the best possible system at reasonable cost. He suggested that the IAEA should document and finalize its protocols, carefully define the parameters for the hubs, and consider implementing

frame relay (VSAT) between the hubs, and integrating access to dedicated VPNs as an alternative. "Voice over" technologies might well be considered because they are less expensive. Similarly, a dial-up environment might be economical, with the power plants contacting the hub once a day, for about 30 minutes, to transfer data. He also suggested that serious consideration might be given to eliminating the hubs and sending the data directly to Vienna. He suggested that the route to obtaining commercial services was to issue a Request For Information (RFI), and from the responses to formulate the strategy and architecture of the system, issue a Request for Proposals (RFP), and then make the award and implement it.

The questions from the audience principally were about the costs of the system. One participant suggested that it would be useful to purchase a block of time for dial-up services; MCI does not sell such blocks, but companies can enroll in off-peak times. Another member of the audience raised the question of saving money by changing the origin of the call. The speaker said that only in America could someone call in and then have the site call them back. A question was posed about siting a hub in the United States. Mr. Sitko believed that this might be possible, though there would be a problem with latency, but it could be analyzed further. Sometimes, the IAEA sets up small offices in other countries with staff from the Agency, as they are now doing in Argentina and South Korea, and later converts them into hubs from where inspectors can transmit information to Vienna. In such cases, the Agency does not make a cost-benefit analysis before establishing the hub.

6.10 Introduction to HOT telecommunications: Nick Leake (Hughes Network Systems)

HOT telecommunications LTD is part of Hughes Electronics, a global company that has the largest VSAT service in the world. Nick Leake described their major satellite hub facilities in Italy and the United States for global coverage, and those in UK and Germany for their European service. The VSAT service is an established technology that offers geographical independence, a uniform service worldwide, full network management, broadband capabilities, and fifth generation fully compatible software. An important benefit from IAEA's point-of-view is that VSAT does not rely on the communication systems of the local country which may be essential in some of the less developed countries wherein the Agency must establish surveillance. Hughes Network Systems already has implemented their global network; four VSAT hubs provide full coverage using INTELSAT and EUTELSAT satellites. INTEL, with its global C band capacity, covers all three oceanic regions (INTELSAT VIII is used for the Atlantic and Indian Ocean regions and the slightly older VII for the Pacific). This reliable VSAT system has had a proven availability better than 99.99% for 35 years. The system has a frame relay backbone network that includes PCBs, and has fully redundant ISDN back up. "Last mile" access is over locally leased lines belonging to the local Telephone Company. Routers at each end of the system have Ethernet interfaces. The entire network is controlled from the Global Technical Assistance Center in UK. Mr. Leake mentioned that the IAEA's SAMBA application already has been tested and demonstrated over VSAT. Here, an additional advantage for the Agency is that it facilitates interactive long-distance learning, which might lower the cost of training the Agency's inspectors, and also the sharing of hubs lowers costs. Their global network includes the Dutch Embassy, and many commercial companies throughout the world. Hughes Network Systems (HNS) introduced commercial VSAT in 1982 with the Wal-Mart network. Now the HNS has four shared hubs in New York, California, Minnesota, and

Maryland that support over 28,000 VSATs operating in 36 independent networks. In addition, companies such as Ford Motors have their own hubs and private networks (there are over 16,000 private VSATs managed by HNS).

Mr. Leake next outlined the contract that they have for building a global VSAT network for the Comprehensive Test Ban Treaty Organization (CBTO) that parallels in some respects a system which might be suitable for the Agency. CBTO requires four satellites; three for global coverage, and the fourth covering Europe. In various countries, sites are established with an outdoor antenna and a small indoor unit that provides via standard data interfaces links to the customer's equipment. Each VSAT communicates to the VSAT hub through satellite radio links, and then the hubs are connected to the customer's data center, in this case, the CBTO international center in Vienna. Information required in participating countries then is sent out (back-hauled) from Vienna. The capacity of the network can readily be expanded to meet the CBTO's needs.

The speaker then showed a set of slides listing the customers, the present network stations and those planned, and discussed the work of the dedicated licensing department who deal with the varying regulations in different countries.

The system is based upon frame-ready components, and Hughes Network Systems offers "Turnkey" services for its customers: they will design and maintain the system, survey sites and install the equipment, and monitor its functions continuously, logging and tracking all faults (there also is a multilingual help desk). The customer can access this data and see the management of the network from the remote sites.

6.11 The DISTCOM solution: Ed Hogan-Bassey (Digital Integrated Space Technology Communications)

Ed Hogan-Bassey continued the session by describing DISCOM's solution to IAEA's requirements for remote monitoring, namely, a simple, automated high-speed data-file transfer system that uses a satellite link. He began by outlining some of the drawbacks with the NetBEUI system currently used by the Agency. One problem lies in dealing with the delay introduced by the satellite link (a 0.5 seconds delay) as it is not a sliding window protocol and the packet size is very small. The best throughput that can be achieved is about 2 to 4kbps, regardless of the bandwidth when using geo-synchronous satellites. Also, NetBEUI requires that any automated file transfer application must be created, and that DOS-level commands are used to initiate transfers. There is no built-in error correction. NetBEUI was selected by the Agency based on their need for security of the data. Mr. Hogan-Bassey suggested that a network based on two protocols, TCP/IP (Transmission Control Protocol/Internet Protocol) has many advantages for IAEA's remote monitoring; among them, such a system can handle a large package size, and has a maximum throughput of 7.5kbps for a 64kbps link. Also, there are numerous applications for automated file transfer (manned or unmanned), there is a built-in error correction that detects bad data and sends the file again, and the network supports communication via NetMeeting, Chat or Internet phone applications. TCP/IP will not compromise security because it is a private network configuration with bulk encryption. A high-level encryption algorithm provides a physical layer of security that prevents intruders from

accessing the computer, and thereby the network. Indeed, he considers that the fear of unauthorized access into the TCP/IP network is misplaced, and it would be easy to "hack" into the NetBEUI system.

The speaker next described his work for the Agency. At the request and specifications of the SGOC, the Systems and Communication Unit tested this mode of satellite and TCP/IP communication. The aim was to establish the technical implications and costs of installing such a system in remote geographical areas. DISTCOM provided the satellite dish and terminal (prototypes), and transmitted the data via the INMARSAT satellite. The configuration of the test consisted of a single hop – a terrestrial ISDN between Vienna and the satellite hub in France (for which only a telephone handset is needed), and a satellite link between the hub and the satellite dish at the remote station. France Telecom set up the link, and the TCP/IP was used. After an initial false start with the prototypes, which were replaced, the terminal performed satisfactorily and the effectiveness of the TCP/IP protocol was verified. Furthermore, a Multicast Dissemination Protocol designed to multicast files (one-to-many transfers) running on top of the TCP/IP performed well. This latter protocol is in the public domain, is being improved, and its application is free. Mr. Hogan-Bassey believes that satellite dishes could be set up in remote locations within a room with windows or bars (to prevent theft). The system could be very satisfactory for securing voice messages and for monitoring fiber-optic seals using video to record scene changes. Rather few images would be generated so that they could be transmitted in a few minutes at low cost. He showed in a preliminary evaluation of costs, with various permutations, that the system would realize savings for the Agency. He concluded that the system seems reliable, and performs well, and given the small number of sites, and the small quantity of data to be transferred, the DISCOM solution is a good one.

6.12 An overview of AT&T Concert: Peter Taylor (AT&T Concert Enterprise Services)

Peter Taylor continued the session with an overview of AT&T Concert Enterprise Services that are part of the AT&T-BT Global Venture. He described this global venture as a seamless, dynamic worldwide service, using local expertise in telecommunications to achieve high standards of consistent performance. He showed slides of the "old" multi-lateral global telecom model that was a patchwork system, based on regional contractual arrangements, and sorely needed a lead member for expanding and bettering the system. AT&T and AT&T-UK were part of this melange. He briefly outlined the events leading up to the global venture, and how the relationship between AT&T, BT, and Concert evolved. Concert, the new coherent model, with inputs from AT&T and BT, manages the entire global CISCO-based platform. With an infrastructure for high-speed 200-Gigabit IP backbone network and complementary equipment throughout, there was instant access to over 100 international cities. Now, after the acquisition of IBM's Global Network (IGN), customers can dial 1,300 cities. Concert's multinational products are simple to buy, competitive in price, and are supported by leading-edge services and technologies. The network covers 6 continents, and 50 countries, including Russia; the network's capacity expanded ten-fold in less than four years. The speaker went on to give more details of the architecture of the network, and the coverage in different parts of the world, including Concert's frame relay service, its voice network, and intelligent call processing, and finally showing a slide of the comprehensive product portfolio.

Mr. Taylor then focussed upon the IAEA's needs, and how Concert might meet them. First, he summarized Concert's value proposition: It offers a seamless global network; a fully redundant backbone; fully owned and managed backbone network to more than 40 countries; fully managed end-to-end service; simplified contracts; integrated billing; and service level guarantees. He stated that Concert plans to establish a presence in Argentina in the first quarter of the year 2000, and mentioned the regulatory problems that may be involved. He suggested that the Agency should consider putting together a document stating where they have and will have remote sites. In this way, they could be approached as a network with shared ports, rather than one by one, and accordingly the costs would fall (with more than five sites, significant saving could be made). Such a single solution would give AT&T more flexibility in pricing.

6.13 AT&T's proposed solution for IAEA: Lester Martin (AT&T)

This presentation, by Lester Martin, was closely tied in to the previous talk, and offered the Agency definitive resolutions for their problems. He suggested, as a basic, an expansion of the frame relay network with shared ports, adding more surveillance cameras, and TCP/IP encapsulation; this would provide a secure, simple, and ubiquitous system with the flexibility for growth. Mr. Aparo inquired about the possibility of dialing out from a POP (Post Office Protocol) site to a remote site of the frame relay to the termination site used a local dial line; this cannot be done. However, Mr. Martin stated that a customer's own equipment could be used at a POP site. Since the IAEA's equipment is sealed, this could resolve a problem in Argentina where the frame relay is sited in a hotel and no one is responsible for its security. Mr. Aparo mentioned that the broad bandwidth of this AT&T system was unnecessary for the Agency since their transmissions were short ones and a small bandwidth would be preferable. Mr. Martin replied that the 64k port could not be split, and that each port has excess access capacity (in some cases up to 50%).

The speaker noted that the minimum contract was for one year; with longer time, the price drops. A solution for the IAEA might be to purchase a low base rate, and to use a "burst" rate for the few times when the volume of traffic required it. In future, AT&T plan not to charge for "bursting" on international communications; there is no charge for it now domestically. The pricing of access lines also varies with country, being cheap in the United States and the UK where there is competition between communication companies, but rising steeply where competition is limited.

Mr. Martin connected the higher expenses that the Agency encounters to the piecemeal planning and additions. It would be better to set out the overall configuration needed, though not integrating secure data with non-secure material, so that trade-offs could be made within the system to cut costs. He considered that the Agency should adopt TCP/IP encapsulation within their system, and suggested moving to a layer 3 level (AT&T offers layer 2, and other companies have layer 3).

6.14 CTBTO lessons learned: William Farrell (SAIC-Center for Monitoring Research)

William Farrell gave the afternoon's final presentation on experiences gained over five years at a prototype international data center (PIDC) that models for the Comprehensive Nuclear Test Ban Treaty Organization (CTBTO) network. The CTBTO will be collecting ~10Gbyte/day of data from a worldwide network of sensors. The PIDC was set up to analyze and disseminate data and products to support monitoring nuclear tests in different environments, and to send out the information to national data centers.

In an overview, Mr. Farrell pointed out that data problems occur most often before the information enters or leaves the communications circuits. Also, failures were attributable to the voluntary contributors of the information, and to hardware, software, and human faults at the PDIC. He discussed the global private VSAT system that CTBTO is establishing, noting that its status would be elaborately monitored, and that additional means would be sought to track the status of the individual stations. He described communication technology at the hub and spokes of the network, emphasizing the advantages of centralized management, and commenting on the difficulties in managing the spider-web of tail circuits at the spokes' ends; he cautioned against using copper in conduits in less developed areas as it often is removed. He showed slides of the global seismic, hydroacoustic, and radionuclide networks.

The technologies employed include Unix, security measures, and the Web. Unix has socket-level interfaces for streamlining the data, and e-mail is used for text data. Middleware, such as Oracle (database management system) and Tuxedo (TP monitor), are used extensively. Security measures include firewalls, and packet filters. Encryption is not needed, but the measures must ensure that the data have not been tampered with; therefore, DSA signatures on a time-series data are required, and S/MIME authentication for text data. The Web is used to transmit the monitoring information to the signatories of the treaty, but this can safely go outside private lines. The Web is useful for disseminating the material. Several valuable lessons were learned; particularly, that obtaining information about the state of the data providers is labor-intensive. He advocates using standard protocols, and having redundant circuits, with a private network as a baseline and fail-over to the Internet. He urged the Agency to plan for computers to fail and processes to stop, so that the original design of the system should be carefully thought out, choosing on that will function continuously over a long time. Copious status logs should be maintained.

There was a unified initial design for the CBTO network, not a piecemeal one. This design was given to the vendors with details of terms of reference for the sensors at each station, the bandwidth needed, and the headspace, so that they could suggest the best satellite system, and the most cost-effective way to implement the network. He urged the Agency to follow suit.

6.15 Data communications for safeguards information: Tony Capel (Comgate Engineering Limited)

Tony Capel made the final presentation from the service providers. His analytical overview, exemplified in detailed slides, covered the application requirements, the network configurations, its costs, the configuration selected, security measures, and finished with an example of its implementation.

Under application requirements, he first discussed monitoring fuel movement with 12 cameras, radiation monitors, and electronic seals, and then storing and forwarding the data. A 3:1 compression rate was assumed (using a lossless compressor). He compared the time that it would take to move differing amounts of data at channel throughputs of 64kb/s and 128 kb/s via this store and forward system. He similarly explored the real-time mode, using one or two cameras (with different frame rates), radiation monitors and a microphone for sound. In this case, aggressive lossy compression was assumed. Since the images transmitted may not meet legal requirements (a local copy was made which could be transmitted later at a lower compression rate for archival purposes).

The network configuration Mr. Capel analyzed consisted of 6 remote monitoring sites sending data to the IAEA hub in Toronto, Canada, which then sent it to Vienna (the store and forward mode). He compared the various options that could be used in those circumstances, calculating the five-year cost of each (including installation). For the site-monitoring network, there were large differences in these costs. The least expensive was one using a local Digital Subscriber Line (DSL), or an Asymmetric Digital Subscriber Line (ADSL), combined with an Internet Protocol (IP) network; this option might have a minimum level of real-time usage. Transmission by satellite from the local area was the most costly option although advantageous in that there are no fiber optic lines on the site. Furthermore, if little data are to be sent the number of sites on the same footprint of the satellite can be increased. He then showed the five-year costs for options for the storage site network. Again, there were large differences, the most favorable one is a combination of local DSL and IP network.

Mr. Capel made recommendations to the Agency for selecting an IP protocol network service: Its quality should be guaranteed by agreements (developments underway will soon allow the IP networks to offer service guarantees comparable to those of ATM networks) and network layer security could be addressed using commercially available IP security products. He suggested that if public IP networks were not acceptable, private ones are feasible (e.g., using IP over ATM or frame relay). He would require conformation of the performance of any solution before it was installed. He showed his final selected configuration for the network of 6 stations and the IAEA hub in Toronto, including a mobile inspector who can dial into the Internet without affecting the hub's technology. The hub would have two circuits for redundancy.

Mr. Capel moved on to discuss the security measures essential to the Agency, with a slide of an example implementation reaching from the remote sites to Vienna. ATM and frame relay packages are reasonably secure, but not enough for the IAEA. He suggested having signing capacity at the data's origin, immediately after compression (though signing before

compression would be required if a lossy compressor were used, e.g. for real-time data). Network layer encryption is economical and could be applied using self-contained stable Internet Protocol Security (IPSec) boxes installed in series with each node's connection to the IP network. IP data transmitted by each node (e.g., monitored site) would be sent using an authenticated and encrypted secure "tunnel" to the corresponding destination node (e.g., in Vienna). The IPSec system is available commercially. Mobile inspectors must carry an IPSec box (or use IPSec software in the laptop) to access the network from a laptop computer. These boxes are small (and will become smaller with further development, and cost between $5,000 and $15,000 depending upon their data throughput capacity. He also discussed other related security issues, including audit trails, key management requirements, use of public key infrastructures (PKI), security policy and certificate issues, and signature verification. He recommended the implementation of a comprehensive IAEA-wide key management approach based on PKI and the use of dedicated self-contained IPSec security devices (he recommended against the implementation of IPSec using software within existing computers or laptop computers.

7.0 GENERAL FORUM: Facilitator Massimo Aparo (IAEA)

It became clear during the meeting that the IAEA faces the unenviable task of choosing among several very promising technologies for transmitting data from their remote sites. Whilst this choice, in itself, is challenging, the Agency's very special requirements confound the issues. The security and authenticity of the transmitted data must be assured, and the IAEA's requirements exceed those of many other organizations. There are significant problems at the remote sites, such as the lack of a local communications infrastructure, and often, political ones. A major hindrance to the Agency is that a system cannot be selected solely on the grounds of its meeting these requirements. The costs of buying, installing, and maintaining the system pose big constraints, entailing the need for cost-benefit analyses. The Agency faces severe budget restraints and staff is never sure what monies will be available, even in the next budget, but they assured member states that remote monitoring would save money. Finally, there is the vexed question of where the technologies will go in the future, and whether the system selected now will prove to be the best in the long term.

The presentations of the technology providers showed that they were cognizant of these complex problems and were willing to extend their efforts to resolve them and provide the IAEA with the best possible communication system. However, all expressed their wish to have some preliminary guidance from the Agency in terms of the issuance of a requirement document specifying the basic parameters that the system must have.

Thus, the discussions, which followed, centered on economics and Request for Information (RFIs).

Mr. Aparo opened the forum by expressing the Agency's satisfaction with the meeting, which had allowed staff to meet the service providers face-to-face and to become familiar with the various systems that were available. Equally, he thought that this interaction with the IAEA's staff would be valuable to the providers in clarifying the Agency's requirements. He expressed his thanks to the organizers of the meeting.

Is remote monitoring preferable to sending out inspectors?

There was debate about whether there is any value in having remote stations and if the Agency would be better served by sending out inspectors to collect the data from remote sites and hubs. This might be a viable option if there were modest amounts of data, and time was not pressing. Thus, to send an inspector to Argentina (where the Agency will start to operate in 2000) might cost about $6,000, the equivalent of using frame relay transmission for a month. Remote sites might be automated to simple transmit information on their state of health, and store the data until the inspector collects it. Such separation would reduce costs, at least until the expense of transmitting all the data came down. Also, unattended monitors at remote stations are costly, and a secure pipeline is needed to send out the information. Inspectors still must visit them to check the seals, and technicians also to maintain the equipment.

Arguing against this option were concerns about the security of the inspectors in politically unstable areas, and costs. For example, the expenses are very high in sending an inspector to sites with weapons-grade materials as many escorts are needed. Remote monitoring also is advantageous in removing responsibility from the local country; lightening this load benefits the member nations. As the various safeguards are integrated, fewer cameras will be needed and expenses will fall, especially in countries having a reasonable communications infrastructure.

Remote monitoring is valuable in reactors handling core fuel in multi-unit stations, and where spent fuel is transferred to storage; in both cases, inspectors must be present for long times.

Lessons learned from the present communications systems

The Agency has already installed a large number of remote stations and hubs and linked them in various ways to Vienna. For example, frame relays are in place from Toronto and Tokyo to Vienna. However, too little time has elapsed for the IAEA to thoroughly assess the savings made; the analysis started in September and is still underway. The coming year is a crucial one since there will be no change in their program until 2001, and by then, the information should be available (although the IAEA will need support in collecting it). The Agency is considering putting in frame relay in Rio, Brazil; it was suggested that a decision might be delayed until there are more definitive answers, particularly since there is equipment already collecting the data at the nuclear sites. Indeed, with their limited funds the Agency might limit their plans for increasing the number of stations with remote monitoring. One participant strongly urged the Agency to freeze further development of remote monitoring for two or three years, and then reassess the technologies.

Request for information from the Agency

The equipment vendors were unanimous in asking the Agency to consider preparing and sending out a request for information specifying their preconception of the system needed, their mission statement, and their operational requirements. The projected budget need not be part of this early stage document. IAEA staff stated that they lacked the resources to do this, and would

have to seek help from member states. On the other hand, they conceded that many of the issues about encryption and authentication have been resolved and that there are a number of excellent documents from which they could model their RFI (the CTBTO system was not one of these). The RFI should be solution-driven, not problem-driven as was done in the past, but retain flexibility.

Summation

Michael Farnitano, representing the host organization, summed up the substance of the forum. He spoke again of the need to reassess the costs of the existing network, and from this evaluation, to focus and sharpen the requirements in the RFI. He stressed the Agency's need for coordinated support from the member states in all these effort, as had happened in the trials in Canada (reported by Tony Capel). Different scenarios might necessitate different solutions.

He suggested that the service providers might possibly respond to an RFI at no cost, which would be of great benefit to the Agency, and might even consider travelling to Vienna to explain their systems. Otherwise, the Agency might consider using an intermediate consultant to first clarify the parameters of their system (alternatively, the services of a consultant might be more valuable after receiving the responses to the RFI).