Technology Development for Nuclear Transparency Applications

John N. Olsen and Charles D. Harmon
Cooperative Monitoring Center
Sandia National Laboratories i
Prepared for the
Third Annual JNC International Forum on the Peaceful Use of Nuclear Energy
Tokyo, Japan, February 21-22, 2001

Abstract

Nuclear energy has an important role in the mix of energy supplies for the coming years, yet is a source of concern on safety and proliferation grounds. The nuclear energy industry addresses these concerns by using transparency to demonstrate compliance with international treaties and conventions and to show the public that operations are safe and emissions are within authorized limits. Transparency measures are becoming increasingly based on technology, both to decrease costs and to increase availability of information. Modern transparency technologies for international nuclear safeguards are tending toward integrated sensor systems, Internet accessibility, and improved software analysis. Public acceptance measures rely extensively upon Internet tools and are beginning to take on a regional nature - reflecting the potential trans-boundary consequences of any future accident. Security of transparency information is also improving as limited sharing of sensitive information is contemplated for the future

Introduction

Even as the peaceful use of nuclear energy continues to contribute to economic development around the world, concerns about safety and nonproliferation continue to require renewed attention. Demonstration of safe operations and responsible material control is the role of transparency. Transparency in nuclear activities serves different purposes for different partners. Nuclear operators share safety data with their domestic population and local authorities, but they also share material control data with regulatory bodies and the International Atomic Energy Agency (IAEA). Some measures are mandated by law and are obligatory, while other measures are voluntary, intended to allay concerns and establish positive relationships. In order to focus on transparency technologies in this paper, we will note that thorough definitions of transparency and the motivations of various "stakeholders" for participating in transparency measures are available in our previous paper[2].

Transparency measures in the context of the nuclear industry represent additional overhead. Although these costs are necessary, the use of technology to reduce costs while maintaining quality is highly important in transparency activities. Technological tools can also reduce human exposure to radiation and improve the security of nuclear materials in some transparency applications.

In this paper we will summarize development and demonstration of new technologies to support transparency measures. While we will describe certain technologies being used in a specific transparency application, the application opportunities are much larger. Thus, sensor hardware or analysis software to support IAEA safeguards might also find uses in voluntary transparency measures. Similarly, "trusted sensors" developed for international disarmament might find broader applications in international transparency.

The following discussion will highlight first two new sensor packages for remote monitoring and summarize an on-going demonstration program at the Waste Isolation Pilot Plant (WIPP). Then, we turn to the issue of providing transparency while protecting sensitive information. Concepts here focus on secure transmission of protected information or secure analysis to provide sharable output. Finally, we consider transparency more broadly, using the example of the regional web-site, *Nuclear Transparency in the Asia Pacific*, and a virtual tour technology that might be useful in many web-sites. We close with the topic of analysis of transparency data - making sense of it all through *Knowledge Generation* software.

New Results in Remote Monitoring

There are three elements in any remote monitoring system: sensors to measure observable quantities; communication links; and data storage and analysis systems. It is appropriate to start out with a review of two improved sensor systems. The current demonstration at the Waste isolation Pilot Plant (WIPP) will serve to illustrate a complete system concept. Further examples of remote monitoring technologies will be found in the paper[3] on the system at the JOYO reactor, which was engineered in collaboration between the JNC and Sandia.

Item Monitoring "Electronic Sensor Platform" (ESP)

A battery-powered and radio-reporting sensor package is essential for many applications of unattended, long term remote monitoring. This is particularly true when the sensor must be attached to a container or equipment whose location is not permanent or where hardwired connections would interfere with facility operations. The "Electronic Sensor Platform" (ESP)[4] is aimed at this need. The system is composed of the ESP itself and a communications module, known as the "Interrogator/Transceiver" (IT).

The sensor package is battery powered for up to 4.4 years of ultra-low power radio frequency communication at 915 MHz. The current sensors measure basic quantities, like motion, temperature, and fiber optic seal integrity. The system can also accept analogue and digital signals from external devices, such as radiation detectors. The sensor is particularly strong against tampering or imitation. Each signal carries an authentication signature calculated from a Sandia-improved encryption algorithm; all messages and events in messages have unique counts. In case of physical tampering to incapacitate the sensor, the ESP destroys its own signature key, so that it cannot be imitated or re-started later. The ESP preserves the last 100 messages in its buffer in case of temporary communications failure.

The Interrogator/Transceiver, IT, requires external power because of frequent communications with many reporting ESPs. The IT communicates to the data storage system by means of an RS-232 port.

The applications below at the Waste Isolation Pilot Plant (WIPP) and in the Virtual Private Network are typical demonstrations.

Modular Monitoring System: The "Box-On-the-Wall"

In many monitoring applications it may be desirable to mount an entire sensor suite in one unitized assembly. For example, it may be desired to limit the installation time of a monitoring system and decrease the access time of personnel to a nuclear material storage facility. The *Box-On-the-Wall (BOW)* is intended for monitoring access to assets within a nuclear material storage facility.

The BOW would be mounted inside the facility above and to the side of the door. Having a camera looking straight ahead and one looking to the side across the doorway, the BOW captures triggered images of the interior for assessment of sensor-generated events. Entry or movement within the space would trigger door (balanced magnetic) switches or passive infrared detectors. These inputs and BOW enclosure tamper switches could trigger the cameras. Cameras can use infrared illuminators to ensure "dark room" sensitivity. The BOW also communicates with a ESP sensor package. This sensor suite typically monitors the status of fiber optic seals and movement of stored items. For redundancy, a second BOW unit would be mounted inside the facility on the other side of the door. The camera in each BOW monitoring across the doorway would be adjusted to also monitor the other BOW.

The BOWs are interfaced to a power module unit outside the storage building. This unit supplies the low voltage DC power, houses an un-interruptible power supply (UPS), monitors the status of the AC power, and contains the network communications link. The outside unit also has tamper detection features. The data is communicated to a storage computer located at a nearby data collection and storage facility. BOW systems have been installed for long term testing on two empty storage sites at Sandia.

Nuclear Waste Repository Monitoring at "WIPP"

In 1999 the Waste Isolation Pilot Plant (WIPP) hosted a demonstration of a number of transparency technologies, which continue to be upgraded. As the world's only licensed and operating geologic repository for nuclear waste, tests at WIPP are experiences in coping with real life conditions in an operating facility with strict configuration control mechanisms. Transparency technologies at WIPP were featured in a workshop[5] in July 2000 on transparency in the back end of the fuel cycle. Based on this start, WIPP may evolve to be a site for international testing and development of transparency systems.

A distinguishing feature of the WIPP transparency system is that it is Internet –accessible[6]. Compared to the previous generation of modem-accessed systems, the data availability to the public is much higher; the public potentially can find the site through search engines.

The WIPP transparency system is composed of three sensor types:

1. NTvision video surveillance cameras[7], capable of change detection
2. T-1 sensor packages, attached to simulated waste containers
3. Environmental monitors above ground and in a repository tunnels 650 meter below ground

The WIPP system is typical of a configuration that might be chosen for public acceptance transparency. The web-viewer can observe near-real time video sequences of activity around a stack of simulated waste drums and can call up archived images, as well. The two NTvision cameras can trigger themselves when activity starts or can be triggered externally by sensors or operator commands. On the drums themselves, there is an ESP package to monitor motion and temperature (basic safety data) and a fiber seal (a security feature). In addition, environmental information affecting both the container below ground and the public above ground is available.

Future expansion of the demonstration could include monitoring actual waste drums and including radiation sensors above and below ground in the web-site. A portion of a tunnel has been set aside for cooperative experiments that might include international development of new sensor systems in this realistic test environment.

Handling Sensitive Information:

Transparency concerning nuclear activities poses serious concerns over protection of sensitive data. That is, while the nuclear industries and government ministries intend to use transparency to reduce concerns about nuclear activities, or to show compliance with treaties and agreements, there are economic and security limits to transparency. Some information must be protected, even while associated information can be shared. Two approaches to data protection are of interest. In the first, sensitive data is shared but access to that data is protected in an Internet-based *virtual private network.* A different approach, using a *trusted analysis system*, analyzes highly sensitive information but transmits only sharable data.

Virtual Private Networks

Nuclear material monitoring is an example of bilateral transparency - between the IAEA and a State- that requires confidentiality. As the IAEA responsibilities to safeguard nuclear materials continues to grow, while implementing INFCIRC 540 protocols, the cost of secure data transmission may become an obstacle. Virtual Private Networks (VPN) can provide secure data links over high-bandwidth Internet links, while improving inspector access and potentially reducing communication costs. Sandia National Laboratories and Finland's Radiation and Nuclear Safety Authority (STUK) have successfully tested[8] the use of a VPN between STUK and the IAEA in Vienna as a field demonstration.

The potential cost advantage of the Internet is fairly obvious. In leased-line data networks, the system must pay for international lines between all partners. In an Internet system, only fees for access to the local provider arise. Cost aside, the Internet offers more data transmission paths, so that reliability may be improved at the same time.

Previously, Internet transmission raised concerns about data security. A VPN allows secure data transmission over an untrusted public network, such as the Internet. VPN users can define encrypted and/or authenticated tunnels through the Internet:

- *Encryption* converts data from a readable format to cipher text that only the intended recipient can decipher. Most VPNs include encryption algorithms such as 3DES, DES, RC5, Blowfish, CAST, or IDEA.
- *Authentication* verifies that the data has not been altered, substituted or removed. It does this by creating a unique signature based on the data. If the data were altered, re-authentication by the recipient would show mismatched signatures. VPN data authentication can use a number of algorithms including MD5 and SHA-1.

The demonstration between STUK and the IAEA utilized both functions. Thus, the original data was encrypted and sent within a new data string and an authentication signature was appended to the end of the string.

The STUK data transmitted was from a station monitoring airborne radiation monitoring. The task for the VPN was to assure that data could not be intercepted by hackers or altered by intruders. Thus, the STUK installation included a video camera, door switches and instrument cabinet switches for physical security. Some of the switches could trigger the video camera. The integrity of the data was further strengthened by means of periodic injection of aerosol particulates, whose chemical signatures were known. (This step would involve manual inspection under an electron microscope.)

New keys for encryption were automatically exchanged every hour; authentication keys were updated every eight hours. No security problems were found in seven months of operation and data availability through the Internet was 100%.

Trusted Sensor Systems

Rigorous standards for data security may exist in future agreements to monitor nuclear materials or processes. The data to identify a particular nuclear material or process may contain information that must be protected for economic or physical security reasons, even while transparently demonstrating that the material is "accounted for" or that a process is "as declared." For example, in a reprocessing plant it might be desired to be transparent regarding the separated plutonium inventory, while protecting information regarding the process efficiency (information of economic importance).

Sandia is developing monitoring technologies that can process extremely sensitive data and yet only transmit sharable information. Although this is intended to support future weapon dismantlement agreements, the applications could extend to transparency in peaceful uses of nuclear energy. Two general approaches to a *trusted sensor* system may illustrate the concept:

- Divided hardware and software design isolates classified data from unclassified output. - This approach generates a *Trusted Radiation Attribute[9]*. The goal in this sensor is to identify weapons-grade plutonium and confirm that the monitored item constitutes more than a certain amount. High resolution gamma spectra in the 600 keV region identify low ^{240}Pu/^{239}Pu materials as weapons-grade; then peak-to-continuum ratios allow a lower bound, mass estimate based on low angle scattering. This data is very sensitive information. The analysis must be confined to a simple processor (PC-104 card) that is welded into a stainless steel container; the analysis card is only allowed to communicate the final result to the output card via a one-way optical link. Software on the analysis board must be authenticated, but not read, from the outside. The steel container is designed for eddy-current weld-checking and also suppression of electrical emissions. Thus, the classified information has no path to the outside world, but an inspector can verify that an object is indeed, a treaty-controlled item.

- A processor analyzes spectral data, pulse by pulse, in a manner that is incapable of generating classified output, yet identifies a previously known object. - This instrument has been labeled *Radiation Continuity Checker (RCC)[10]*. Its use would be primarily to identify an item, thus providing continuity of knowledge. The RCC observes the gamma spectrum with a NaI detector and computes a cumulative value based on a weighted multiplier for each pulse. Each channel in the spectrum analyzer is assigned a fixed weighting value. Since the sum is computed one pulse at a time, a classified spectrum does not accumulate; however, the resulting sum is an accurate identifier of an item. Attention to collimation of the input gamma rays allows the background to be reduced to negligible levels. The detector, analogue-to-digital converter, and microprocessor are housed in a tamper-resistant fiberglass package. In theory, a nuclear weapon placed in storage pending destruction would be analyzed once by the RCC. Subsequent inspections would confirm that the weapon was still in storage until the time that a properly verified dismantlement could take place.

Internet Transparency Trends

A common feature in many applications for transparency technology is the use of the Internet for disseminating the data. As an example, we feature a regional Internet site that is based in many ways on the existing transparency web-sites of many organizations throughout the Asia Pacific. The goal of the *Nuclear Transparency in the Asia Pacific[11]* web-site is to provide a "one-stop shopping" site for viewers interested in broad access to nuclear energy information related to safety and nonproliferation. A new transparency tool, *virtual tours,* is being considered for the regional web-site. Individual operating companies may also find it useful to strengthen their public acceptance efforts.

Regional Transparency Project on the Internet

The Internet offers an efficient, cost effective way for power companies, research institutions and governments to mount nuclear transparency efforts. Many of the organizations represented at this conference are leaders in this respect. Unfortunately, the fragmentation of information between sites, language differences between the host countries, and institutional complexity exhibited in sites make it very difficult to actually assemble understanding from all of this transparency.

The *Council on Security Cooperation in the Asia Pacific (CSCAP)* is attempting to address this problem by developing a "one-stop shopping" entry point to transparency efforts throughout the Asia Pacific. CSCAP is a non-governmental process that works on many security topics; nuclear cooperation to counter proliferation and address safety concerns has been a very active area for the last five years. With support from the US DOE our group at the CMC has offered technical assistance to the CSCAP. The result is a web-site titled *Nuclear Transparency in the Asia Pacific[12].*

The web-site attempts to serve four major goals:

- Describe nuclear transparency technologies and display example applications, primarily in Japan, Korea, Taiwan and the U.S.
- Overview nuclear industries of the Asia Pacific and supply numerous hyperlinks to industry, research and government web-sites
- Institute sharing of actual near-real time data from many sources; the focus is on airborne radiation monitoring for safety and emergency warning
- Provide a *Current Events* section to highlight stories of general interest as supplied by the member CSCAP committees

In addition, the web-site contains many background documents on proposed regional nuclear cooperation (PACATOM or ASIATOM) and a full history of the activities of the CSCAP Nuclear Experts Group that guides the site development.

Each of these functions is partially available elsewhere. The problem is that search engines really are not very good at crawling across multiple languages and searching for esoteric information deep within giant corporate web-sites. CSCAP believes that a unified entry point will serve a useful function as transparency takes on regional and international importance.

Airborne radiation data is useful across the region because of the obvious trans-boundary effects of a radiation accident. The CSCAP web-site features links to national monitoring in Korea[13], site monitoring in Japan[14], and regional monitoring in the U.S.[15]. This function will shortly embark on a more ambitious phase in which data sent directly (over the Internet by ftp) to the server at the CMC will be archived and displayed in a unified, user-friendly manner. Taiwan[16] has been sending direct data for a year now and the JNC's O-arai site will start shortly. Combined with the LANL *NEWNET* system this will provide an exercise in developing[17] an international database with a uniform appearance and common units. We are very interested in adding new partners to this endeavor.

Virtual Tours as a Transparency Tool

The wide use of the Internet in commercial applications, like sale of real estate, has generated a new transparency tool - the *Virtual Tour.* If nuclear power plant visits in Japan, South Korea, China, Taiwan and US have made strongly positive impressions on our CSCAP Nuclear Experts Group, why not help a wider set of viewers take virtual tours? The thought is that web-sites could show some typical areas of facilities to people who have not had opportunities for first-hand visits. The images in the tour would be pre-recorded; they would not be real-time.

The CMC has purchased a camera and software system by iPIX[18], which can be used to create web-site based virtual tours. With the iPIX camera (a very wide-angle lens on a digital Nikon camera) only two images are needed. The software "stitches" the images together, so that the viewer can move his "eyes" around to any angle, as if he were in the room. Furthermore, "hot spots" can be added where the viewer can click for close-up images. The "hot spots" can even transport the viewer into the next room or back outside.

Security is a concern, of course. Image resolution in the pre-recorded web-viewer would not be sufficient to expose details of security features or certain areas in the images could be blurred or masked before the image is included in the web-site.

The CMC is currently building a virtual tour of a reactor facility at Oak Ridge National Laboratory. This first application will be a simulation of an inspection for the purpose of training inspectors. A less detailed tour would be an effective and entertaining tool in improving public acceptance.

Making Transparency Useful: Knowledge Generation

Transparency between nuclear facilities and the IAEA or regulatory bodies will increasingly rely upon electronic means. Remote monitoring systems will gradually assume some of the functions of traditional material safeguards and strengthen the powers of regulators in areas of safety compliance. Operating around the clock, incorporating inputs from dozens to hundreds of sensors and in a facility where multiple activities are happening, the monitoring system could generate huge amounts of data. Obviously, the data volume and complexity could overwhelm human analysts. Hence, the need for automated *Knowledge Generation (KG)[19]* to sift through the data and assign the sensor sequences to known causes, or highlight unexplained events.

The key to KG is to model all expected processes on the basis of expected sensor signals. This requires some thought about sensor design and placement so that identical sensor sequences will not occur for different processes. In an ideal situation, the KG program could identify all processes that occur and compare those to the declarations made by the facility operators. There would be no extra events and no missing events; materials safeguards would be complete and automatic.

KG is useful outside of safeguards also. Sensor signals outside of pre-set bounds would identify malfunctions. Sensor sequences could identify processes that were not proceeding as modeled - perhaps an indication of deviation from safe operations, perhaps an indication of material diversion.

KG software was tested at a robotic material handling facility at Sandia. In this test ESP sensor packages were attached to simulated nuclear containers and moved around a facility with 3 infrared breakbeams, 4 passive infrared motion sensors, 2 digital cameras (DCM-14 Neumann) and 2 door switches on entries. A robotic vehicle moved the containers about the facility in the presence of people, who also triggered some of the motion detectors. In this environment the KG identified all events and also caught an accidental breakage of a fiber optic seal. In the course of the test, the greatest difficulty was separating random human motions from the well-modeled robotic vehicle patterns.

In cooperation with the IAEA and ABACC, Sandia has tested KG software by monitoring a spent fuel transfer campaign at the Embalse plant in Argentina during November 1999. Although hampered by several radiation detector failures, the KG software identified fuel transfer events and could distinguish alternatives to the basic expected process. The software is expanding to account for more variations (slower container weld times, material left in the hot cell overnight, steps out of expected order, etc.). This is still a work in progress, but will be an essential tool in future monitoring systems.

The operator display is seen to be key to a useful KG system. At the most abstract level the display compares observed and declared processes, and points out how many discrepancies occurred. On more detailed levels, the operator can examine the discrepancies within the processes and even look at the sensor raw data, if desired. With inclusion of material control serial numbers, the system can also tackle more abstract concepts, like "continuity of knowledge."

KG analysis need not be limited to safeguards. Imagine an Internet linked, worldwide system of airborne radiation monitors for emergency warning. With KG software these data could be compared to meteorological inputs; changes could be tracked back through air transport calculations to a Global Information System (GIS) database of declared nuclear activities for rapid identification of problems.

Conclusions

Technologies to support transparency measures continue to evolve. Sensor platforms have become more modular in nature, can carry out many functions, and contain improved data security capabilities. Internet connectivity will provide the key to reaching a broad range of viewers with public acceptance transparency, while supporting confidential transparency in a cost-effective manner.
Successful implementation of the technologies noted here will generate huge amounts of data. More attention must be devoted to generating real understanding, as suggested by the Knowledge Generation software development program.

---

[1] Sandia National Laboratories is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

[2] Charles D. Harmon, John N. Olsen, and Howard D. Passell, "Nuclear Facility Transparency: Definitions and Concepts," presented at the U.S.-Japan Energy Seminar, Washington, DC, October 4-6, 2000 and available at http://www.cmc.sandia.gov/00reserch-analysis/paperandreports/

[3] Yu Hashimoto, "Demonstration of Remote Monitoring System," Session II, this conference.

[4] Steven J. Blankenau, Sandia National Laboratories, sjblank@sandia.gov

[5] Workshop summary available at http://www.cmc.sandia.gov/Nuc_Trans/RACsummary.html

[6] See http://wippdsc.wipp.CARLSBAD.nm.us/default.htm

[7] Len Burczyk, Los Alamos National Laboratory, lburczyk@lanl.gov

[8] Heidi Anne Smartt, Susan Caskey, Robert Martinez, and Tapani Honkamaa, "Application of a Virtual Private Network to the Finnish Remote Environmental Monitoring System"

[9] Dean J. Mitchell and Keith M. Tolk, "Trusted Radiation Attribute Demonstration System", presented at INMM 41st Meeting, New Orleans, July 16-20, 2000.

[10] A. Bernstein, B. A. Brunett, N. R. Hilton, J. C. Lund, and J. M. Van Scyoc, "The 'Radiation Continuity Checker', an Instrument for Monitoring Nuclear Disarmament Treaty Compliance," Presented at IEEE Nuclear Science Symposium, Lyon France October 2000; Submitted for publication to: IEEE Nuclear Science Symposium, Conference 2000 Proceedings, IEEE Transactions on Nuclear Science.

[11] http://www.cmc.sandia.gov/Nuc_Trans/

[12] http://www.cmc.sandia.gov/Nuc_Trans

[13] Korea Institute of Nuclear Safety, KINS, at http://iernet.kins.re.kr/cgi-bin/iernet and Korea Electric Power Company, KEPCO, http://www.kepco.co.kr/nuclear.html

[14] Japan Nuclear Cycle Development Institute (JNC) provides data from O-arai site at http://www.jnc.go.jp/zooarai/Oantai_j/html/map_jnc.html and Tokai site at http://www.jnc.go.jp/ztokai/kankyo/realtime/map_vllg.html and Tokyo Electric Power (TEPCO) has recently opened the data from Kashiwazaki-Kariwa at http://www.tepco.co.jp/kk-np/monitoring/mp002.html

[15] Los Alamos National Laboratory monitors around various DOE facilities in the western U.S. and posts the data at http://newnet.lanl.gov/

[16] Taiwan Atomic Energy Council's Radiation Monitoring Center (RMC) at http://www.trmc.aec.gov.tw

[17] To be carried out at the CMC by a visiting engineer from the JNC's O-arai site.

[18] Information available at http://www.iPIX.com

[19] John Brabson and Sharon Deland, "Knowledge Generation," presented at INMM/ESARDA 3rd Workshop on Science and Modern Technology for Safeguards, Tokyo, Nov. 13-16, 2000.