LA-UR-01-4547

Overview of an Unattended Monitoring System

August 8, 2001

by

James K. Halbig
Nonproliferation and International Security (NIS) Division,
Los Alamos National Laboratory

Overview of an Unattended Monitoring System

Contents

1.1. Introduction **1**

1.2. General Description **2**

1.3. System Hardware **6**

1.4. System Software **8**

1.5. Source Documents ..... Error! Bookmark not defined.

Overview of an Unattended Monitoring System

1.1. Introduction

An unattended-monitoring system continuously captures and records information in the absence of an inspector. The use of this system satisfies two major considerations. One is to allow an inspection agency to draw conclusions about the operation of a facility in the absence of an inspector, and the other is to minimize the impact of the inspection process on the facility. The continual presence of an inspector at the facility is a burden to both the inspection agency and the facility.

In the context of this report, an *unattended-monitoring system* has a collection of sensors and support electronics (instruments) that look at a positively identifying data set representing attributes of the object of the monitoring. A positively identifying data set is a characteristic that can be visualized, such as a strip chart of radiation count rate from a sensor, or the state of a door switch or seal. It can be generalized to a series of video images as well. These instruments have the capability of communicating among themselves so that one can alert others that the first has an indication of an event in progress and that the others should go into a higher state of alertness.

Data from the various instruments are collected at a central repository or focus. The repository, for purposes of this document, is the Radiation Collect Computer. This computer also provides the focus for state-of-health information on the instruments and on the Collect computers in the system.

Data are collected from the central repository and reviewed to check and verify the declarations made by a facility operator. The review can be as simple as examining graphical strip charts along with included video images and status of "physical protection"-type sensors up to identifying segments of data to be analyzed in depth with sophisticated analytical programs. The Review program can, for example, automatically detect events (peaks or edges on the strip charts) and from them determine the direction of motion of a target based on parameters set in the review program. The suite of Review software includes the capability to compare operator declarations against results found from the review and analysis of the data from the instruments.

Unattended assay systems are very similar to unattended monitoring systems except that they return data from which quantitative results can be determined during the review and analysis process. For example, an unattended monitoring system can sense a canister of plutonium, while the unattended assay system will also tell you the canister contains 50g of plutonium. Because the two types of monitoring systems are based on very similar sensors, electronics and review software, they can and have been easily combined into a hybrid unattended monitoring system, with the main difference occurring at the higher levels where analysis is done. The proposal in the body of this report does **NOT** include the use of unattended assay systems for the FMS.

A second-generation integrated monitoring system as implemented in Kazakhstan and Japan provides for the integration of elements that might otherwise be thought of an independent "layers" of safeguards. Such a system collects data from all the individual instruments. It

allows, at the lower level, some instruments (such as radiation monitors) to trigger other instruments (such as video cameras). It allows, at the higher level, review of the radiation data sets to determine what happened in the radiation dimension, while simultaneously allowing quick reference to other dimensions in order to resolve anomalies or further verify conclusions. While the system is designed to filter data (reduce the amount of statistically indistinguishable data returned to the central repository) a lot of data are collected and stored. When normal operation is verified using the radiation data sets, other data need not be reviewed. However, in anomalous circumstances or in the event of failure of some element, then other data may be reviewed. This concept gives one "defense in depth". However, unlike systems that are redundant (that duplicate hardware and functions), this system allows the use of instruments based on different technologies to provide data from which the same conclusions can be drawn as from the primary radiation-based sensors. This both provides the benefit of "redundant conclusions" and challenges an adversary to defeat more than one technology in order to subvert the system.

Unattended integrated monitoring has evolved from a secondary, tag-a-long technology compared to seals and video-based monitoring, to one that can be used as a primary system for monitoring the movement of radioactive materials, including special nuclear material. Such systems use radiation as the primary data set and incorporate additional technologies to provide data that supplements the primary data sets and provides fault-tolerance as opposed to redundancy.

Standard practices of containment and surveillance do not constrain the application of a system based on radiation monitoring, but neither are these practices totally ignored.

The main goal of the integrated monitoring system is to provide definitive, decisive, defendable results from which an inspector can draw conclusions about the operation of a facility. *Definitive* means that the data sets from the system clearly and un-ambiguously indicate what activities (of those it was designed to sense) took place in the area that is under safeguards. Definitive results are derived from a basis (e.g., physics) of the sensors that is appropriate for the required sensitivity. *Decisive* means that the definitive data leads to a clear, unquestionable conclusion about the activities in the area under safeguards. *Defendable* means the design and deployment of the sensors, the state-of-health of the instruments and the authenticity of the collected and reviewed data are such that the conclusions drawn from the data returned by the system cannot be discredited.

1.2. General Description

The integrated monitoring system uses distributed, autonomous instruments to monitor characteristic data sets at key points in the plant. The instruments operate full time and provide data to a central location on demand of a Collect computer. The autonomous instruments perform basic data acquisition functions, adapt to changing conditions, do low-level analysis to determine if an event of interest has been sensed, and minimize the amount of statistically indistinguishable data temporarily stored in the instrument and eventually

passed on for review. The basic architecture of an integrated monitoring system is shown in Figure A.

The strip chart (radiation) sensors are generally shown as the peripheral ovals (those furthest from the network). Sensor support electronics are shown as inner ovals. Instrument network nodes are shown as small circles between support electronics and the instrument-network loop. The three elements make up an instrument. Instruments are linked to each other and to the central Collect computer via an instrument network. An instruments gains access to the instrument network via the instrument network node. The instrument network provides for authenticated movement of triggers among the instruments, movement of data and commands (including triggering) among instruments and the Radiation Collect Computer and time synchronization of the strip chart instruments. Cases such as the GPS antenna involve a sensor attached directly to the hardware and intelligence of the instrument network node because a separate support electronics package is not required.

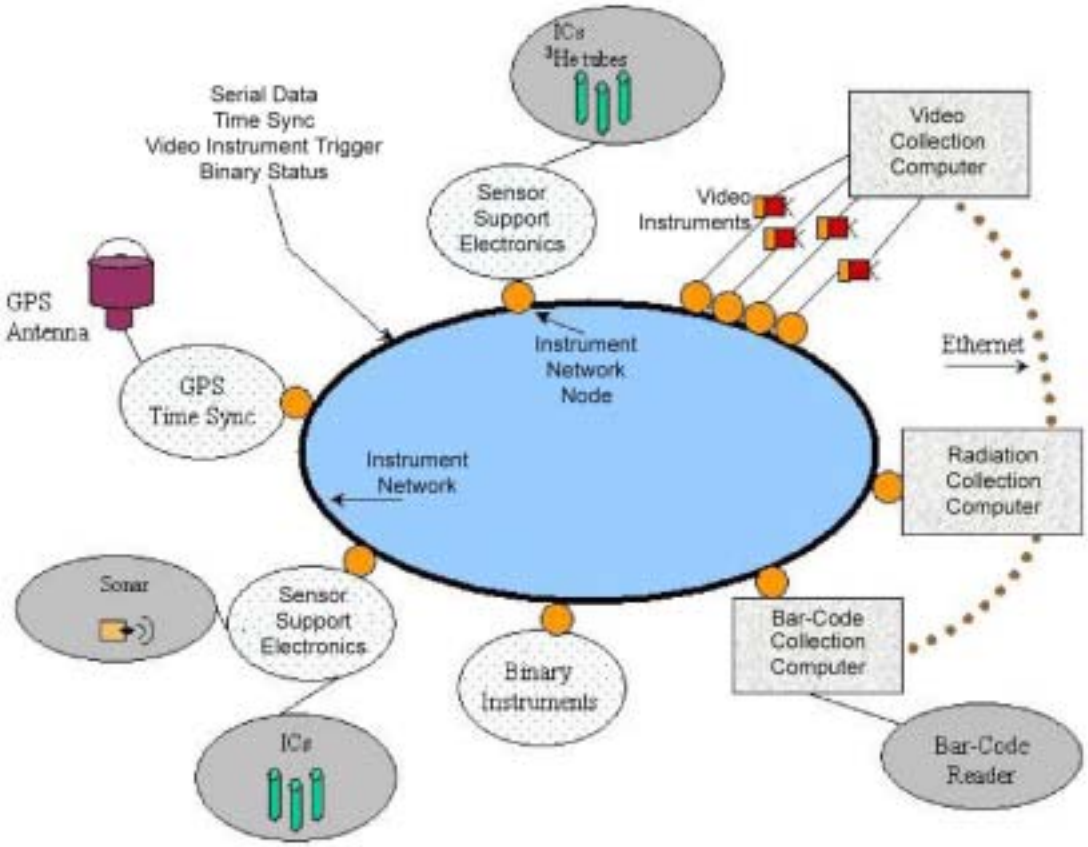

Fig. .A. Basic monitoring system architecture.

The video instrument is composed of the light sensors (cameras), the support electronics for the camera, and the instrument network node. Cameras connect directly to a video computer via a point-to-point RS-485 link for particular applications [7,8] in which the instrument

network connects to instrument network nodes in each individual camera. The Video Collect Computer connects to the Radiation Collect Computer via an Ethernet link. Because of the potentially large volume of video data, the Ethernet is used because of its higher bandwidth.

Instruments and the collect computers are, individually housed within a security boundary, with no unauthorized access allowed. The security boundaries for strip chart instruments are connected via a virtual secure conduit provided by the Instrument network protocol. The video data that is 12–15 kilobytes per frame in size is authenticated at the camera. Hence, the network cabling is not required to be secure.

The secure conduit is effected by the protocol implemented in the instrument network node that receives a serial data stream from sensor support electronics or a computer. One secure boundary encloses the sensor (or computer) and its instrument network node. The instrument network node wraps that data stream in a cocoon of network protocol that includes security. This cocoon of information is transmitted over unsecured wires that connect to other nodes on the instrument network. All the nodes reside within other security boundaries. A receiving node will break the cocoon open, and then, after having verified the authenticity of the cocoon, pass the serial data stream on to the intelligence to which the node is attached. The receiving intelligence is guaranteed, in this scenario, that the data are authentic with a specific, legitimate origin. The authentication shall provide two guarantees. (1.) The integrity of the data has not been purposely or accidentally compromised. (2.) The source of the data is assured. A third characteristic of authentication, the non-deniability of the transmission may not be of much importance here.

A very important function that the Instrument Network Node provides is the elimination of point-to-point wiring in favor of logical functions that are interfaced to the network node. The low-bandwidth requirement of the radiation instruments allows the Instrument Network Nodes to be connected in a free topology as opposed to the requirements of (10baseT and 100baseT) Ethernet. This means reduced wiring imposition on the facility and reduced wire and installation costs to the installer. The free topology can, in addition, be connected in a loop that provides the capability for uninterrupted communications even with a single cut in the loop.

The final computer in the unattended monitoring system is the Review Computer. The inspector uses the Review Computer to assemble and organize the data in order to allow conclusions to be drawn. The Review Computer can be interconnected with the central data repository for convenience if security allows. This is shown in Fig. B.

The software that runs on the Review Computer is basically a suite of programs that support an efficient and convenient graphical review of the data sets from the various sensors. The inspector can move between the various correlated data channels to determine what transpired during the period of unattended operation. The basic Review program has the capability to search for events and determine direction of motion of an item of interest. Analysis programs placed on top of the Review program may do more sophisticated review or analysis depending on the application and its needs.

Overview of an Unattended Monitoring System

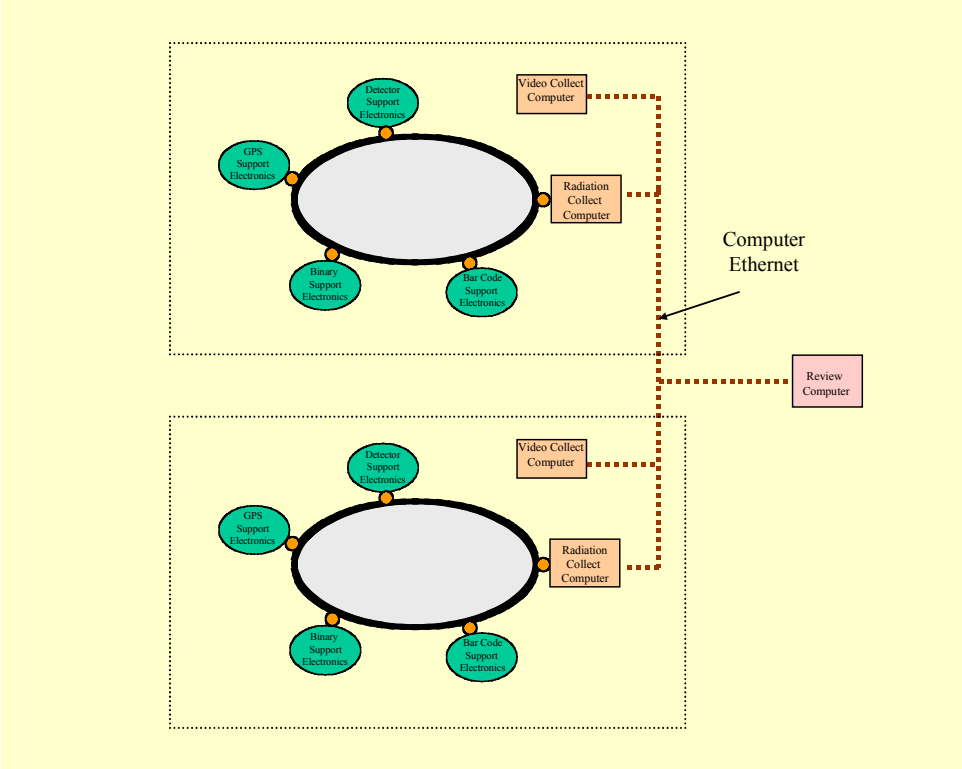

Fig. B. Connection of the Review computer to the Collect computers.

The architecture of the system allows "third-parties" to provide instruments and Collect and Review software modules that interface to the instruments by well-defined protocols. The video sensors are a good example of this. The cameras generate frames that are moved to the central archive computer. The basic video-review engine is provided by a third party. The engine was interfaced to the review suite by a simple program written for two different camera systems. [6]

Other instruments can easily be adapted for use in this system. A sonar device, for example, was obtained with a frequency output (output frequency is proportional to echo time). This allowed the data from the sonar to be input in a general pulse-counting channel. Data treatment, transfer and review were provided by existing capabilities of the system in this case.

Little has been said so far about the firmware and software of the system. The firmware, software stored in non-volatile memory, controls the operation of the autonomous instruments. It is key to the robust, effective operation of the instruments. Software runs in the computers that have higher level operating systems. The software provides control of the off-load and subsequent treatment, storage, and further movement of data. It also provides the user interface to the review and analysis software.

The hardware and software have been designed as an ensemble. The ensemble is modular and orthogonal. Modular is well understood, orthogonal means that the specification of the interface of the modules is very well defined, and defined in such a way that the removal, addition or replacement of one module does not cause changes in another module. This allows the ensemble to be effectively expanded or contracted, but it shall be done with understanding and forethought.

1.3. System Hardware

The radiation detectors are generally uniquely designed for a specific facility to measure a specific attribute with a required sensitivity and precision and/or accuracy. They are the eyes of the radiation portion of the monitoring system. The detectors and their implementation shall be such that an adversary cannot successfully shield the sources of interest from the detectors. There are two parts to this statement. The system will be *defeated* if a source can be moved past a detection point with no indication of foul play, because an object of monitoring was moved with no sense of anomaly. The system is said to have been *blinded* but not defeated if a source is moved past a detection point without being directly sensed, but a change in the "environment" of the detector that may indicate foul play was sensed. The difference in the two conditions is that when one channel of the system is blinded, there are alternatives, such as other sensor channels, to resolve the anomaly.

The sensor support electronics provide logistical support for the basic sensor. The sensor support electronics provides bias, power for preamps, etc., for a radiation instrument. Signals sent to the support electronics are processed. and raw data are stored locally and may be transmitted to the central archive. The support electronics along with the detector acquire the safeguards-significant data. The support electronics in our architecture shall be autonomous. That is, they along with the detector shall have all the resources required to take and store data in a stand-alone mode. This autonomy demands three capabilities of the radiation instruments. One is built-in intelligence (microprocessor plus associated firmware) to analyze raw data that can 1. indicate an event of interest, 2. send out triggers or alarms if signals exceed a preset threshold so that the instrument can "adapt" to changing signal conditions, and 3. filter data to minimize the storage of statistically indistinguishable data. Data storage is the second capability required of the autonomous radiation instruments. This is so the data can be preserved under adversarial conditions until the inspector can retrieve the data at the next inspection. The final capability is a local energy source that will power the unit under similar adverse conditions or possibly innocently caused power outages until power can be re-established.

A potential security problem exists with the connection of the detectors to their support electronics. A scenario to defeat the system would be to disconnect the cable(s) between the detector and the support electronics and to inject a signal into the support electronics from a separate detector or from a signal simulator. While the support electronics are receiving this counterfeit signal, material may be moved past the orphaned detector. This problem can be met in several ways. Other sensors without this vulnerability can be used to cover the same path. Tamper-indicating conduit may be used to protect the wires that connect the detector to its support electronics. Cables may be short and continuously visible to a camera. The

detector and the support electronics may be enclosed in the same security boundary in some cases. An example of a security boundary could be a sealed, tamper-indicating metal enclosure containing the detector, support electronics and wires that interconnect the two.

The data-collection computer can take on different levels of complexity depending on the requirements of a specific application. A simple example is that the various remote instruments may not transfer their data at all, but instead someone may, at the end of an inspection period, manually store the data on a removable memory card. A network may still be required if triggering is needed, even though data and commands from the Collect computer are not moved over the network. A very high-reliability system as shown in Fig. C may be used in the other extreme.

Figure C shows two identical computers and associated interfaces. Each computer is the clone of the other, but one computer is in cold standby. One computer is called the master, the other the backup. The watchdog function in the instrument network node labeled watchdog w/lon monitors traffic over the instrument network. The watchdog will power down the master collect computer, wait for a short time and then re-power the master collect computer if the traffic indicates a failure in the master computer or its associated instrument network node. The watchdog listens again, after a delay, for communications on the instrument network. The recovery task is completed if traffic is normal. The watchdog will again power down the master collect computer and then immediately power up the backup collect computer if the communications are still not normal. The system should operate normally when the backup collect computer comes up. Actual data are not stored on the disks of any one computer, but are stored instead on a Redundant Array of Independent Disks, which is a very reliable configuration of multiple disks that survives the failure of one of the array disks. Survival means that the data can still be stored to and retrieved from the array even with one failed disk

Another feature of this scheme is that the uninterruptible power supply (UPS) for the Collect computer can be powered down and reawakened for prolonged survival on the limited amount of energy stored in its batteries. The information on a power outage that is sensed by the UPS is obtained by the active collect computer. The collect computer off-loads all the data from the instruments (this is the normal state) and then commands the UPS to power down for an amount of time comfortably less than the time required for the weakest instrument to fill up its resident storage. The collect computer then puts itself in a safe state for the power to go down. When the UPS powers back up the computer re-boots, determines that the mains power is still down, off-loads all the data from the remote instruments, and repeats the power-down sequence. The off-load time is on the order of tens of minutes while the fill time of the resident memory in the remote instruments is on the order of hours. Hence the advantage of a significant survival time is realized.

Overview of an Unattended Monitoring System

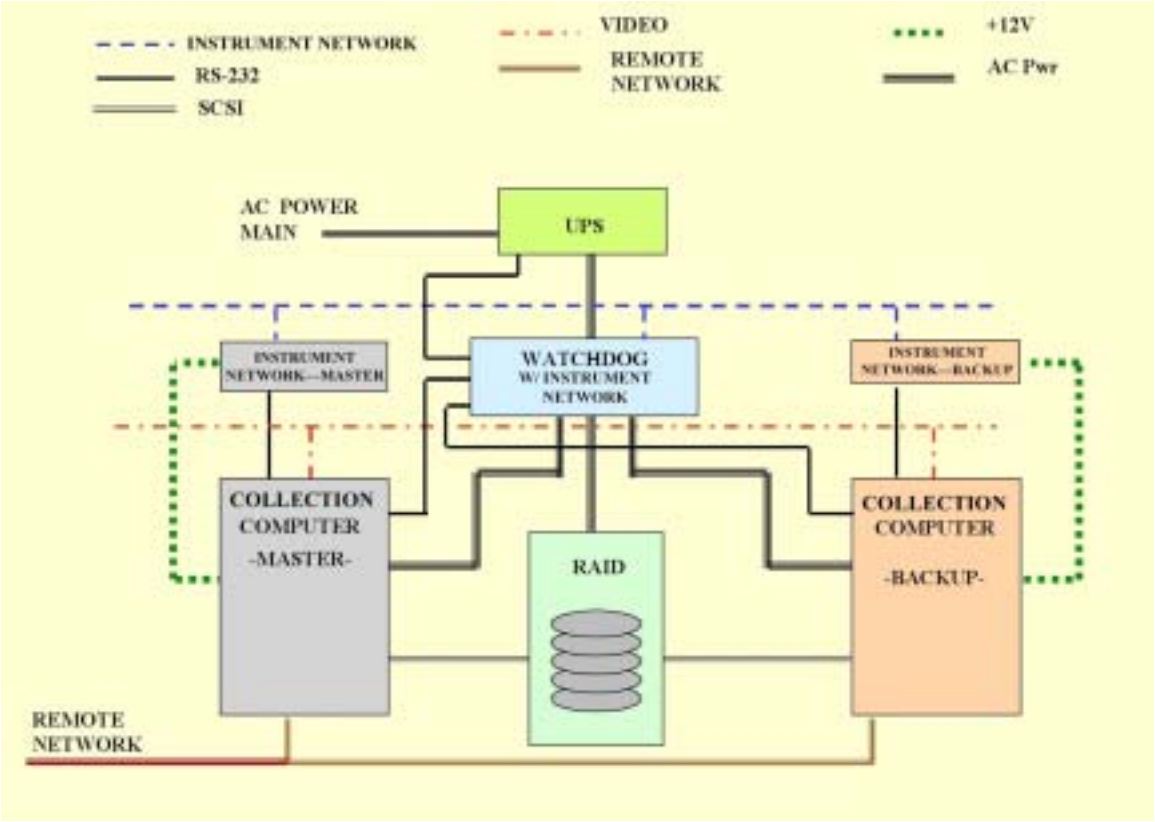

Fig. C. A highly reliable data collection scheme.

1.4. System Software

The software for the unattended monitoring system includes the software contained in the sensor support electronics, the instrument network nodes, the sensor Collect computers and the Review computer.

The system operates unattended most of the time, covering the periods in which the inspector is not present at the facility. Data acquisition is continuous under the autonomous operation of the sensor-support electronics located near the sensors. Data accumulated in the sensor support electronics are offloaded to a sensor Collect computer every few minutes. The sensor-support-electronics software automates the continuous acquisition and temporary storage of data and the dumping of data to the sensor collect computer upon command. It may also automate the elimination of statistically insignificant data. The instrument network node software moves commands, data responses, triggers, time synchronization, and other information among the instrument network nodes. It may also provide binary data input and output. The sensor Collect computer software off-loads the data from the sensor support electronics, organizes and stores the data, displays the status of the sensor subsystem and may provide capabilities to copy data to removable media.

When the inspector is present, data collected in unattended mode need to be reviewed to draw the inspection conclusions. The review computer software retrieves the data from the central repository, organizes the data from several sensor subsystems and provides appropriate displays and analysis so that the inspection conclusions can be drawn.

1.5. Source Documents

[1] J. K. Halbig, S. F. Klosterbuer, R. H. Auguston, G. E. Bosler, H. O. Menlove and M. C. Miller, "Applications for Unattended, Remote NDA Instrumentation," in Conference Record of the 1991 IEEE Nuclear Science Symposium, Catalog #91CH3100-5, Vol. II, (1991) pp. 1246–1253.

[2] S. F. Klosterbuer, J. K. Halbig, W. C. Harker, H. O. Menlove, J. A. Painter, and J. E. Stewart, "Continuous Remote Unattended Monitoring for Safeguards Data Collection Systems," 1994 IAEA Symposium on International Safeguards, Los Alamos National Laboratory document LA-UR-94-256 (1994).

[3] J. K. Halbig, K. E. Gainer, and S. F. Klosterbuer, "An Efficient Network for Interconnecting Remote Monitoring Instruments and Computers," *Nucl. Mater. Manage*., XXIII (Proc. Issue 1994).

[4] P. Staples, J. Audia, Y. Bai, M. Briggs, J. K. Halbig, and K. D. Ianakiev, "Evaluation of NaI(TL) and Plastic Scintillators for use in Remote, Unattended, and Portal Monitoring," *Nucl. Mater. Manage*., XXVII, CD ROM (Proc. Issue 1998).

[5] R. F. Parker, J. K. Halbig, S. F. Klosterbuer, M. E. Abhold, J. M. Audia, Y. Bai, S. C. Bourett, W. J. Hansen, K. D. Ianakiev, and M. R. Sweet, "Integrated Monitoring Hardware Developments at Los Alamos," to be published in the proceedings for ESARDA, 21st Annual Meeting, Sevilla, Spain, 1999, Los Alamos National Laboratory document LA-UR-99-2053 (1999).

[6] S. F. Klosterbuer, S. E. Buck, D. G. Pelowitz, R. F. Parker, W. C. Harker, J. K. Halbig, M. E. Abhold, "Integrated Monitoring Software Developments at Los Alamos," to be published in the proceedings for ESARDA, 21st Annual Meeting, Sevilla, Spain, 1999, Los Alamos National Laboratory document LA-UR-99-1987 (1999).

[7] Y. Yokota, M. Ishikawa, Y. Matsuda, T. Tsujino, M. E. Abhold, S. E. Buck, J. K. Halbig, K. Ianakiev, S. F. Klosterbuer, and T. Marks, "Integrated Monitoring and Reviewing Systems for the Rokkasho Spent Fuel Receipt and Storage Facility*," Nucl. Mater. Manage*. XXVII CD ROM (Proc. Issue), 825–833 (1998).

[8] J. K. Halbig, S. F. Klosterbuer, R. F. Parker, M. E. Abhold, J. M. Audia, Y. Bai, S. C. Bourret, S. E. Buck, W. J. Hansen, K. D. Ianakiev, H. O. Menlove, D. G Pelowitz, and M. R. Sweet, "Integrated Monitoring System—An Overview," to be published for

ESARDA 21st Annual Meeting, Sevilla, Spain, 1999, Los Alamos National Laboratory document LA-UR-99-2109 (1999).

[9] R. Parker, "Intelligent Local Node (ILON) User Manual," UM-ILON-002.102, Safeguards Science and Technology Group, Los Alamos National Laboratory document LA-UR-99-1857 (February 25, 1999).

[10] David Pelowitz, "Multi-Instrument Collect Users Manual," Los Alamos National Laboratory document LA-UR-99-4267 (January 2000).

[11] S. F. Klosterbuer, "Radiation Review User Manual," Los Alamos National Laboratory document LA-UR-99-1655, (February 1999).

[12] Steven E. Buck, Mark E. Abhold, and Shirley Klosterbuer, "Operator Review User Manual, Version 1.31," Los Alamos National Laboratory document LA-UR-99-2205 (May 1999).

[13] Steven E. Buck, Mark E. Abhold, and Shirley Klosterbuer, "TLR Review User Manual," Los Alamos National Laboratory document LA-UR-99-2203 (January 2000).

[14] Steven E. Buck, "Digital Video Review User Manual," to be published by Los Alamos National Laboratory document LA-UR-99-2206 (January 2000).

[15] Steven E. Buck, Mark E. Abhold, and Shirley Klosterbuer, "Integrated Review User Manual," Los Alamos National Laboratory document LA-UR-99-1290 (February 1999).

[16] J. K. Halbig, Y. Bai, K. D. Ianakiev, R. F. Parker, P. S. Reass, L. G. Wiig, S. F. Klosterbuer, and P. S. Hewitt, "MiniGRAND Developments At Los Alamos," *Nucl. Mater. Manage.* **XXVIII**, CD-ROM (1999), LA-UR-99-3976 (1999).

[17] James K. Halbig, Shirley F. Klosterbuer, Robert F. Parker, Jeffry M. Audia, Ying Bai, Steve E. Buck, Kiril D. Ianakiev and David G. Pelowitz, J. S. Kraus, R. M. White, W. Spahn, "Integrating Surveillance and Radiation Detection Technologies", Los Alamos National Laboratory document LA-UR-99-3871, presented at INNM 40th Annual Meeting (July 1999).

[18] Robert Parker, "MiniGRAND User Manual," Los Alamos National Laboratory document LA-UR-99-4400 (October 2000).