LA-UR- 96-2616

Title: A SYSTEMS APPROACH TO NUCLEAR FACILITY MONITORING

CONF-960767--57

RECEIVED
SEP 0 9 1996
OSTI

Author(s): Paul E. Argo, Justin E. Doak, and James W. Howse

Submitted to: 37th Annual Meeting of the Institute of Nuclear Materials Management, July 28-31, 1996, Naples, Florida

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

MASTER

Los Alamos
NATIONAL LABORATORY

A Systems Approach to Nuclear Facility Monitoring*

Paul E. Argo, Justin E. Doak, and James W. Howse
Los Alamos National Laboratory
Los Alamos, New Mexico 87545 USA

Abstract

Sensor technology for use in nuclear facility monitoring has reached an advanced stage of development. Research on where to place these sensors in a facility and how to combine their outputs in a meaningful fashion does not appear to be keeping pace. (We note that this phenomenon is similar to the computing field where advances in hardware technology tend to be several years ahead of similar advances in software engineering.) In this paper, we take a global view of the problem where sensor technology is viewed as only one piece of a large puzzle. Other pieces of this puzzle include the optimal location and type of sensors used in a specific facility, the rate at which sensors record information, and the risk associated with the materials/processes at a facility. If the data are analyzed off-site, how will they be transmitted? Is real-time analysis necessary? Are we monitoring only the facility itself, or might we also monitor the processing that occurs there (e.g., tank levels and concentrations)? How are we going to combine the outputs from the various sensors to give us an accurate picture of the state of the facility?

This paper will not try to answer all these questions, but rather it will attempt to stimulate thought in this area by formulating a systems approach to the problem demonstrated by a prototype system and a system proposed for an actual facility. Our focus will be on the data analysis aspect of the problem. Future work in this area should focus on recommendations and guidelines for a monitoring system based upon the type of facility and processing that occurs there.

I. Facility Monitoring

We define facility monitoring as the detection of unauthorized or anomalous events in and around a safe guarded facility that may indicate an attempt to illegally acquire material or to use a facility for something other than its stated purpose. We want to accomplish this using as little manpower as possible; therefore, we will utilize available sensor technology, remote data communications, and automated data analysis.

We also view facility monitoring as a staged effort that begins with physical protection. This stage is the cornerstone of safeguards at any facility and can never be replaced. (We can, however, imagine the reduction of security forces with the addition of unattended monitoring.) The next stage uses systems to continuously record information about the activities in a facility. An example of this kind of system is in use at the JOYO and MONJU prototype fast breeder reactors in Japan where radiation sensors monitor the movement of fuel bundles at the fresh-fuel input, the reactor core, and underwater spent fuel storage.[1] Periodically, IAEA inspectors visit these facilities and scan the recorded information (possibly aided by computer tools) to ensure no diversion of materials or undeclared use since the last inspection. We are now in the realm of unattended monitoring, but no automated analysis is taking place. This brings us to the stage which is *to detect obvious anomalies or breaches of security*. An example of a tool that can provide some of this functionality is an image processing system that detects motion in critical areas of a vault. Certainly, this stage adds value, but it is not sufficient to cover scenarios involving *insider threat* (i.e., potentially malevolent acts by individuals with authorized access to sensitive materials or processes.) The real challenge is distinguishing between authorized and potentially unauthorized activities when an individual's actions may not be illegal but are certainly *anomalous*. This paper will focus on the detection of anomalous activities.

---

*This work supported by the US Department of Energy, Office of Research and Development.

II. The Next Generation

The next-generation nuclear facility monitoring system will not only be able to deal with varying background levels of radiation, but will also be able to identify the type of nuclear material being carried (characterization) and who the person is carrying the material (face recognition, smart badges, etc.). The monitoring system will be able to use this data to determine each individual's patterns of activity and will immediately recognize activities that differ from that pattern. The information from materials accounting systems (which will include transaction authorization tables) will be linked into the monitoring system, so that deviations from a scheduled special nuclear materials (SNM) movement can be detected and challenged by the physical protection team if deemed serious.

As the database from the set of sensors in the facility grows, modern techniques designed to enhance the "discovery of knowledge" from the database will be implemented. The purpose will be to establish patterns in the data that characterize acceptable activity within the facility and to be able to set up an anomaly recognition program that can detect variances from that activity. Knowledge discovery will be a continuing, ongoing process that is able to follow the changes in facility operation.

An Example

Jack approaches a vault containing SNM to which he has authorized access. He swipes his badge through a reader; then a face recognition system correctly verifies that this is indeed Jack. Much to Jack's surprise, the door to the vault remains locked; the facility monitoring system has determined that it is highly unusual for Jack to be accessing the vault at this time. (It is 5:30 p.m. on Friday and Jack stays this late at work on Fridays less than 1% of the time.) A guard is notified of the situation and arrives to question Jack as to why he is trying to gain access to the vault. Jack explains that he is working on an urgent DOE request for an inventory of the facility's SNM and has had to work late to finish the task. The guard is aware of this request and provides access to the vault.

III. Systems Approach

Facility monitoring is a problem that will not be solved by simply installing the latest sensor technology in a facility. Careful, logical decisions need to be made that consider numerous factors.

1. What is the type of facility?
   The type of facility that is monitored should be a large factor in the kinds of sensors installed, their locations, and the rate at which information is recorded. For example, a nuclear reactor will certainly require different sensors than a waste storage facility. We foresee the need for guidelines, organized by facility type, that help system implementors make smart choices for sensor types and locations.

2. Process Monitoring
   The kind of processing that occurs in a facility will also have a strong influence on the location and type of sensors chosen. For example, assume that we have two reprocessing facilities; one facility takes the spent fuel from a reactor and converts it for use in another type of reactor, and the other takes the same spent fuel and extracts ^{239}Pu for weapons use. Although both facilities are reprocessing facilities, the processing that occurs is significantly different and requires different monitoring.

3. Risk Analysis
   It is important to understand the level of risk associated with a particular facility and the processing that occurs there. What are the consequences if some of the safeguarded materials are diverted or a facility is used in some fashion to assist in the development of weapons? Certainly, a facility with a vault containing plutonium pits from disassembled weapons is a very attractive target. On the other hand, a research reactor may not need as high a level of safeguards. Any automated techniques used to analyze data from a facility should account for high levels of risk by severely penalizing false positives when determining algorithm effectiveness.

4. Financial Considerations
   How much money is available to safeguard the facility? Certainly, this will influence what can be done. The idea is to prioritize and apply the most critical and effective safeguards first, and then do as much of the rest as finances allow. Unattended monitoring can reduce the requirement for expensive physical protection, thereby decreasing cost while maintaining a certain level of safeguards.

5. Data Analysis
Once we have determined the type of facility, the processes that go on there, the level of risk, and the amount of money available, we are in a position to install sensors and start recording data. We then have to determine what to do with it. The next section will discuss this very complex data analysis problem and present our approach

IV. Data Analysis

The general framework from which we approach data analysis segments the process into four primary stages: data gathering, information preparation, analysis, and presentation of results. An ongoing effort at Los Alamos National Laboratory[2] focuses on the development of tools to help system designers make intelligent decisions concerning the processing of their application-specific data.

A. Data Gathering

The first of these stages, data gathering, sounds trivial but is often the most time-consuming of all. The data is frequently not directly accessible on-line and may be in a format that is not compatible with the systems performing the analysis. Organizations (or different factions within the same organization) may hesitate to provide the necessary data because of its sensitivity or classification. These kinds of problems are usually unavoidable and sufficient time needs to be budgeted for data gathering.

B. Information Preparation

The preparation of information is a critical component of all analysis systems. The ability to manage and effectively transform raw data into meaningful features is a prerequisite for analysis by any methodology, regardless of the problem domain. The situation is further complicated when the data is in disparate formats; in facility monitoring, we are dealing with, for example, images from video cameras, numerical readings from detectors (e.g., a neutron detector), and character data (e.g., the name of an operator who entered a record in a materials accounting database). Information preparation must take all the data and process it into a form that is ideal for the candidate analysis methodology.

Here is a list of some of the major components of information preparation.

- *Parsing*: Each source of data must be separated into syntactic units (tokens) so that they can be accessed using an appropriately named variable. The parser must be able to handle virtually any type of data.
- *Rationalization*: Obvious data errors need to be eliminated (e.g., sensor readings that exceed the maximum range given in the sensor's manual), and missing data must be properly treated.
- *Fusion*: Because we are required to handle multiple sensors simultaneously, we must be able to merge the data to obtain information that can only be derived from several data sources. To do so, differences in labeling must be resolved and related variables from different sources combined to avoid redundancy.
- *Feature Extraction*: Even after the raw data has undergone the processing mentioned above, the resulting features may not be useful to the analysis component of the system. As a result, other features may need to be derived by various transformations of existing features. Examples include computing the average rate of flow of a material given readings collected at regular intervals, summarizing material movements made over an entire shift, and standardizing continuous features to unit variance by dividing all the values for that feature by its standard deviation.
- *Value Clustering*: If a feature has a large range (for continuous features) or domain size (for categorical features), we may wish to cluster its values into bins to produce a smaller number of possible values. For example, the feature "time-of-day" when reported in hh:mm:ss using a 24-hour clock has 24*60*60 unique values. Some statistical techniques will not work well with a feature having such a large range. We would perform clustering on the values of this numeric feature to convert it to a categorical feature with a small domain size.
- *Feature Statistics*: Statistics of features, such as the mean, variance, standard deviation, correlation, and covariance, can provide an analyst with useful insights into the nature of the data and help determine an effective approach to analysis. Feature statistics may also be a part of feature extraction because the statistics can be used to create new features (e.g., centering the values for a continuous feature around the mean).

- *Feature Selection*: Feature selection is a method of experimentally determining the most effective subset(s) of an initial set of features. We define an effective feature subset to be one that is not only small, in that it contains only a small fraction of the features present in the initial set, but also highly predictive. If the feature subset is small, the time it takes to train an analyzer and classify examples is decreased. If the feature subset is highly predictive, the analyzer may do a better job at recognizing the appropriate classes for new examples, resulting in a lower error rate.

  Feature extraction and feature selection do not necessarily occur sequentially. That is, we may go back to feature extraction and construct new features that necessitate performing feature selection again, and so forth.

- *Prioritization*: Some features can be of more relevance than others. For this reason, we need the capability of assigning some features a higher priority than others.

C. Analysis

Information preparation, if done carefully, can provide us with useful information to analyze. However, before doing any kind of analysis and choosing a specific analysis technique, a decision needs to be made as to how the data from the various sensors is to be analyzed. We present below three possible options for analyzing sensor data, although specific facilities will likely require variations not considered here.

- Multiple Time-Series Data

  The output of each sensor can be viewed as a time-dependent sequence of data. Some fusion of the results after analysis of each time series individually may need to occur. Examples include the autoregressive, integrated moving average (ARIMA) model and curve smoothers.

- Vector-Based Data

  One can create transactions by taking snapshots of all the sensors at specific time intervals. It is likely that not all the sensors will record information at the same time intervals. For example, if Sensor 1 records information every two seconds and Sensor 2 records information every half second, we may want to sum the information from Sensor 2 so that the information in the transactions represents the same two-second interval. Another consideration is dealing with data in formats, such as video data (images), that does not lend itself to representation as a feature in vector-based data. One solution that has been employed is to do some preprocessing of these types of data to transform them into features. For example, we can calculate the pixel difference from frame to frame for a video camera and create a feature that can be used in a vector-based format. Examples include machine learning algorithms (e.g., nearest neighbor), expert systems, and discriminant analysis.

- Alarm-Based Data

  Some sensors can act as alarms that trigger further analysis using data from other sensors. One example is a door to a vault that opens, triggering the recording of images by a video camera.

D. Presentation of Results

The communication of intermediate and final results to appropriate individuals (most often physical protection personnel) is an invaluable aspect of a facility monitoring system. A guard will want to be immediately notified of any unusual activity; he may want to know the status of a material transfer; and he may want a recommendation of appropriate action in response to an unauthorized activity. For this type of application, some type of immediate notification, such as dialing the pagers of a couple of on-duty guards, is certainly required.

V. EVTRAP

The Enhanced VTRAP (Video and Time Radiation Analysis Program) demonstration* used four neutron detectors and a video camera to monitor the movement of a nuclear source in an enclosed room. (The pixel difference between successive images from the video camera was calculated to convert the video imagery into a vector-based data format.) Although the radiation detectors were set in positions for historical reasons (rather than optimized for monitoring the room), we found that we could simply train a classifier (neural network) to use the radiation and video signals to determine where in the room the source was and which way it was moving. By using each of the 26 locations and directions as "letters," we could derive "words" describing longer sequences of positions. Concatenating similar letters allowed us to be insensitive to the speed of

---

*EVTRAP is a direct follow-on to VTRAP.[3] The primary enhancement is the addition of real-time analysis.

the motion. The words were then examined by a simple rule-based system to differentiate between legal and illegal activities.

VI. Los Alamos National Laboratory Technical Area 18

The Los Alamos Criticality Experiments Facility (TA-18) is a prime example of a completely "attended" monitoring situation. Category I levels of SNM are moved regularly inside the facility, and with each movement one or more armed guards are with the material at all times. This has proven to be not only disruptive to the work at the facility but also extremely expensive. We are preparing a demonstration facility monitoring system with the long-term goal of "moving the guards back to the perimeter fences." In order to achieve this goal, we must show that we can monitor and "protect" the movement of the SNM at least as well as the guard does. We will do this with several types of monitoring systems that interact with each other and share data with an analysis program that can detect illegal activities, warn the guards, and inform guards what has happened.

We are working on a modified version of the material accounting system called LANMAS (Local Area Network Material Accounting System).[4] This system will use bar-code readers to identify the SNM sources being handled and biometric systems (initially the Laboratory standard badge/palm reader) to determine (and verify) the identity of the person doing the movement. In addition, there will be an authorization portion of the accounting system that will keep track of all upcoming materials movements within the facility. As material is actually moved, the movement can be checked against this authorization table.

The movement of SNM will be monitored by radiation sensors, movement detection systems, and biometric systems for identifying the participating individuals. Portal radiation monitors at the entrances to storage vaults and safes will detect passage of any SNM into or out of the vaults/safes. Movement detection systems (e.g., video and infra-red) will detect any activity at the entrances to vaults and safes, and passive biometric systems (e.g., face recognition) will identify the personnel. Access to the vaults and safes will be through badge readers and biometric verification systems (e.g., palm reader, fingerprint scanner, speaker verification, and iris scanner), and before doors are unlocked the authorization table will be checked. Sources will be scanned, initially by bar-code readers, but eventually by "smart" radiation detectors that will check the source characteristics against stored information for validation. Once the SNM is outside the vault, an array of radiation and movement sensors (e.g., EVTRAP) will be used to follow and characterize the movement of the material. Again, this will be constantly checked against the movement authorization tables, and alarms sounded if the movement doesn't match that expected. The check-in of the SNM to its destination will happen in a similar manner.

These monitoring and authorization systems will work together to monitor the activity inside TA-18 that is connected to the movement of SNM; this information will be relayed to the security/protection force. Video images of regions where SNM is being handled will be routed to monitors, and annotated logs of activities (and expected activities) will be available for immediate perusal.

A large database of SNM movement will be generated by this system. The advanced facility monitoring part of the project will be the design and implementation of tools to examine and characterize the activities contained in this database. The bottom line is that we are attempting to design a system that will allow us to detect that "once-in-a-lifetime" attempt by an insider to move nuclear material out of the facility or to an area of the facility more susceptible to external attack

VII. Summary

Unattended facility monitoring can provide many benefits, including cost reduction and enhanced safeguards. The next-generation facility monitoring system (a mixture of modern sensor technology and advanced data analysis techniques) may even be able to detect insider sabotage through anomalous activity. To assist designers of such monitoring systems, we feel that there should be some general recommendations guiding the choice of sensors and their locations for the specific characteristics of a facility. Designers also need to consider how the data from sensors will be processed, especially during information preparation and analysis, to most accurately predict the state of the facility. Some of our ideas for facility monitoring were demonstrated with the EVTRAP activity; the Los Alamos Critical Experiments Facility will give us our first opportunity to test these concepts in an actual facility.

References

1. S. F. Klosterbuer, et al., "Continuous Remote Unattended Monitoring for Safeguards Data Collection Systems," in Proceedings of the IAEA Symposium on International Safeguards 1994: Vision for the Future, IAEA, Vienna, Austria, 1994.

2. Justin Doak, Joan Prommel, and Barbara Hoffbauer, "STAR: Software Toolkit for Analysis Research," *Nucl. Mater. Manage.*t **XXIV**, 1106-1109 (1995).

3. J. A. Howell, H. O. Menlove, C. A. Rodriguez, D. Beddingfield, and A. Vasil, "Analysis of Integrated Video and Radiation Data," *Nucl. Mater. Manage.* **XXIV**, 162-167 (1995).

4. Bruce Erkkila, Mike Boor, Rena Whiteson, Jenny Smith, Jo Ann Painter, and Joe Claborn, "LANMAS: a New Generation Computerized MC&A System for the DOE Complex," *Nucl. Mater. Manage.* **XXV** (1996).