TRUST
TAMPER-RESISTANT UNATTENDED SAFEGUARDS TECHNIQUES

A Joint Canada/USA Progress Report

Sponsored by the
US Arms Control and Disarmament Agency (RA68-130)
and by the
Atomic Energy Control Board of Canada

J. G. McManus
Associate Scientific Adviser
Atomic Energy Control Board
Ottawa, Canada

A. V. Engel, Jr.
Advanced Systems Development
Sandia Corporation
Albuquerque, New Mexico
ABSTRACT

TRUST is a joint Canada/USA safeguards research and development project. The objectives of this project are to develop and evaluate prototype instrumentation, unattended and secure, which is applicable to the safeguarding of power reactors and other nuclear facilities and to test tamper-resistant techniques and devices in an operating power reactor. The Nuclear Power Demonstration reactor at Rolphoton in Canada has been selected as the site for the field test of the developed instruments and techniques.

The design guidelines and preliminary design considerations of the project are described briefly. The instruments designed for installation at the NPD reactor and methods for their interconnection and operation are described. The generation of information is described, and its flow is traced from sensors, along transmission paths, and to storage and recovery modules until the information is available for use by a safeguards inspector.

The techniques developed to protect instruments and recording stations are described. For small volumes of the order of 1 cubic foot, especially prepared glass containers which will indicate unauthorized entry or influence are used. A large volume, of the order of 600 cubic feet, containing the central recording station is protected by a radio frequency monitor which detects unauthorized entry. Flow of information along unprotected transmission lines between secure containers is protected by simple yet effective coding techniques.

Finally, the test results available at the date of publication of the report will be discussed briefly.
INTRODUCTION

The preamble to the Treaty on the Non-Proliferation of Nuclear Weapons expresses, on the part of the States concluding the Treaty, "their support for research, development and other efforts to further the application, within the framework of the International Atomic Energy Agency safeguards system, of the principle of safeguarding effectively the flow of source and special fissionable materials by use of instruments and other techniques at certain strategic points." In the summer of 1968, it became apparent to authorities involved in safeguards in the United States of America and Canada that a cooperative safeguards development program might be of mutual benefit to the two governments, support the principles of the NPT, and assist the IAEA in carrying out its increased responsibilities under the NPT. After several general discussions between officials of both governments had confirmed a mutual interest, the two parties agreed to join in an effort "to design, build, install, and test on a CANDU-type power reactor, the prototype of an unattended tamper-resistant/tamper-indicating safeguards instrumentation system." The cooperating agencies in the two governments are the United States Atomic Energy Commission, the United States Arms Control and Disarmament Agency, Atomic Energy of Canada Limited, and the Atomic Energy Control Board of Canada.

The experiment will be conducted at the Nuclear Power Demonstration reactor at Rolphton in Canada. This is an on-power-fuelled reactor moderated by heavy water and cooled by boiling heavy water. The on-power-fuelling, the high plutonium production capability, and the fact that it is operated by a public utility, the Ontario Hydro Electric Power Commission, make this an excellent test facility for this project.

The experiment is under the direction of a Working Group composed of members of the contributing agencies and contractors. This paper is a brief outline of the design of the system and the safeguards philosophy developed by the working group.

OBJECTIVES

The objectives of the program are:

1. To develop and evaluate prototype instrumentation (unattended and secure) which may be applicable to the safeguarding of power reactors and other nuclear facilities.
2. To test tamper-resistant/tamper-indicating techniques and devices in the severe environment of an operating power reactor.

These objectives have been kept clearly in mind by the Working Group. The system as it is now designed is tailored to the NPD reactor. The Working Group does feel, however, that many of the devices and most of the techniques developed and tested in this program will be directly applicable to other reactor types, other nuclear facilities, and even to other disarmament projects outside the field of atomic energy.

In order to promote the wide use of information developed, all parties have agreed to make the results of this project available to the International Atomic Energy Agency. The Director-General of the IAEA has expressed great interest in the project, and Agency observers have already attended Working Group meetings. The Working Group will provide the cooperating agencies and the IAEA with sufficient information that they can make reasoned decisions on the use of developed equipment.
The Working Group will develop inspection procedures which optimize the allocation of manpower and money available to a safeguards agency. In preparing these procedures and in carrying out the test program, the Working Group will bear in mind the need to maximize the effectiveness of the system and to demonstrate its credibility.

DESIGN GUIDELINES

The following design guidelines were laid down by the Working Group:

1. The system must not interfere with the normal operation of the reactor.

2. The system must not impose an unacceptable burden on the facility operator.

3. The system must be so designed that the integrity of the independent safeguards data is maintained, although all design and operational details of the instruments are given to the operator.

Guidelines 1 and 2, above, are completely in accord with safeguards principles laid down from the very beginning of the safeguards discipline; everyone will probably agree on their desirability and necessity.

The necessity for Guideline 3 arises from two considerations. It is the policy of the IAEA that the design details of all instrumentation be revealed to all participating governments. The system must be acceptable to the operator. The consent of the operator who is responsible for the safe and economic operation of the station must be obtained before any reactor instrumentation can be installed. The only way such consent would be obtained from a conscientious operator would be in a circumstance where all the design and operation details were made available to him, and if they involved, in his estimation, no risk to the station.

GOALS

Working within the design guidelines, the Working Group hopes to achieve the following goals in the development of its instruments:

1. To achieve a safeguards inspection method involving unattended instruments which competes in cost effectiveness (including the amortized cost of purchasing, installing, and maintaining the equipment) with alternate methods of achieving the same results (e.g., more extensive use of inspectors).

2. To make the overall inspection system utilizing unattended instruments more acceptable and less intrusive than alternative methods of inspection.

PRELIMINARY CONSIDERATIONS

When problems which have been discussed only on general and philosophical levels are first faced on a practical level, cherished concepts sometimes have to be abandoned. The first concept which was abandoned was that of the tamper-proof instrument. It does not appear that there is a container which cannot be opened, a barrier which cannot be penetrated. Given enough time, money, and ingenuity, any lock can be opened and any seal defeated. This is not cause for abandonment of the project, however, because the major purpose of the system can still be achieved if the
system deters diversion because of the risks and efforts required to alter or replace the independent safeguards data and if the system indicates that it has been tampered with. Thus, we have dropped "tamper-proof" as an acceptable safeguards adjective and substituted tamper-resistant/tamper-indicating.

Once a decision has been made to use instruments to contain or monitor the flow of fissile materials from a reactor, several basic philosophical approaches are possible. One method of containing the flow of materials produced within a facility would be to construct an envelope or barrier around the facility and then place measurement and detection instruments at the access ports to the envelope. This method, which has been called the "containment" approach, greatly simplifies the problems of designing the controlled entrance but transfers those problems to the development of an impermeable barrier. For example, to ensure that an escape route through which a 3-inch-diameter fuel bundle could be passed did not exist in the containment of NPD would have required a disproportionate amount of effort. In more general terms, a complete "containment" approach to an instrumented safeguards system which would not require a technical breakthrough that would make large surface areas confidently tamper-resistant/tamper-indicating is not foreseen.

An alternative to the containment approach would be a "surveillance" system where all fissile material produced was measured and accounted for. A very accurate tamper-resistant/tamper-indicating measure of the number of fissions occurring in the reactor and an equally accurate method of checking that the produced plutonium was still in the spent fuel elements in the bay would seem to be an adequate assurance that no material has been diverted. Unfortunately, the accuracy required of these two measurements has not yet been obtained, even by reactor operators with all the information available to them. The possibility of making these measurements in a secure fashion with unattended instrumentation is (at present) vanishingly small.

The Working Group also considered the possibility of applying tamper-resistant/tamper-indicating techniques to the sensors the operator had installed for his own information. This approach was rejected for several reasons. An unacceptably large number of functions required monitoring to provide an unambiguous signal. The tamper-resistant/tamper-indicating techniques available or foreseeable were not easily applicable to existing sensors, and, finally, the design of an acceptable data interface between the operations and safeguards information systems posed several problems. Most of the presently installed sensors are vital to the operation or safety of the reactor or one of its subsystems, and a completely separate information network using separate sensors seemed essential.

The Working Group then considered the method of applying surveillance to a reactor by means of inspector-installed instruments which would observe all refuelling operations so that an accurate count of all fuel bundles removed from the reactor could be obtained. If this method were coupled with surveillance of the route to the spent fuel bay and of the bay itself, then all fuel removed from the reactor could be accounted for by the system. A measurement of reactor power and a measurement of the plutonium content of fuel in the spent fuel bay would provide a valuable source of redundant data which could be used to cross-check other sources of information. This was the approach finally adopted.

Early in their deliberations, the Working Group became aware that any unattended system was vulnerable to harassment by an operator. He can damage equipment "accidentally." He can cause component failures which tend to discredit the system in the eyes of the inspector. He can operate his equipment to provide ambiguous information. He can insist that any installation on any of his equipment be made only by his operators. He can restrict the movement of the inspectors for "radiological safety" reasons. Or he can remove installed safeguards equipment because of an "operational emergency." Harassment of this nature is one obvious and unavoidable way to discredit or defeat an instrumented system. However, the Working Group concluded that harassment was a manageable problem because the inspection agency would always retain the option of replacing the unattended system with continuous resident inspection. It became clear that the desired effectiveness and reliability were not being achieved by the instrumentation.
THE NPD SAFEGUARD EXPERIMENT

The CANDU type of reactor is well suited to monitoring by an unattended instrumentation network. The customary configuration (see Figure 1) consists of a core lattice of horizontal fuel channels cooled and moderated by heavy water. Two remotely operated fuelling machines, working always at opposite ends of the same channel, insert and remove fuel bundles while the reactor is on power. In the larger plants, the refuelling operation is essentially continuous, with a spent fuel bundle being discharged every hour or so. Such frequent refuelling would require continuous resident inspection if instrumentation was not used.

As has been mentioned, the configuration of the fuel, its initial composition, the path it follows, and its exposure history all have a bearing on the choice of safeguards methods. The usual fuel transfer operation proceeds as follows: a new fuel bundle is fed into the rotating magazine of the machine from either new fuel room. The bundle is an assembly of concentric rows of pins separated by coolant channels. Individual pins are zircalloy tubes containing pressed pellets of unenriched uranium oxide. While bundles vary somewhat in size and weight for different reactors, the ones for NPD are not atypical. The assemblies have a diameter of ~7.5 cm, a length of ~50 cm, and a weight of ~10 kilograms. The machine moves to the reactor face, couples to the selected channel, and removes shielding and sealing plugs which it holds in vacant positions in the magazine.

The other machine similarly joins the opposite end of the channel. By coordinated movements of the two rams, the new bundle is added to the fuel string at one end while an irradiated bundle is pushed out at the other and the channel is resealed. The machine receiving the used bundle will discharge it into the spent fuel chute if the bundle has reached the operating burnup level of ~8000 megawatt days per ton. Otherwise the bundle may be returned to the core in a different position to aid in flux flattening, a process which makes the flux more nearly uniform throughout the core.

In summary, either machine will normally receive fuel from the new fuel room or the reactor core. Under extraordinary conditions, fuel could be placed in a machine while it is outside the reactor vault in the service area. Usually either machine will eject fuel only at the spent fuel chute or into the core. However, it can possibly eject fuel into the vault, the service area, or the new fuel room.

The rates at which refuelling operations are performed have an important bearing on required safeguard observation frequency. Machines move vertically and laterally at about 3 cm/sec, while the cycle of unsealing, removing fuel, and reclosing a channel consumes about 20 minutes.

Freshly discharged fuel bundles are, in most cases, highly radioactive and may only be safely handled under water in the spent fuel bay or in casks until the bundles have cooled for many months. An occasional bundle may remain at an outer core position for several months before removal and would have far below average intensity. The safeguard plan being contemplated in the TRUST experiment would require all fuel discharged between inspections to remain in the cooling pool for subsequent counting and assaying.

Since the project is intended to demonstrate generally applicable techniques rather than to safeguard a specific facility, much latitude was taken in the interest of economy. Where symmetry permits and experimental rules could be formulated to cover the omission, only one completely protected measurement is taken when, in principle, duplicates are required. Some of the money and time saved by this shortcut have been reinvested in demonstrating other general-purpose devices during this experiment. Although longer times might be desirable, data storage capacity for only 1-1/2 months is being incorporated under the assumption that no innovation is required to expand the capacity arbitrarily.
Figure 1. Surveillance Instrumentation Location
THE INSTRUMENTATION SYSTEM

For clarity, it is convenient to consider and discuss the unattended instrumentation as two interdependent subsystems: one to detect diversion by making sufficient independent measurements to preclude any unmonitored branch in the flow of irradiated fuel and to validate the operator's records; another to prevent deception by securing these independent measurements in such a way that all falsifications are detectable. The strong interdependence between subsystem designs has dictated that measurements taken to prevent diversion be of a kind that can be made most secure. In the TRUST Project, we were able to choose only nuclear and optical measurements—which are fairly easily secured, as contrasted with contact measurements which are more readily falsified. Significantly, failure of either subsystem makes the whole system vulnerable to exploitation within externally imposed limits on plant input and output.

DIVERSION DETECTION

The diversion detection subsystem consists of a combination of hardware and software. The design approach requires that measurements be taken of significant quantities, in correct locations, at adequate frequency, and with sufficient accuracy to describe fuel flow and reactor operating conditions. The data thus taken are analyzed and compared with station records to determine whether or not safeguard requirements are being met.

Monitors for diversion are direction-indicating bundle counters and the surveillance cameras which include the gamma level detectors and field of view motion detectors which trigger them. The locations of these instruments are shown in Figure 1 and a functional block diagram is shown in Appendix A.

Crucial elements in the system are the bundle counters attached to each fuelling machine and each spent fuel chute. Irradiated fuel moving past a pair of collimated ion chambers (Figure 2) produces signals which indicate the presence of a bundle and its direction of travel. The sequence of signals associated with a fuel movement reveals whether a bundle has been transferred from the core to the spent fuel bay or has been moved from one channel to another. Both background radiation and fuel bundle activity are expected to vary widely; the first depends on fuelling machine position in the vault and the content of its magazine, and the second depends on the bundle's position in the core and its dwell time before removal. Allowance for the widest possible range of signal-to-background ratios is made by reading only the difference between outputs of the two ion chambers.

An independent neutron power monitor, a commercial ion chamber mounted in a stepped plug in the biological shield (Figure 3), is intended to confirm plant records of power production. Unlike the bundle counter, it puts out quantitative data and must be calibrated against an agreed-upon standard. An attempt is being made to use the 16-level (4-bit) output in non-linear fashion. Near the nominal power level, smaller increments would give greater accuracy; while, at low power where continued operation is unlikely or impossible, coarser data would be acceptable. Readings are recorded at regular intervals (10 minutes) on demand.
Television cameras (Figure 4) monitor the reactor faces, fuelling machine vaults, and the spent fuel bay. The cameras detect diversion by watching for fuel handling with equipment other than the fuelling machines at the reactor face and for attempts to insert decoys and remove fuel from the spent fuel bay. Resulting pictures of the fuel channel being serviced confirms operator's fuel-handling records.

In the prototype system, only one end of the reactor is under TV surveillance.
A gamma level trigger on the spent fuel bay camera keeps it alert to the possible hasty removal of fuel without involving the time-consuming operation of putting it in a flask. Another camera-triggering device, which is optically sensitive to motion (Figure 5), will produce more frequent pictures when protracted activity is observed. Cameras also protect data by detecting tampering with the bundle counters, with the neutron power monitor, and with themselves. Television was chosen instead of a film camera because of its adaptability to a radiation environment. Long-term, low-level exposure will not obscure the early portions of a record, nor will a plausible accident wipe out all the data.

The Working Group is persuaded that the choice and layout of sensors will reliably count and trace irradiated fuel, confirm the operator's records, and detect diversion if the data are not falsified. One of the goals of the experimental portion of the project is to verify that the design logic is sound and that undetected diversion is not possible.

**Data Protection**

If it is assumed that the diversion detection logic is without fault or can be made so, preventing undetected data falsification becomes the chief security burden. Independent measurements can be falsified in several ways, all of which must be guarded against:

1. The field surrounding the sensors may be altered to produce false readings.
2. The sensitivity or calibration of the sensor can be changed.
3. The sensor can be disconnected and a substitute input attached to the data lines.
4. True records can be replaced by false, but credible, records generated by the diverter.

The first method requires introduction of sources, shields, or sinks near radiation instruments, image substitution in front of TV, or movement of the sensor to a new location. Sources, sinks, and shields are precluded by camera surveillance and cross-check logic; image substitution is complicated by use of wide-angle lens and mirrors; relocation is prevented by site seals or tilt sensors for package motion, or both. Disabling or harassing fields—temperature, magnetic, radiation—are designed against and/or detected by dosimeters, temperature-sensitive coatings, etc.

The second method requires access to sensors. Attempted access is detected by glass containers with closure seals. Opening these containers destroys a fingerprinted (uniquely identified) seal laced through holes in the body and cap, while penetrating the container leaves easily discernible visual indication.

The third method can be detected statistically if authentic data are coded. Since profitable diversion requires repeated spoofing, a not-too-sophisticated form of random coding will give very high probability of detecting repeated diversion attempts. For radiation instruments, data are digitized, combined with a stored random authentication word (part of which is a coded read
command), and then transmitted. TV information is authenticated by scanning the picture in a random pattern before transmitting.

The fourth approach—record replacement—is most serious for TV data because the authentication words may be readily determined and recombinied with false pictures. Given correct corresponding readings on other sensors, substitution could go undiscovered. The recording station is therefore protected by an intrusion monitor which detects and records disturbances in an RF field in the screen room surrounding the equipment. When the disturbance exceeds a certain threshold electrical value, a counter indicating an intrusion is advanced. Power interruptions are also counted and recorded. Since the type of counter used in both instances is neither reversible nor capable of recycling, erasure is not possible.

COMPONENT DESCRIPTION

The subsystem whose purpose is to prevent data falsification includes, besides cameras, glass secure containers, tilt sensors and power-loss monitors, digital data authenticators, a coded clock, a picture permuter, battery power, and the recording station intrusion monitor.

The diversion detectors—bundle counters, the cameras and their gamma and motion sensors—are protected from tampering by glass secure containers. Tilt sensors and power-loss monitors are enclosed by these same vessels. The secure containers are made of Pyrex glass with aluminized inner surfaces (Figure 6).

![Figure 6. Secure Container](image)

The bodies are closed-end cylinders, and the bases are gasketed flanged plates held in place by a fractional-turn pin lock. Once closed, the lock is restrained by a fiber-optic seal threaded through aligned holes in both body and base (Figure 7). Unlocking the container will sever the seal. The aluminum coating acts as a radiant-heat barrier and even very small holes are easily seen. Penetration through the connector, if not otherwise obvious, is detected by fracture of a small stressed-glass plate imbedded in transparent plastic inside the container (Figure 8).
Tilt sensors prevent the undetected relocation of packages which cannot be readily fixed in place with a site seal. The devices proposed for this experiment (Figure 9) are helical columns loaded to near buckling by a mass which is part of an electrical circuit.
Slight lateral acceleration, of the order of 1/100 gravity, will cause the column to buckle and allow the weight to make contact. The natural frequency of the sensor is less than 1 cycle per second; therefore, it will tolerate sharp shocks and vibration without tripping. The device also has a heavily damped self-leveling feature which allows some installation misalignment. Tilt sensors are associated with 2-bit digital counters which will indicate number of operations as 0, 1, 2, or 3 or more (numbers greater than 3 not counted). The power-loss monitor, which consists of high- and low-voltage sensors, uses a similar method of counting and shows the possibility of sensor disconnect. To keep the unattended instruments on-line during short power interruptions (up to 1/2 hour) a battery and trickle charger are located in the recording station. The digital data authenticators, whose function is elaborated in another section, consist of punched tape readers (Figure 10), integrated-circuit adders, and shift registers. Punched tape is also the input to the permuter which controls the sequence in which TV pictures are scanned. The recorder, which stores all the digital data on magnetic tape, contains a digital clock, the synchronizing source for the entire system. Precise time control is not necessary because ambiguities of several seconds are required for spoofing.

Given access to the inspector's records during his absence, the would-be-diverter could falsify some data and prejudice the cross-checking capability of the system. To foreclose this eventuality, the recording station is protected by an RF volume monitor. Recording apparatus is contained in a conductive cavity, in this instance a commercial screen room. A standing wave pattern at about 110 megahertz is introduced into this cavity at 1/10 watt through two stub antennas. With all equipment in place and doors closed, a bridge circuit is balanced and the nulling circuit is irreversibly opened from outside the room through a fusible switch. Reopening the door or probing through the walls with conductors will disturb the field and trip the intrusion counter. The counter will record 10,000 intrusions, both legal and illegal, before requiring replacement. Protection for the counter is provided by a stressed-glass secure container.

DATA AUTHENTICATION

Digitizing and encoding the bundle counter and power monitor data involve conventional techniques. Authentication of the video data employs the same encoding techniques applied in a novel way. The heart of the encoding system consists of prepunched tapes in each secure container and in the recording station. Thirteen thousand 8-bit random words are punched into each tape, and each reading is combined with one of these words before being transmitted. Sensors can be triggered by commands either internal (to the package) or external (from recording station); and, since signal origins are a part of the system logic, they are identified by labels in the code format. The neutron power monitor is an exception in that it reads only on periodic external command. When the output of bundle counter ion chambers reaches a sufficient level, the signals initiate an authenticate-and-record sequence (Figure 11). Two bits giving direction of bundle motion, two bits showing power monitor reading, and one bit indicating internal initiation are combined (non-carry add) with the next authentication word from the punched-tape. The result is loaded into a register, shifted the number of positions indicated by the first two bits of the authentication word, and transmitted to the recorder. Since long periods of inactivity in the fueling procedure are not abnormal and may be simulated by disconnecting counters to cover a diversion effort, the status of all bundle counters is checked at random intervals. An external 2-bit command, together with a 1-bit address to indicate its external origin, is substituted for ion-chamber output. The power monitor count is also read in, and authentication is performed. Spent fuelclide bundle counter packages differ in
that a tilt sensor instead of a site seal precludes relocation of the sensors. Both tilt sensor and power monitor counts must therefore be read out of this instrument.

Figure 11. Digital Authentication Sequence

Similar but more elaborate authentication takes place in the spent fuel bay TV camera package. Single frames are transmitted on random interval command but, in addition, sensors which monitor package tilt, motion in the field of view, and unusual gamma levels will also trigger the shutter. When a frame is recorded, the source of the trigger signal is identified to provide either a clue to possible illegal activity or an indication of system fault. One word from the punched tape authenticates the identity of the triggering signal and serves as a time fiducial for the picture to be transmitted. The adjacent random word from the same tape controls the order in which the picture is scanned. Therefore, for a given number of data points, twice as many authentication words are expended for the TV as for other sensors. The system would be vulnerable to falsification of pictures without this second level of authentication. Motion in the field of view, while legal, could be used as a harassing tactic to expend the recording capacity in a time much shorter than the interval between inspections. To prevent this, a 10-minute lockout sets the maximum rate for motion-triggered pictures.

In the camera selected for this system, the line order in which the picture is scanned is determined by a 9-bit binary control which proceeds from line 1 through line 512 in order and then resets for the next frame. In Figure 12, counter outputs are shown entering the permute on the nine lines at the left. The permute, interposed between the counter and deflection circuit, is equivalent to eight double-pole double-throw switches whose state is controlled by random words from the punched tape. The resulting scanning sequence for any picture is unpredictable as the example indicates. When the counter calls for line 171, line 171 will be scanned if the permute is loaded with word P1, line 301 if P1, and line 527 if P1. Although the random word can readily be determined from the record, it cannot be predicted with certainty until 128 lines have been recorded, a matter of 5 seconds. While the illustration shows how incoherent an authenticated picture becomes, the extent to which an image is visually scrambled is not significant here. A potential diverter is
not trying to reconstruct the picture; he already knows and controls its content. He is trying instead to intercept the signal, strip off the authentication word, combine it with his false picture, and reintroduce the result to the recorder within an undetectably short time.

\[
P_I = 1 1 1 1 1 1 1 1 1\]
\[
P_{II} = 0 0 1 1 1 1 0 0\]
\[
P_{III} = 0 1 0 1 1 0 0 1\]

**Figure 12. TV Authenticator**
DATA COMPRESSION

Prolonged periods of unattended operation could yield an unmanageable volume of records if no attempt was made to restrict the amount of data recorded. Once storage capacity is fixed, diverter-induced premature runout must also be avoided. Read command signals serve not only to authenticate data but also to control the rate at which it is collected. The minimum sampling rate must be such that the shortest significant event has a high probability of being detected, while the maximum rate must not exceed storage capacity during the interval between inspections.

Data from bundle counters are preprocessed by logic circuitry at the sensor end to eliminate all nonessential information; neutron power monitor data have a low information content which changes infrequently. They present, therefore, no storage problem. A 6-inch reel of half-inch magnetic tape readily accommodates 3 months of data at the planned rate for NPD. By contrast, the recorded television pictures, if taken constantly at a normal rate, would become so voluminous in a few days as to be useless. Compression is achieved in two ways:

1. Pictures are triggered only frequently enough (on an average of every 16 minutes) to catch events which would result in significant diversion (with high probability). Tilt, gamma, and optical motion sensors will also trigger the camera. The random interval command is possible in 2-minute increments and restarts after each exposure.

2. Bandwidth is reduced by using a slow-scan camera which records each frame in 20 seconds as contrasted with 1/30 second for conventional cameras. In the start-stop mode, the volume of tape used is reduced by a factor of 2. (Cost of audio, rather than video, recording is less by a factor of at least 20.)

INSPECTION PROCEDURES

Limiting the complexity of the inspector's duties has been a strong motivating force behind the TRUST system design. Uncoded data channels and a printer were included to provide an immediate and convenient cross-check with operator's records. Where possible, sensor packages are being made readily replaceable to avoid extensive on-site service. Having determined the integrity of the site seal, or after scanning data, the inspector can remove the complete secure container and replace it with another loaded with a fresh supply of authentication words. Interpretation and authentication of digital data are intended to take place at a central computing facility, and we hope to automate reconstruction and inspection of TV pictures with pattern-recognition techniques. Preliminary inspection procedures have been drafted, and their efficacy will be tested by the NPD experiment.

TEST RESULTS

A number of major subassemblies are nearing completion, but the entire prototype system will not be assembled and checked out for another 2 or 3 months. Therefore, up to this point in the program, testing has been confined almost entirely to functional experiments with little diversion and falsification simulation. Some of the current design features are the result of early attempts to substitute TV images and to penetrate secure containers.

Bundle counters have been tried in several collimator configurations and at two different locations on the fuelling machine in an effort to improve discrimination and increase sensitivity. Variability of background radiation with fuelling machine position and magazine contents, when coupled with large differences in bundle signatures related to in-core cooling time, makes deriving an unambiguous signal very difficult. Functional limitations on counters have yet to be established.
Recording TV pictures on audio-frequency equipment and reconstructing them has resulted in some loss of resolution as anticipated. The loss appears acceptable for the purpose of this system. The RV authentication permuter has been successfully demonstrated, and the digital data authenticator and package tilt sensors have shown adequate sensitivity.

Stability of the RF volume monitor has been tested, with satisfactory results, over a period of several months in a screen room mock-up. All attempts to penetrate the glass secure containers without leaving easily discernible visual evidence have so far been unsuccessful. Holes as small as 0.1 millimeter in diameter, produced by electron beams and lasers, are conspicuous in the mirrored surfaces without magnification (see Figure 13).

![Figure 13. Holes in Secure Container](image)

**PROJECT STATUS**

The Working Group has chosen the safeguard approach considered most appropriate to the specified reactor type. The logical design of the instrumentation system has been established and the needed measurements specified. Sensors of the appropriate type have been designated for the required locations. Specialized equipment design and construction is underway in Canada and the U.S. Preliminary component evaluation has already begun, and laboratory evaluation of subsystems will be performed during this summer. The on-site experimental phase beginning this fall will test both the functioning of the system, its reliability, accuracy, and life, as well as its susceptibility to subversion.
CONCLUSIONS

The highest credibility is properly assigned to conclusions based on data from independent sources which are essential to any safeguards system, but, in practice, information obtained from the reactor operator may be used to assist the safeguards inspector substantially. For example, the burnup data calculated by the operator's fuel-handling program may be verified by accurate analysis of a few irradiated bundles. If proper sampling techniques are used, considerable reliance may then be placed on the operator's burnup data. The occasions are frequent where data obtained through normal plant operation, if substantiated by limited but independent sources, can be used to advantage by the safeguards inspector.

Two classes of information will be available to the inspector making use of this instrumentation system. The first class, independently supplied by his tamper-resistant/tamper-indicating instruments, is generally of low accuracy and high security. The second class of information, available from the operator's records and instruments, is generally of high accuracy and low security. Rather than attempt to provide a complete record of reactor operations with secure instruments, the system will provide enough secure information that the reactor operator's records can be cross-checked and verified on a statistical basis. The inspector will then be able to rely on the operator's records with a much higher degree of confidence.

After careful study and preliminary investigations, the Working Group feels that there is a strong probability that instruments can be developed which will provide secure, independent, and credible safeguards data. It is also apparent, however, that any such tamper-indicating instruments, although they may prevent undetected diversion, are vulnerable to harassment by a potential diverter. The essential requirement here is that the instrument system should indicate that it has been defeated. If this happens, the inspection agency can fall back on equally effective, but possibly more expensive methods, such as resident inspection.

These new instrumentation systems may allow the inspector to reduce both the time he must spend at a facility and the degree of access he requires to apply credible safeguards. However, since the operator can at any time render an instrumented system ineffective or make design changes which could circumvent the installed instruments, the inspector must have at least the right of access he now enjoys. Limited rights of access would not provide for those occasions when the instruments no longer do the job, either on account of failure or harassment.

It should be evident from the foregoing discussion that the NPD experimental safeguard scheme, the sensors, and the authentication devices do not greatly extend the art. However, this joint Canadian/USA effort has one important attribute: it will provide one of the earliest opportunities to determine, in a systematic way, the value of unattended instrumentation as a complement to inspection.

The overall objective of safeguards is to provide early detection of the diversion of nuclear material to other than peaceful purposes and, by the risk of such detection, to deter any such diversion. The system, as developed, should be sufficiently effective to convince the operator or would-be-diverter that the effort he must expend to achieve a successful diversion is of considerably greater value than what he would achieve or obtain by such a diversion. It is on this general basis that the effectiveness of this system will ultimately be assessed.
APPENDIX A

FUNCTIONAL BLOCK DIAGRAM