2

Department of Energy/Office of Intelligence and National Security

DOE/AN/ACNT-93A

Arms Control and Nonproliferation Technologies

Second Quarter 1993

Tags and seals for controlling nuclear materials

The cover

Observers from the Department of Energy and the Defense Nuclear Agency watch as a tag/seal is applied to a uranium hexafluoride cylinder during the demonstration held at Portsmouth Gaseous Diffusion Plant.

The purpose of *Arms Control and Nonproliferation Technologies* is to enhance communication between the technologists

who develop means to verify compliance with agreements and the policy makers who negotiate agreements.

Tags and seals technologies demonstration

In June 1993, the Department of Energy conducted a demonstration of the ability to tag and seal potential nuclear material containers appropriate for the U.S.–Russian conversion of highly enriched uranium (HEU) to low-enrichment uranium (LEU). Begun in the Office of Arms Control and Nonproliferation, the task was carried out after DOE's reorganization by the Office of Research and Development. Tags and seals that were previously developed at the DOE national laboratories and under the sponsorship of the Defense Nuclear Agency were demonstrated on three possible containers: the Department of Transportation Specification 6M HEU container, the AT-400R HEU container, and the Type 30B uranium hexafluoride cylinder.

Published by
U.S. Department of Energy, Office of Intelligence and National Security
John G. Keliher, Director

DOE ACNT Project Manager
Michael F. O'Connell

Scientific Editor
George Staehle

General Editors
Cynthia Talaber
Sue Stull

Scientific Editorial Consultant
Peter Moulthrop

Art/Design
Ellen Baldwin

Printing and Production
Lawrence Livermore National Laboratory

Correspondence
George Staehle or
Sue Stull
Arms Control and Nonproliferation Technologies
Lawrence Livermore National Laboratory
P. O. Box 808, L-205
Livermore, CA 94551

Phone
(510) 422-7365

Arms Control and Nonproliferation Technologies

Second Quarter 1993

Contents

Introduction

Christos Makris
DOE Office of Research and Development

The desire to uniquely identify valuables is not new to human thought. Written history shows that the ancient Egyptians used seals to identify government documents, while the Babylonians used tags and seals for their trade with the Indian and Chinese civilizations. Since the discovery of nuclear fission and its subsequent use in national defense, few valuables have been more prized than special nuclear materials (SNM). Nations currently possessing SNM safeguard their existing inventories, while proliferant nations seek to obtain sufficient quantities of SNM to exploit nuclear energy for military purposes. International treaties and agreements related to safeguarding SNM often require using tags and seals within the material control and accountability system.

Our office recently had the opportunity to exhibit current state-of-the-art tag and seal technologies as could be applied to the U.S. purchase of Russian highly enriched uranium (HEU). DOE offices responsible for treaty policy and negotiation collaborated to invite the Russians to the Portsmouth Gaseous Diffusion Plant located near Piketon, Ohio, in June 1993. The visit was part of an exchange review of the enrichment facilities in Russia and at Portsmouth. A part of the review was a briefing and demonstration of tags and seals currently used in DOE's domestic safeguard systems or undergoing research and development. The reader should consider that the tags and seals described here have varying characteristics, including cost, ease and length of time for application and removal, and method of verification (visual, electronic, photographic, etc.).

This issue of *Arms Control and Nonproliferation Technologies* summarizes the demonstrations and addresses related topics. The first article, "Basic Nuclear Material Control and Accountability Concepts as Might be Applied to the Uranium from the U.S.–Russian HEU Purchase," describes safeguards subsystems necessary for effective nuclear material safeguards. It also presents a general discussion on HEU-to-low-enrichment uranium (LEU) commingling processes and suggests applicable key measurement points.

The second article, "A Framework for Evaluating Tamper-Indicating-Device Technologies (TIDs)," describes their uses, proper selection, and evaluation. The final three articles discuss the tags and seals applications and general characteristics of several nuclear material containers: the Type 30B uranium hexafluoride container, the AT-400R container, and the DOT Specification 6M container for SNM.

Finally, the Appendix displays short descriptions and illustrations of seven tags and seals, including: the E-cup and wire seal, the python seal, the cobra seal, the tamper tape seal, the secure loop inspectable tag/seal (SLITS), bolt-and-loop type electronic identification devices, and the shrink-wrap seal.

Our office greatly appreciates the ambitious efforts of all participants and authors. Special thanks go to the Defense Nuclear Agency (DNA) for its support through USAF Captain Roy Nelson of DNA's Albuquerque Field Command. Captain Nelson played an integral part in the SLITS seal for this demonstration. Dr. Leslie Pitts, EG&G Washington Analytical Services Center, gave valuable support in orchestrating daily activities. Mr. Rich Boelens of the Portsmouth Gaseous Diffusion Plant, Martin Marietta Energy Systems, assisted the scientists in setting up their demonstrations and obtained the necessary nuclear material containers. We especially thank Mr. Andrew Bieniawski, DOE/HQ, who made the demonstrations possible.

Basic nuclear material control and accountability concepts as might be applied to uranium from the U.S.–Russian HEU purchase

C. Ruth Kempf
Brookhaven National Laboratory

Nuclear material control and accounting and physical protection systems are designed to deter, prevent, detect, or respond to unauthorized possession, use, or sabotage of nuclear materials. This article presents a brief summary of material control and material accounting fundamentals, followed by a synopsis of appropriate materials accounting and materials control system components that might be involved in the U.S.–Russian HEU to LEU (highly enriched uranium to low-enrichment uranium) process.

Safeguards—an introduction

Physical protection primarily addresses the *outsider threat*; i.e., it detects, assesses, delays, communicates, and responds to such a threat. Materials control primarily addresses the *insider threat* by providing detection capability for both abrupt and protected diversion or theft of nuclear materials, by providing information for the assessment of threats, and by assisting in recovery of missing nuclear materials. Materials accounting primarily addresses the *insider threat* by providing detection capability for protected theft or diversion and, in normal operations, it is the only safeguards and security element that provides periodic assurance that the nuclear materials are actually present in the correct amounts and at the correct locations.

Safeguards and security systems, including materials control and accounting and physical protection, are designed to provide varying degrees of control, accounting, and protection depending on the different types, quantities, physical forms, and chemical or isotopic composition of the nuclear materials in a manner consistent with the risks associated with theft or diversion scenarios for those materials. This is called the principle of "graded safeguards."

Some fundamentals of material control and accounting

Nuclear material control

Nuclear material control consists of measures designed to prevent unauthorized movement of special nuclear materials and to detect theft or diversion promptly. It comprises a set of management and process controls designed to

- Assign and exercise responsibility for nuclear materials.
- Govern the movement, location, and use of nuclear materials.
- Provide containment and surveillance of nuclear materials.
- Monitor the inventory and process status.
- Detect unauthorized activities involving nuclear materials.
- Help resolve apparent losses of nuclear materials.

Material control can include: (a) the use of barriers to access, such as secured vaults, physical enclosures, and access controls; (b) channeling material through authorized flow paths and storage locations; (c) monitoring of process lines and remote instrumental surveillance; (d) use of secure containers and storage; and (e) the use of seals and identification codes. Material controls fall into four functional areas:

- *Access controls* of personnel to nuclear materials; to nuclear material accountability, inventory, or measurement data; to data-generating equipment or to any other items or equipment that might be manipulated to compromise the safeguards system.

- *Material surveillance programs* that monitor nuclear materials to detect unauthorized activities.
- *Material containment programs* that provide control over nuclear materials operations for materials access areas, storage areas, and in-process areas. This can include the use of tamper-indicating devices (tags and seals) on containers.
- *Detection and assessment capabilities* that, when interfaced with physical protection and material accounting, provide a high probability of detection of removal of special nuclear materials from authorized locations. These capabilities can include functions such as daily administrative checks of material balance areas; programs for control of tamper-indicating devices; portal monitors to facilitate physical or electronic search of vehicles, personnel, packages, or containers for unauthorized removal of special nuclear materials; waste monitors; process monitoring; and near-real-time accountability.

Nuclear material accounting

Through nuclear material accounting, the locations and quantities of nuclear materials within a facility (and, during shipment, between facilities) can be tracked. It comprises a set of procedures and systems to

- Perform nuclear material measurements.
- Verify location and quantities of nuclear materials through physical inventories.
- Maintain records and provide reports on nuclear materials.
- Perform data analysis to account for nuclear materials to detect losses of nuclear material.
- Help resolve apparent losses of nuclear materials.

Basic materials accounting concepts include the ideas that nuclear materials must be measured and that the measurement systems used must be subject to measurement control programs. Locations of nuclear materials must be verified via periodic inventories carried out according to documented inventory procedures and in parallel with accounting and confirmation measurements. Accounting records must be kept and reports must be prepared periodically from these records. The accounting system must link all movements, transfers, processing, shipments, etc., of nuclear materials throughout a facility. It must include data analysis and loss-detection programs (statistical programs, inventory difference evaluation, and shipper/receiver difference analysis). Finally, the materials accounting system must provide for the investigation and resolution of apparent losses of nuclear materials. This can be accomplished through responding to preset indicators and investigation and reporting.

In general, there are two types of materials forms: "item" and "bulk." "Item" materials are in units—for example, fuel assemblies, containers of uranium hexafluoride, or containers of metal pieces. "Bulk" materials are not partitioned; bulk materials would be poured into receiving tanks and processed through pipes, reactors, extractors, etc. Some facilities handle only items. Examples are storage facilities (where the items might be storage containers), dismantlement facilities (where items would be nuclear weapons parts) and nuclear reactors (where the items would be fuel assemblies). Some facilities handle both item and bulk materials. These facilities generally receive items, process bulk, and produce items. Examples could be reprocessing, fuel fabrication, conversion, or blending facilities. As can be imagined, accounting for items is much more straightforward than accounting for bulk materials. The first may involve mainly tracking of containers with identification tags and/or seals, while the second may involve extensive and complex measurements. However, the quantity of nuclear material contained in an item must be derived from some type of measurement.

In material accounting, accounts are records that show the amounts of nuclear material at specific locations or in specific process equipment. Transactions record the changes in accounts when nuclear material is transferred from one location or process to another. A material balance area (MBA) is an accounting device that usually corresponds to a specific physical area (or areas) of a plant containing related processes and/or storage areas. Flows of material into or out of an MBA must be measured. The use of MBAs allows losses of nuclear material to be localized in space and time.

Records of nuclear material movements into, through, and out of MBAs form the basis of the materials accounting system for a facility. Material accounting records systems must describe all nuclear material transactions and inventories; identify inventory adjustments by MBA; be updated regularly and by authorized personnel only; and provide an audit trail for all transactions.

A value for the total nuclear material inventory present within a given MBA (or for an entire facility) can be obtained from the accounting records. The fundamental accounting relationship is

Beginning Inventory + Receipts
– (Transfers + Shipments)
= Ending Inventory (1)

At the start of the accounting period (month, year, etc.) a physical inventory is taken of the materials in each MBA. During the period, nuclear materials will be moved and/or processed, measurements will be taken, and records of these will be kept as part of the accounting. A "book inventory" can be calculated for the MBA and/or for the facility at the end of an accounting period by taking the beginning physical inventory and adding measured receipts (or additions) and subtracting measured transfers, shipments, or other measured withdrawals (for example, waste materials). Ideally, the next physical inventory will equal the "book inventory." Finally, the result of equation (1) is used with the ending physical inventory result as expressed in equation (2):

Book Inventory
– Ending Physical Inventory
= Inventory Difference (ID) (2)

The difference (if there is one) between the book inventory and the ending physical inventory is called an inventory difference (ID). Material unaccounted for (MUF) is a term used for ID in international safeguards.

A non-zero ID can mean that a diversion or theft of nuclear material has occurred. For such a conclusion to be drawn, however, sufficient consideration must be given to the quality of information present in the accounting data, including measurement uncertainties. For any facility in which nuclear materials are processed in any way (taken out of their initial receipt containers and subjected to some chemical and/or physical change), the accounting records will necessarily contain data corresponding to measurements of material. Since no measurement is perfectly accurate, there will be uncertainties in the amounts of material recorded. These uncertainties should be, as far as possible, kept to a minimum (a role played by measurement control programs, as discussed below). They can, however, contribute to non-zero IDs. Additionally, shipper/receiver differences (SRDs) or generation of hard-to-measure forms of material (for example, deposits in pipes and tanks known as "process hold-up") can also contribute to IDs. Detection of a theft or a diversion of nuclear material through the use of IDs requires that the ID stand out against the background of measurement uncertainties.

Nuclear material loss-detection elements include control limits for inventory differences, statistical tests for accounting and measurement values, long-term inventory difference tracking, and SRD detection. SRDs may be due to measurement uncertainty; different measurement methods; errors in records, reports or measurements; or loss of material in transit. U.S. domestic safeguards materials accounting requires that SRD must be assessed and, if found to be significant, resolved according to procedures given in DOE Orders.

Measurements and measurement control

Measurement methods can be divided into destructive and nondestructive analyses, and bulk (mass or volume) measurements. Destructive analyses include chemical procedures (such as gravimetric, titration, and spectrophotometry methods), mass spectrometry (isotope ratios and isotope dilution mass spectrometry), and radiometric methods (gross alpha and others similar to nondestructive analysis methods). Nondestructive analyses can involve gamma ray spectrometry (for example, to measure uranium-235 186-keV and plutonium-241 145-keV gamma rays), calorimetry, and passive and active neutron measurements.

Through the use of measurement control programs, all

measurements used in materials accountancy can be traceable to the national measurement base by means of standards and reference materials. The facility measurement systems can be calibrated against secondary or working standards. Standards are used for assessing measurement uncertainties. There are several different types of standards, including those for mass, isotopic, chemical, and nondestructive analysis.

Measurement control programs assess random and systematic measurement errors. Facilities must implement measurement control programs on virtually all measurement systems that generate accountability values. These programs must provide for repeated measurements of materials with known values, detection of out-of-control conditions, and measurement comparisons. A program must provide for maintenance of primary standards, periodic recalibration of secondary and working standards and check weights, check weighings of scales, and scale recalibration when out-of-control conditions are detected.

Uranium materials flow—MC&A implications

As part of the U.S.–Russian HEU purchase, uranium extracted from dismantled nuclear weapons will pass through several physical and chemical processes on its way to becoming low-enrichment fuel for civilian nuclear power plants. Several different types of facilities may be involved, each with its own physical layout and each with its own chemical/physical process sequence. For example, from weapons dismantlement facilities, one would expect HEU metal pieces in containers (tagged and sealed, as appropriate) to be the output. Similarly, output from fuel fabrication facilities could be low-enrichment uranium fuel assemblies (tagged and sealed, as appropriate). Both of these examples could be considered opportunities for item accounting.

Uranium-containing items from a dismantlement facility that are shipped to storage or to conversion facilities would have their tags and seals checked for integrity upon receipt. Fuel assemblies received at a power reactor would be similarly checked. Once items (containers) are used as input to processing stages, item accounting ends and "bulk" accounting begins. This would be as true for a conversion facility as it would be for a reprocessing or fuel fabrication facility. Bulk material movements are more difficult to track, and materials control and accounting systems must accommodate this.

Movement of uranium between facilities implies a need for materials control and accounting activities at both facilities, and linking the facilities as well. A statewide nuclear materials control and accounting system is essentially composed of integrated facility-level MC&A systems, tracking materials within and between facilities.

Development of MC&A systems

The main components of a nuclear materials safeguards system are: nuclear materials accounting, nuclear materials control, physical protection and security, and human reliability programs. These components are shown in Figure 1, with emphasis on the development steps needed for materials accounting and materials control. The specifics of a safeguards system depend on the specifics of a facility, i.e., its physical layout, processes, procedures.

Early in the design of materials accounting and control, based on facility design information, MBAs must be defined for appropriate states, steps, buildings, processes, etc. For each MBA, nuclear material measurement points must be designated and accounting systems must be set up. Fundamentally, the nuclear materials entering and leaving an MBA must be determined or known, and the physical inventory within that MBA must also be obtainable.

Material accounting for an MBA would consist of ledgers that contain data on beginning inventory, receipts, transfers (including losses), and ending inventory. These data are recorded from primary documents that include transfer sheets, inventory forms, measurement reports, etc. Each time an MBA receives material, a transfer document would indicate the amount and "batch" or other identification. The accounting equations given earlier would be applied to the MBA and the "inventory difference" for the MBA could be tracked.

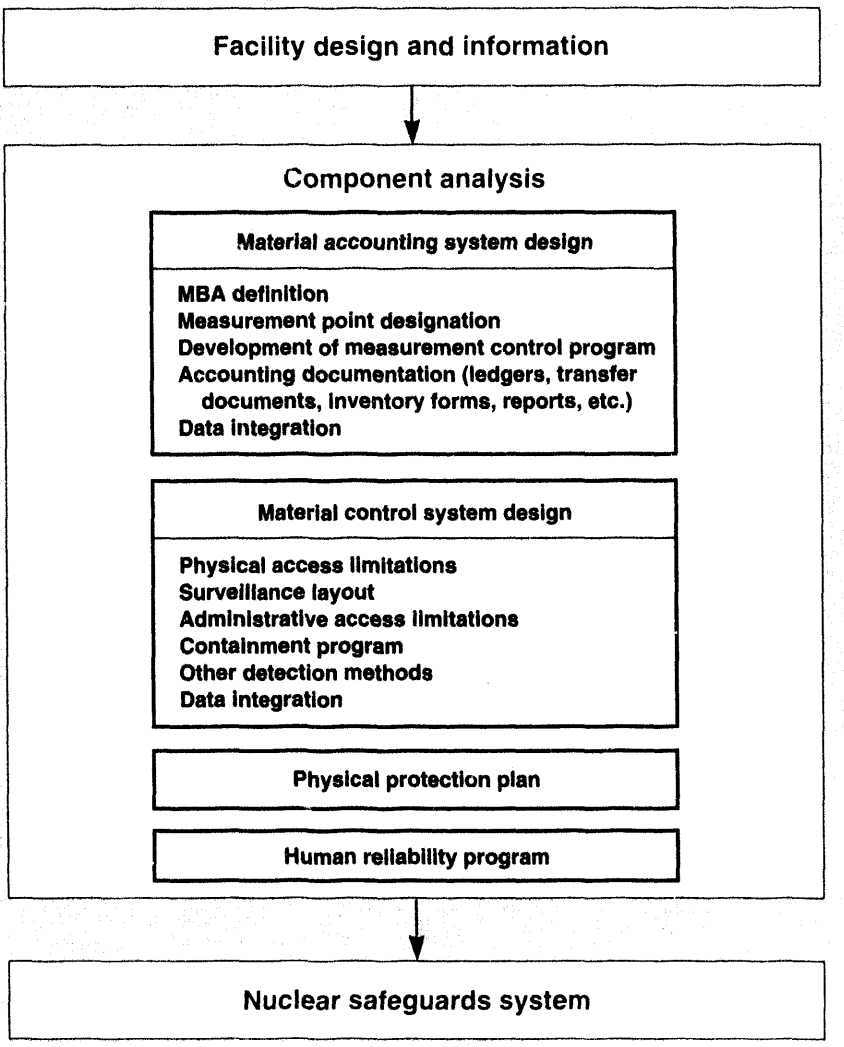
Similar or analogous measures would apply for each MBA. A unifying accounting system would fold together data for all MBAs into one general ledger

from which an overall ID could be determined for a facility/process as a whole. "Acceptable" values for individual IDs and for the universal ID depend on the safeguards "value" of the nuclear material. For instance, the ID for an HEU stage should be much smaller than the ID for an LEU stage. Further, as discussed earlier, the integrity of the numerical value of the ID is a function of the quality of measurements and of interactive accounting and control components.

Specific material control components that might be used for a processing MBA should involve physical access limitation to the process area (for example, personnel carrying uranium containers would have to pass through a physical portal and be screened upon entry to and exit from the MBA), and container tags/seals, etc., would be monitored.

In general, when materials move out of a physical processing stage (for example, a reactor or centrifuge) they are either directly pumped to the next stage or they are put in containers and physically moved from one stage to another. Safeguards "credit" can be given for physically restricted stages, as long as all inputs and outputs are monitored. As an example, the enclosure in which a metal-to-oxide reaction occurs can be assumed to "contain" the nuclear materials during that reaction. Once completed, however, the oxide is again "exposed" to a potential theft or diversion. Thus, material accounting and control measures must be implemented; for example, a measurement could be made of the output and containers could be tagged and sealed. The container identities (serial or identification number) and contents would then be entered in the accounting documents and ledgers for that MBA.

Figure 2 provides a schematic presentation of processing steps, with each having been designated an individual MBA. The physical process in MBA-1 could be metal-to-oxide reaction, in MBA-2 oxide-to-fluoride reaction, in MBA-3 purification, etc. The transfer into the MBA comprises several MC&A measures, including: (1) an entry in the preceding MBA ledger for a transfer out of



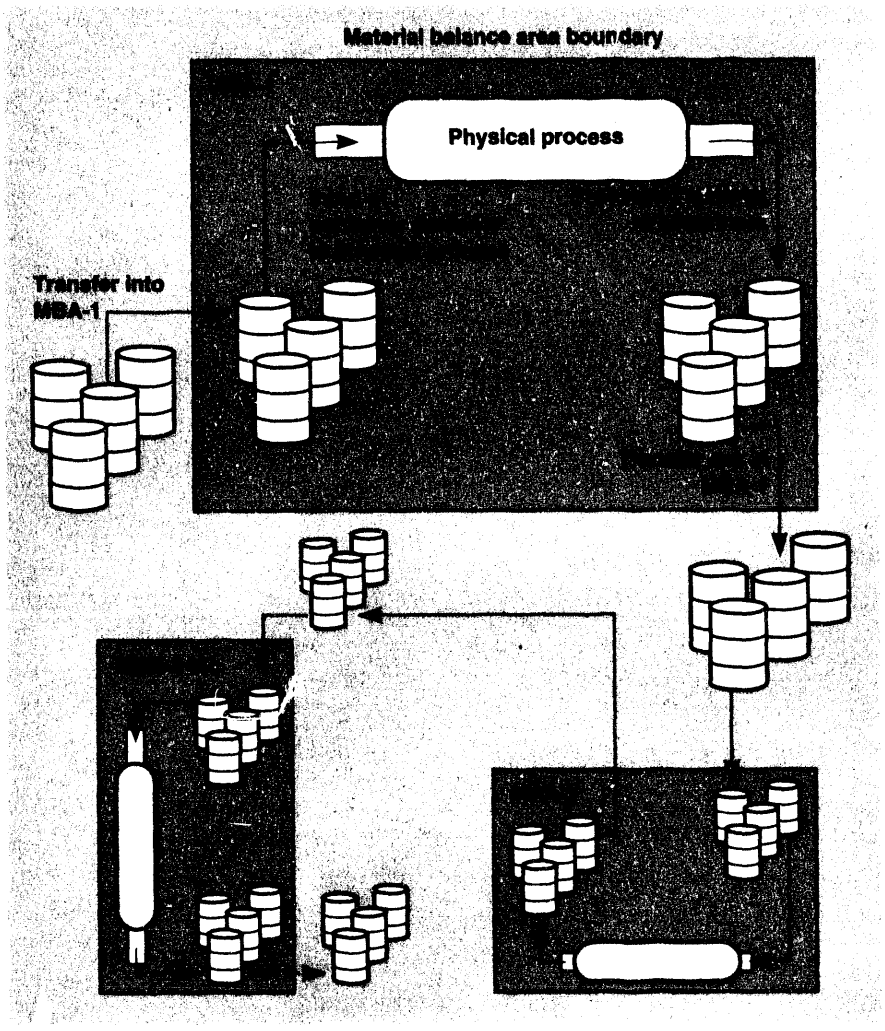
■ *Figure 1. General safeguards system development steps for any facility or process.*

x amount of material in batches/containers with identification numbers; (2) confirmatory measurements of the containers, and/or checking of tags/seals and documentation of these steps; and (3) given that all material is present and that tags/seals are intact, an entry in the MBA-1 ledger for a receipt of *x* amount of materials and the container identification numbers. The transfer out of MBA-1 would involve analogous steps to (1), (2), and (3), except that the MBA-1 ledger would show a transfer out and new tags/seals would be applied.

At the input of container contents to the physical process, limitations on access of personnel may be applied at storage areas and from the point that tags/seals are removed from incoming containers; similar limitations would apply as the processed material is moved to containers. Surveillance may be used at any stage in which materials are being stored (temporarily or for longer periods) before transfer in or out of MBAs, or before input into a physical process within an MBA.

Figure 2 indicates linkages between MBAs. Transfer documentation and material control procedures for these linkages must be used. The same principle applies when the transfers are no longer simply within one building but are between buildings or even between sites. Physical protection can be provided anywhere, but will almost certainly be used around whole buildings and in transfers between buildings and/or sites.

It must be emphasized that the MC&A system described cannot be taken as complete or necessarily even consistent, since such a system would be highly dependent on details of relevant facilities, processes, and procedures. Further, a complete integrated MC&A system for any nuclear materials processing facility requires months of effort to design, develop, test, implement, and evaluate.



■ *Figure 2. Nuclear materials processing and transfer between MBAs.*

A framework for evaluating tamper-indicating-device technologies

Padmini Sokkappa
Lawrence Livermore National Laboratory

Decisions about verification technology and implementation options should be made in a way that is logical and defensible based on the available data. This article describes a framework for evaluating tamper-indicating-device (TID) technologies. In addition to serving as a decision aid in making TID technology and implementation choices, the evaluation framework is also an aid in documenting assumptions and technical performance, organizing and focusing discussions on relative strengths and weaknesses of alternative technologies, and guiding further technology development activities.

Purposes of TIDs

The role of a TID is to alert authorities to unauthorized tampering with or opening of a container, package, door, or other objects to which a TID has been applied. TIDs are not designed to prevent unauthorized tampering and can easily be removed or broken. They are exactly what their name implies: tamper-*indicating* devices. They are typically applied to objects such as containers, packages, or doors in such a way that the interior cannot be accessed without damaging the integrity of the TID. (Henceforth, the term container will be used to refer to containers, packages, doors, or other objects to which a TID may be applied.) TIDs generally have identification characteristics, such as a serial number, that serve as a unique identifier. This unique identifier serves to prevent replacement of a violated TID with a new one. It may also serve as a reference for locating records, such as a video image, or other unique characteristics of the TID. Verification of the integrity of a TID includes verifying that it has the correct unique identifier(s).

Verification of TID integrity provides confidence that the situation is as intended. Conversely, a violated TID or nonverification of integrity indicates possible tampering and should stimulate investigative and/or corrective actions. For example, nonverification of a TID on a nuclear material container could be followed by measurements to verify that the contents of the container have not been altered. In addition to an actual violation of TID integrity, conditions that can result in nonverification of integrity include a missing TID, a TID serial number discrepancy, a damaged TID, or an improperly applied TID. Determining TID integrity may be accomplished by a number of means including visual inspection, use of automated readers, and post-mortem examination.

Selection of a TID

The decision about what kind of TID to use requires weighing (i.e., trading off) factors such as cost, relative potential improvements in protection, and operational impacts. The primary reason for using TIDs is to provide a rapid and easy means of verifying that the contents of a container have not been altered after application of the TID. Therefore, severe operational impacts or susceptibility to innocent causes of nonverification of integrity (such as accidental damage, improper application, and misrecording or misreading of unique identifiers) defeat the purpose. Selection of the proper TID for a particular application requires careful consideration of a number of important factors, including

- *Purpose of the TID*: The principal purpose of a TID may be for material control, accountability, and/or protection against covert tampering.
- *Type of container*: The design of the container should accommodate the application of the TID. Availability of access paths to contents of the container that do not impact the integrity of the TID should be considered.

- *Robustness*: The durability of the TID should be appropriate for the physical environment and amount of activity to which the container will be exposed and the duration of use.
- *Reliability*: The level of susceptibility of the TID and associated application/verification equipment to random failure should be acceptable.
- *Ease of application/removal*: Consideration should be given to operational impacts. Removal of TIDs includes the removal of any associated glues or residues.
- *Effectiveness*: Vulnerability of the TID to evasion scenarios such as counterfeiting, resealing, or bypassing must be considered.
- *Interface with other safeguards and security elements*: Consideration should be given to other safeguards and security elements protecting the container. This affects the level of effectiveness required and the credibility of potential evasion scenarios.
- *Cost*: The cost of utilizing a particular TID technology includes the capital costs of the TIDs and any associated equipment, plus any relevant maintenance and manpower costs.

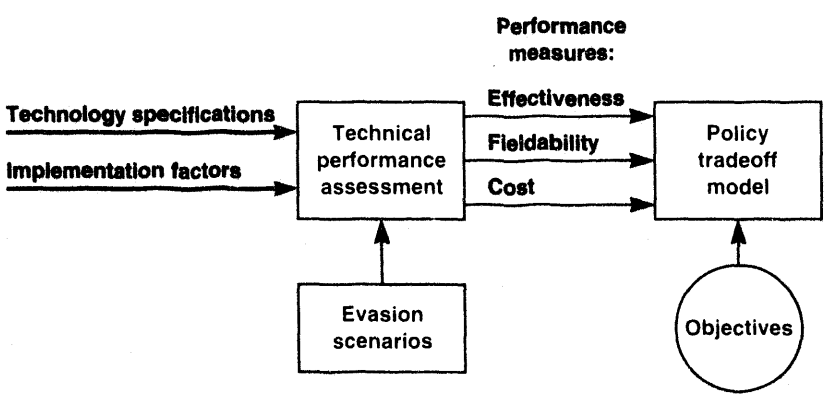
The general framework for evaluating TID technologies is discussed below (see Figure 1). The framework facilitates the logical and systematic consideration of the above factors in selecting a TID for any particular application.

Evaluation framework

The first step in evaluating alternative TID technologies is to identify the alternatives to be considered and to define them *unambiguously*. Unambiguous definition of alternatives requires a mixture of both technology specifications and implementation factors. The goal is to make explicit any key assumptions upon which performance assessments may be based. Technology specifications should include a description of the verification process to which the TID will be subjected, including the security features to be examined and the mechanism for examining these features, definition of any application and/or verification equipment required, and identification of any special requirements (such as surface requirements or power supply) or constraints (such as temperature range) that could limit its use.

Implementation factors that need to be defined include the type of container to which the TID will be applied, the location and method of application, the environment in which the TIDs will be applied (for example, indoors or outdoors), the kind of handling operations to which the containers will be subjected after the TIDs are applied, where and how these containers will be stored, and where the verification of the TIDs will occur (indoors, outdoors, in a laboratory, etc.). If verification of the TID uses pass/fail settings, these settings should be specified. Assumptions about who supplies, applies, and verifies the TIDs, as well as the training these individuals are assumed to have had, should also be defined.

The measures used for evaluating the technical performance of the alternatives should be comprehensive and include all the important factors that differentiate among alternatives and that are of concern to the decision maker. The key performance measures of concern when considering TIDs for a particular application have been divided into three categories—fieldability, effectiveness, and cost. Measures of fieldability include the lead time required for deployment (this includes time to obtain the required number of TIDs and associated equipment and, if applicable, any remaining research and development time); the portability of application and verification equipment; the robustness and reliability of both the TIDs and any associated equipment; and



■ *Figure 1. Framework for evaluating tamper-indicating-device technologies.*

operational impacts such as the time required for application, verification, and removal of the TIDs. Effectiveness refers to the difficulty of evading a TID either by producing a counterfeit (i.e., replacing the TID with a duplicate that is indistinguishable from the original) or accessing the contents of the container without damaging the TID or leaving other detectable signs of tampering. Effectiveness is measured on three scales: the time required to carry out the evasion attempt, the cost of carrying out the evasion attempt, and the likelihood that the evasion attempt would be detected. Cost includes the capital cost of the TIDs and associated application and verification equipment, any maintenance costs, and the cost of any additional manpower requirements resulting from application and verification activities.

Assessing the level of performance of each alternative for each of the performance measures requires careful consideration of the technology specifications and implementation factors. For example, robustness of the TID depends heavily on the handling operations and conditions to which the container will be subjected. Performance related to the effectiveness of a TID depends on the evasion strategies that may be used. The evasion strategies in turn depend on the type and size of the violations of concern. In order to evaluate the effectiveness of a TID, the assumptions about the evasion strategies must be defined. This includes defining the basic steps of the evasion scenario, the level of expertise of the evasion team, and the equipment/materials that the evasion team is assumed to possess. Evasion scenarios for which covert perpetration is not possible given the other safeguards and security elements protecting the containers should not be considered. Evasion scenarios fall into three categories: counterfeit; reseal (removing the TID from the container, accessing the containers contents, and then reapplying the TID in such a way as to be undetectable); and bypass (accessing the contents of the container in a manner that does not affect the integrity of the TID, such as cutting a hole in the bottom of the container). In evaluating the likelihood that an evasion attempt will be detected, the TID verification procedures must be considered. In particular, it is important to know whether the container itself will be examined or just the TID. In evaluating costs, the number of TIDs required must be determined as well as the number of sets of application and verification equipment, including the desired number of backups.

Unless the performance evaluations show one alternative to be superior to all the others on all performance measures, trade-offs will have to be considered in order to make a technology choice. Policy trade-offs among the performance measures (for example, cost or operational impacts versus effectiveness) can easily vary depending on the application context and are closely related to the nature of the violation of concern. The violation of concern is itself a policy question that should be supported by a technical understanding of the military and strategic significance of violations. As noted earlier, the principal purpose of the TID and its interface with other safeguards and security elements are important considerations, and these factors may strongly influence the trade-offs to be made among performance measures. If the TID is to be used broadly as a component in a materials control and accountability program, cost and ease of use may be key performance factors. On the other hand, if the primary purpose of the TID is to protect against covert tampering with a limited number of highly sensitive items, the key performance factors may be effectiveness, robustness, and reliability.

The performance measures, technology specifications and implementation factors that are considered in the framework have been organized into worksheets to facilitate systematic evaluation and documentation of the key factors affecting TID technology choice. Using the evaluation framework can be of value even if policy trade-offs among performance measures are unknown and only limited information about the application context is available. Alternative technologies can be evaluated relative to the performance measures using a specified set of assumptions. The effects of varying the assumptions can also be considered. This type of evaluation serves to identify the strengths and weaknesses of alternative technologies, point out "technology gaps," and provide insights that may guide further technology improvements.

Sealing the Type 30B uranium hexafluoride cylinder

Joseph Dooley
Oak Ridge National Laboratory

The Type 30B uranium hexafluoride (UF_6) cylinder is typically used for transport of low-enrichment (less than 5%) UF_6, normally between the enrichment plant and the fuel fabricator's facility. The cylinder is one of a family of standardized containers used for UF_6 traffic.[1] The cylinder nominally holds 2.5 tons of UF_6 and has an empty weight of about 1400 pounds.

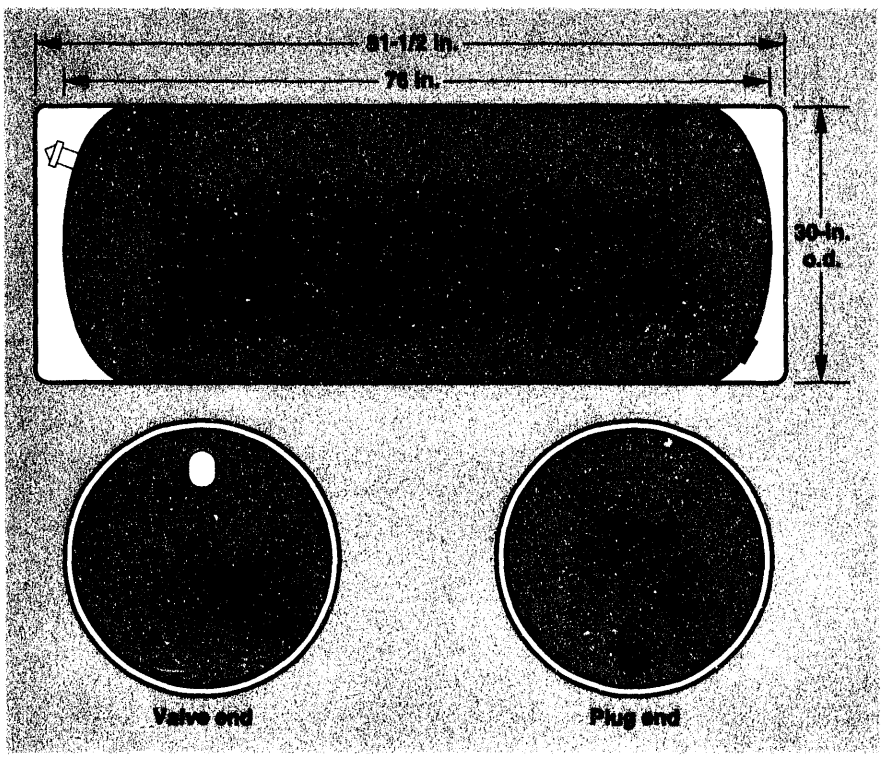
Service environment

The 30B cylinder (Figures 1 and 2) is subjected to large temperature excursions in routine service. At the producing facility, the cylinder is filled with liquid UF_6 of about 220°F, and this liquid rapidly heats the steel container to about the same temperature. After filling, the cylinder is permitted to cool for about 3 days to solidify the UF_6, usually in an open-air yard. In U.S. practice, the valve is sealed for tamper indication while the cylinder and valve are still hot.

For long-distance transport, the valve cover is installed and the cylinder is lifted into an "overpack," which fits closely about the cylinder, providing about 6 in. of padding and insulation on all sides. The overpack is split horizontally, with latches around its perimeter to hold it shut. The overpack also has loops on both halves to permit the installation of tamper-indicating devices. At its destination, the cylinder is removed from the overpack and may be stored for an extended time, either in an open yard or shed.

If the cylinder contents must be sampled as part of the receiving process, the cylinder is moved to an autoclave (steam-heated enclosure), where the valve cover and port cover (under the seal) are removed. Then a line is connected to the port, and the autoclave is closed and heated to liquefy the contents again (about 220°F). After withdrawal of the sample, the cylinder is reclosed, resealed, and returned to a cool-down pad, and eventually returned to storage.

Several heating and cooling cycles are therefore inherent in the service life of the 30B, which creates a difficult and demanding service environment for the tags and seals.



■ *Figure 1. Schematic of the UF6 cylinder model 30B.*

Description

The 30B is made from 1/2-in.-thick carbon steel. The dimensions of the 30B UF_6 cylinder, shown in Figures 1 and 2, are nominally 30 in. diameter by 81-1/2 in. long. It has slightly domed ends, overhung by skirts on each end.

There are two penetrations into the cylinder, the valve at the top of one end and a drain plug at the bottom of the opposite end. The valve is used to fill and empty the cylinder in normal operation. The drain plug is removed only to drain and dry the cylinder after decontamination or after hydrostatic pressure testing for initial or periodic certification.

A nameplate spot-welded to the valve end of the cylinder identifies the cylinder during normal service tracking and provides other technical data about the cylinder.

A valve cover, made from 11-gage steel (approximately 1/8 in. thick), is usually provided with each cylinder. The cover is basically a box that covers the valve, fits within the overhang of the cylinder skirt, and is secured by two eyebolts that thread through tabs on the end dome and into the cover from both sides. One version of the cover uses only the bolts to secure it, while another version uses a pair of small hooks in conjunction with the bolts to secure the cover.

■ *Figure 2. Type 30B UF6 cylinder. Valve is above name plate on end facing camera. Valve cover is on the ground at the near end.*

Seals test-fitted on the 30B

By virtue of the limited number of entry points to the cylinder, few provisions for seals have been made or are needed. Simple and effective tamper-indicating devices have been used routinely in the enrichment industry to seal the drain plug and valve.

The drain plug can be sealed with any type of loop seal, such as in Figure 3 with an E-cup-and-wire seal. Seals such as cobra, python, SLITS, or an electronic identification device were also fitted on the drain plug. Figure 3 shows one permissible version of the drain-plug sealing loop, a loop actually welded to the plug. The other version is the use of a

■ *Figure 3. E-cup-and-wire seal in place on Type 30B cylinder drain plug.*

plug with a small-diameter hole drilled through the wrench flats, which can permit threading of loop seals.

The skirt's extension beyond the dome ends of the 30B cylinder provides a protected area for seals to be attached. This reduces the probability for accidental damage, provided that seals or tags use loops with little slack, thus keeping the seal sheltered.

The valve itself may be sealed in a number of ways, several of which were fitted to the 30B cylinder. The shape of the valve permits a transparent bag to be secured around the entire valve assembly using any loop seal as a drawstring. Figure 3 shows the E-cup-and-wire seal in the application. Space inside the valve cover will accommodate any of the loop seals.

The entire valve and port cover may be enclosed in a shrink-wrapped seal inside the valve cover; however, the shrink wrap must be able to tolerate the peak temperature of about 220°F. Seals derived from tamper tapes also can be employed on the valve port cover if care is taken to place the bar code so that it can be read.

Some seals do not work on the 30B cylinder. Because of extreme thermal cycling and consequent rusty condition of the external surfaces, tags or seals that rely upon direct adhesion are not suitable. The port cover and valve body, however, are exceptions because their aluminum bronze construction usually has a good surface for adhesion. The EID bolt seal cannot be employed because no appropriate bolts exist on the 30B cylinder, although the seal might be used on the overpack bolts. The EID loop seal, whose electronics may not survive the thermal cycling, is not likely to be useful on the 30B.

Application pointers

Multiple layers of tags or seals can be used, but the exact combination should be chosen carefully. For example, a seal applied to the valve itself is not readily accessible for inspection if the valve cover is also sealed, unless the valve cover seal is broken, replaced, and documented. The prescribed level of inspections for verification of cylinder identity and condition must be consistent with practicality.

The choice of a tag and seal also fulfills two purposes. First, it identifies the cylinder and its contents. Second, it helps ensure integrity of contents during the shipment-storage-use sequence. A logical conclusion is that cylinder identity could be maintained primarily by the drain plug tag/seal while integrity of contents could be ensured through the transport sequence by less complex tags/seals. Using a more elaborate seal could make the shipment more readily identifiable in some scenarios.

Essentially, the seals and tags are applied so as to establish the identity of the cylinder and its contents as early as possible in the transport-storage-use sequence. Negotiations would define the specific path that the blended material takes and the degree of assurance that the parties desire, including the points at which the sampling occurs.

For each sampling, the cylinder will experience unsealing, heatup, a valve open/reclose cycle, resealing, and cooldown. Because the drain plug is not opened during the sequence, that area is a good location for one of the robust tags or seals that establishes the identity of the container throughout the sequence. SLITS, cobra, python, and the E-cup-and-wire seal are likely candidates provided their components and features are able to withstand the service environment. The E-cup-and-wire seal, already used in UF_6 traffic, has wide acceptance in the industry.

The valve can be secured immediately after the cylinder-filling operation. From an operations viewpoint, common sense would have the combination tag and seal be as similar to existing commercial practice as the nature of the sequence permits. Tamper tape or shrink wraps could be used on the valve, augmented by the use of a bag with one of the more

robust tags and seals as a drawstring, a combination very much like existing practice. In this case, all the loop-type tags/seals, including the EID loop, could be used because the valve seal is broken before heating or is installed after cooling.

As the testing at ORNL showed, the valve cover accommodates any of the loop seals. However, sealing the valve cover would be redundant. The cover is normally in place only when the cylinder is being moved; it is designed to be removed in seconds to verify the integrity of any tag/seal applied to the valve itself. If the cylinder is to be transported a significant distance, the cylinder is placed in an overpack, and the valve cover is not accessible without opening the overpack, which may itself be sealed. Thus, little is gained by sealing the valve cover when other tags/seals are applied.

The overpack offers possibilities for using the full spectrum of the tags and seals, except for shrink wrapping. For example, eyes on the halves of the overpack permit application of any of the loop seals, and a long, continuous, sealing loop could permit single-point inspection of the overpack seal. The latches on U.S. overpacks permit the attachment of the EID bolt monitor. Tamper tapes are also viable for the overpack. The E-cup-and-wire seal is routinely used for overpack seals.

Reference

1. ANSI Standard, Uranium Hexafluoride Packaging for Transport, ANSI-N14.1-1991.

Sealing the AT-400R container

Robert Courtney and Ken Ystesund
Sandia National Laboratories

The AT-400R container for shipping/storage of fissile materials is under development at Sandia National Laboratories in support of the program for Safe and Secure Dismantlement (SSD) of nuclear weapons. (In some circles, the SSD program is now known as the Cooperative Threat Reduction program.) The container was evaluated to demonstrate the utility of seals developed by the DOE national laboratories and the Defense Nuclear Agency (DNA).

■ *Figure 1. E-cup-and-wire seal applied to (left) the overpack locking ring security bolt and (right) the overpack lid bolts on the AT-400R container.*

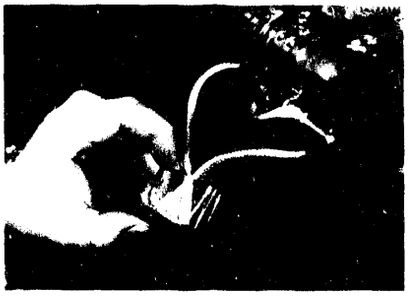
Description

The present AT-400R-series design consists of an outer container (overpack) and two possible configurations for the inner containment vessel, both capable of being used for transport. The inner containment vessel of the AT-402R has a bolted lid that allows easy access to the contents; for long-term storage conditions, the AT-401R inner lid is welded to the inner containment vessel. The inner containment vessel used during this demonstration and evaluation was the storage version with a welded lid; consequently, there were no features that would allow the application of loop-type seals.

Although the design features of the AT-400R container for the SSD Program are well established, the overpack was slightly modified here to accept the E-cup-and-wire seal normally used on the DOT 6M container and the various seals developed by the participating national laboratories and the DNA. Minor modifications were made to the container:

- A locking ring with a security bolt was applied to the lid of the overpack. The security bolt is similar to the one used on the DOT 6M container.
- The heads of the 12 overpack lid bolts were drilled to accommodate the loop-type seals used in the demonstration and subsequent evaluations.
- The rim edge of the inner containment vessel was ground flat in one location to permit easier application of Pacific Northwest Laboratory's tamper tape seal.

(Any proposed modifications for the AT-400R container will be coordinated with the Sandia design group and may result in a change in container designation.)

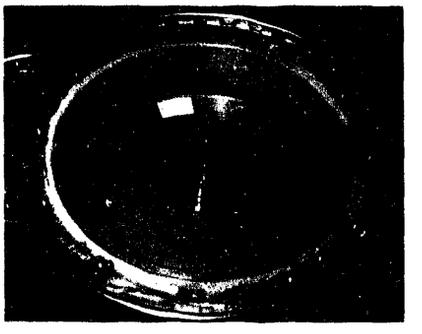


■ *Figure 2. Secure loop inspectable tag/seal applied to the overpack locking ring security bolt.*

Tagging and sealing of the AT-400R

Table 1 shows the facility and/or agency responsible for applying specific seal technologies to designated locations of the AT-400R container for these evaluations.

To facilitate the application of the tamper tape to the inner



■ *Figure 3. Tamper tape applied to the inner containment vessel.*

containment vessel, a flat region approximately 2 in. long was ground on the outer edge of the lid rim. A flat region to accommodate the tamper tape could become part of the container fabrication specifications.

The drilled bolts that secure the lid to the overpack provided a convenient method of applying all types of loop seals. However, several washers had to be used to raise the bolt heads above the reinforcing ring to achieve the clearance necessary to apply the loop-type seals. The final AT-400R design is expected to have beveled edges on the countersunk holes in the reinforcing ring, which will facilitate seal installation.

The tamper tape, when used in conjunction with the shrink-wrap film, can serve as a reference point for seal verification during subsequent inspections of the shrink-wrap patterns. This particular layered tamper detection scheme does not involve modifications to the inner containment vessel.

Handling of the AT-400R

Procedures have not been established for the AT-400R container to handle highly enriched uranium (HEU). However, some general guidelines can be suggested. If the containers are to be stacked, there is a potential danger of damaging seals applied to the top of the container. Similarly, there is a possibility of damaging a seal if it is permitted to hang on the side of the container. The SLITS and the cobra seal can utilize protective covers that may eliminate or minimize damage to the seal body.

Application scenarios

The most likely sealing locations on the AT-400R container and associated seal technologies are listed in Table 1. The shrink-wrap seal was not suggested for use on the outside container because of the high probability for damage. Use of the tamper tape over the locking ring and a loop seal through both the locking ring bolt and the bolts securing the lid provide a layered protection scheme that would provide greater assurance that the container had not been compromised. There is the possibility of using only one loop seal to tie the locking ring security bolt to the bolts used to secure the lid to the container. Because of their dimensions, the cobra seal, the E-cup-and-wire seal, and the SLITS are the leading candidates to be installed on the overpack lid bolts if the containers are to be stacked. The current python body is too large to be applied in this manner.

The two seals best suited for application to the inner containment vessel include tamper tape and shrink wrap. Either could be used alone, but together they provide a complementary, layered tamper detection system. Typically, the use of a layered tamper detection system enhances security while providing a backup seal if one is accidentally damaged.

Table 1. Seal applications.

Container location	Seal technology	Applying agency or facility
Overpack locking ring	Tamper tape (see page 27)	Pacific Northwest Laboratory
Overpack locking ring security bolt	E-cup-and-wire seal (see Figure 1, page 18)	Pacific Northwest Laboratory
	Secure loop inspectable tag/seal (see Figure 2, page 18)	Defense Nuclear Agency/ BDM Federal
	Cobra seal (see page 26)	Sandia National Laboratories
	Bolt-type electronic identification device (see page 29—applied as on DOT 6M)	Lawrence Livermore National Laboratory
Overpack lid bolts	E-cup-and-wire seal (see Figure 1, page 18)	Pacific Northwest Laboratory
	Secure loop inspectable tag/seal	Defense Nuclear Agency/ BDM Federal
	Python seal (see page 25)	Sandia National Laboratories
Inner containment vessel	Tamper tape (see Figure 3, page 18)	Pacific Northwest Laboratory
	Shrink wrap (see page 30)	Sandia National Laboratories

Sealing the DOT specification 6M container

Halvor A. Undem
Pacific Northwest Laboratory

Containers manufactured to U.S. Department of Transportation (DOT) Specification 6M have been used by DOE in the United States to ship fissile materials. The *Highly Enriched Uranium (HEU) Transportation Study*[1] suggested that they might also be used if HEU were to be shipped directly from the Russian Republic to the United States.

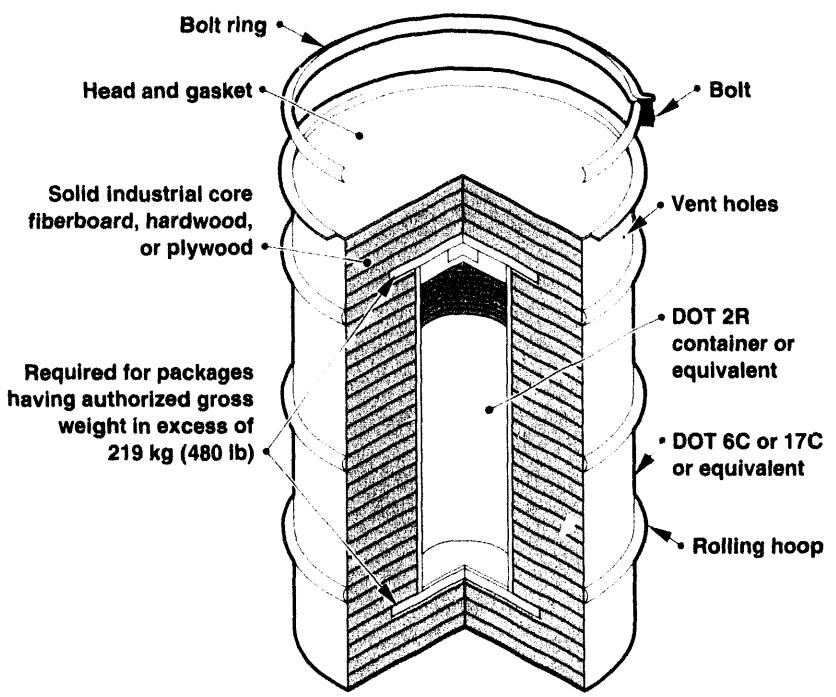
Description and transportation requirements

The DOT 6M container meets regulatory requirements for packaging of certain fissile materials as prescribed in International Atomic Energy Agency (IAEA) Series 6, 1973 Edition, and U.S. regulations. Specification 6M requires certain parameters for the container's physical construction, authorized contents, marking and labeling, and other general conditions.

The containers are steel drums ranging in size from 10 to 110 gallons. Standard construction is shown in Figure 1. The drum also contains an inner container constructed to DOT Specification 2R (Figure 2). It is this inner 2R container that actually holds the fissile material.

The authorized fissile contents of the DOT 6M include uranium-233, uranium-235, and various isotopes of plutonium. However, there are restrictions on the allowable quantities of any of these, depending on the form of the material (metal or alloy vs compound), particle size, the ratio of hydrogen to fissile atoms in the inner container, decay heat rates, and isotopics. For example, uranium-235 shipments are limited to a maximum enrichment of 93.5%, and quantities of 7.2 to 13.5 kg in metal or alloy form.

Other general conditions for use of the DOT 6M include documentation requirements for use of the 6M certification, quality control documentation, registration compliance, and others.[1] The DOT 6M certificate provides authorization to transport fissile materials in the 6M certified container only "from point of entry to final destination within the United States and from point of origin in the United States to point of exit."[1] However, as stated earlier, the specification currently satisfies IAEA regulations. The current certification expires on February 28,1994.



■ *Figure 1. Typical assembly detail for DOT 6M container.*

Tagging and sealing of the DOT 6M

The DOT 6M specification explicitly calls for the closure device on the container to "have means for the attachment of a tamperproof lock wire and seal or equivalent."[1] A standard tamper-indicating device (TID) for the DOT 6M is the E-cup seal with lock wire (see page 24).

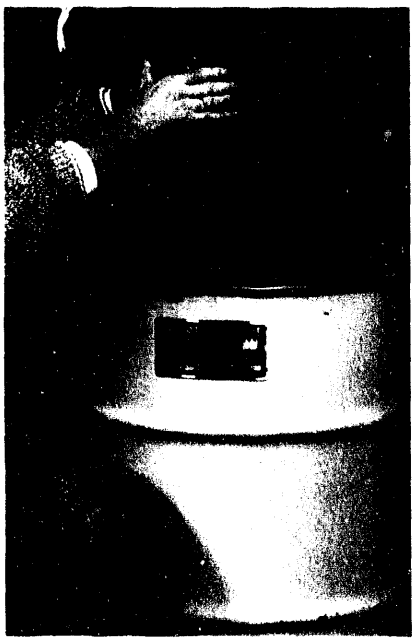
Equivalent TIDs developed by the U.S. government for arms control and nonproliferation purposes may also be useful in sealing the DOT 6M container. "Loop and lock" concepts, similar to the E-cup-and-wire principle, include the SLITS (secure loop inspectable tag and seal) device developed by the Defense Nuclear Agency (page 28), the electronic loop and seal device developed by Lawrence Livermore National Laboratory (page 29), and the python and cobra seals developed by Sandia National Laboratories (pages 25 and 26). Although similar to the E-cup and wire in installation, these arms control–developed seals provide a far more sophisticated unique identification (i.e., tagging) function, as well as highly sophisticated tamper indication.

There are also arms control TIDs that provide an equivalent tagging and sealing function without using the "loop and lock" principle. Examples include Livermore's bolt-on electronic identifying tag (page 29), Pacific Northwest Laboratory's tamper tape seal (page 27), and Sandia's shrink wrap (page 30). Some of these TIDs and their operation, as well as those mentioned above, were described in a previous issue of this publication.[2]

Handling of the DOT 6M

Handling requirements for DOT 6M containers vary with respect to organizations (Pacific Northwest Laboratory vs Oak Ridge National Laboratory, for example) and within organizations, depending on the content of the container and criticality requirements.

Loading, handling, and shipping requirements are developed at local sites in compliance with local, state, and federal laws with respect to environment, safety, and health, as well as control of radioactive substances and/or fissile materials. These requirements are generally documented in the form of local orders or procedures. An example from Hanford Operations is Procedure Z0-200-520.[3]



■ *Figure 2. Inner container (DOT Specification 2R) that holds fissile material.*

The purpose of the Hanford procedure is to provide instructions to workers for inspecting DOT 6M containers and subsequently loading them with canned nuclear material, in this case, plutonium oxide. It deals explicitly with precautions and limitations, prerequisite actions, tools, equipment and material requirements, and performance. Material Control and Accountability (MC&A) and Safeguards and Security (SAS) requirements must be accommodated as well.

Precautions and limitations include concerns for criticality and safety. Among the criticality requirements are minimum spacing restrictions, limitations on the number of containers that can be open at any one time, and limitations on the amount of fissile material per the DOT 6M specification. The maximum decay heat is also cited.

Another section, prerequisite actions, includes balancing current calibration for MC&A purposes. Tools, equipment, and material include references to other procedures and documents, and complete lists of required tools and safety equipment. One of the procedures, Z0-200-028, *Move Nuclear Material*,[4] includes

all site transportation requirements for moving the DOT 6M when loaded, including the use of specially trained crews.

Finally, the performance section of the procedure contains detailed, step-by-step instructions for inspecting, labeling, and loading the DOT 6M container. Explicit instructions are provided for inspecting the shipping container, labeling the container, packing the containment vessel, and closing up the DOT 6M container.

The inspection procedure, for example, includes 23 explicit steps, some with substeps, including Quality Control and Radiation Protection Technician surveys. Labeling the shipping container involves 7 steps. Packing the containment vessel requires 18 steps and 5 criticality warnings. Finally, closing up the DOT 6M container calls for 18 steps, including application of TIDs which are controlled and logged.

Application scenario

Although current plans call for blending of the HEU to low-enrichment uranium (LEU), and subsequent shipment of LEU to the United States, there still exists the issue of transparency measures with respect to Russian HEU before it is blended.

The DOT 6M could be applied in this scenario, and used to transport Russian HEU from dismantlement facilities to conversion and blending facilities. However, the use of the container and TIDs on the container cannot be separated from the MC&A and SAS infrastructure in which the container is used. The problem must be worked as a whole. DOE, with its weapons complex, fissile materials handling, and tags and seals expertise, remains a prime U.S. resource in examining issues related to MC&A, SAS, and the related use of TIDs as this important transaction is executed between the Russian Republic and the United States.

References

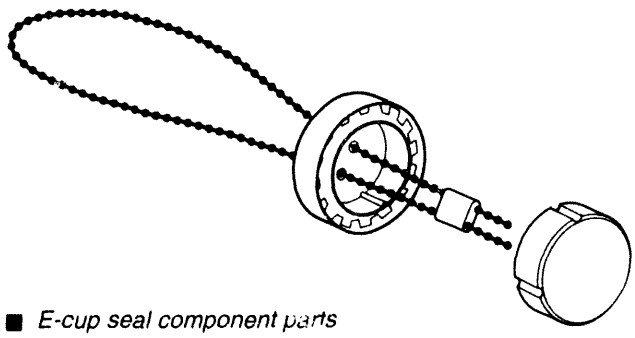
1. Department of Energy, Office of Arms Control and Nonproliferation, *HEU Transportation Study*, Appendix D-1 (September 1992).
2. *Verification Technologies*, Third Quarter 1992, Department of Energy, Office of Arms Control and Nonproliferation, DOE/DP/OAC/VT-92B.
3. *Plutonium Finishing Plan, Environmental Waste Operations, Inspect and Load DOT-6M Containers*, Pacific Northwest Laboratory, Westinghouse Hanford Operations, Hanford, WA, Z0-200-520, Rev/Mod E-0 (June 1992).
4. *Plutonium Finishing Plan, Environmental Waste Operations, Move Nuclear Material*, Pacific Northwest Laboratory, Westinghouse Hanford Operations, Hanford, WA, Z0-200-028, Rev/Mod E-2 (April 1992).

Appendix

Tag and seal technologies evaluated at the Portsmouth Gaseous Diffusion Plant demonstration

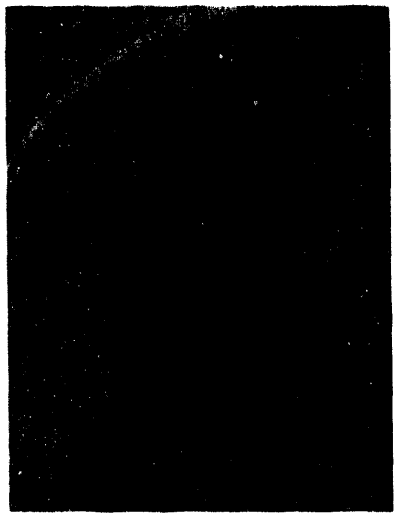
E-cup-and-wire tamper-indicating seal

The conventional E-cup-and-wire combination is used as a tamper-indicating device for routine shipments of 30B UF_6 cylinders within the United States. Each E-cup contains a stamped number that the shipper provides to the receiver, and the receiver verifies the seal number and that the seal is intact when the containers arrive at his facility. The E-cup is formed by a press-fit of two separate halves that clamps to a wire holding a plastic bag around the cylinder valve.



■ *E-cup seal component parts*

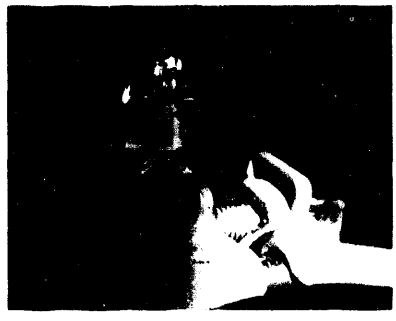
■ *E-cup seal applied to Type 30B UF_6 container*



■ *E-cup seal applied to DOT 6M container*

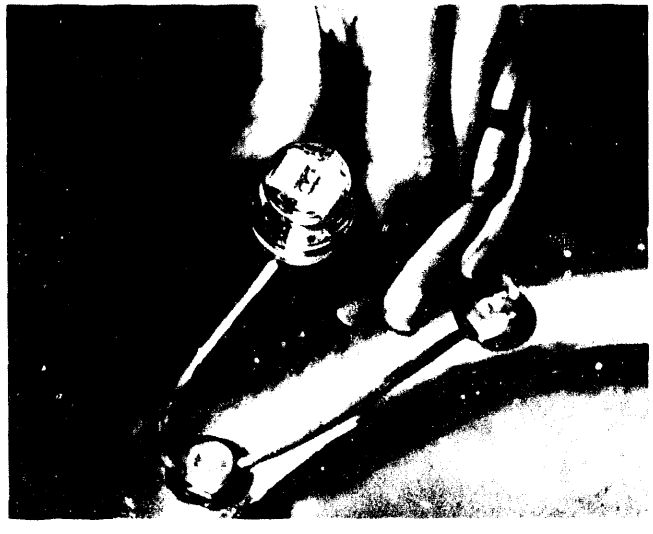
Python seal

The python seal is a passive fiber-optic loop seal consisting of a clear, polycarbonate seal body and a loop of fiber-optic cable. Installation is effected by looping the cable ends through or around the object to be sealed and terminating the loop in the seal body. At installation, a unique pattern is created on the seal face at the ends of the fiber-optic bundle. This pattern is photographically recorded. For an additional level of security, the seal includes a reflective particle tag that is photographed with the optical fiber pattern. Verification of seal integrity after installation is accomplished by comparison of an image obtained at the time of verification with that obtained at installation. The verification function can be performed automatically using a computer-based reader and correlator, or by an operator making visual comparisons of photo images.



■ *Python seal applied to DOT 6M container*

■ *Python seal applied to Type 30B UF_6 container*

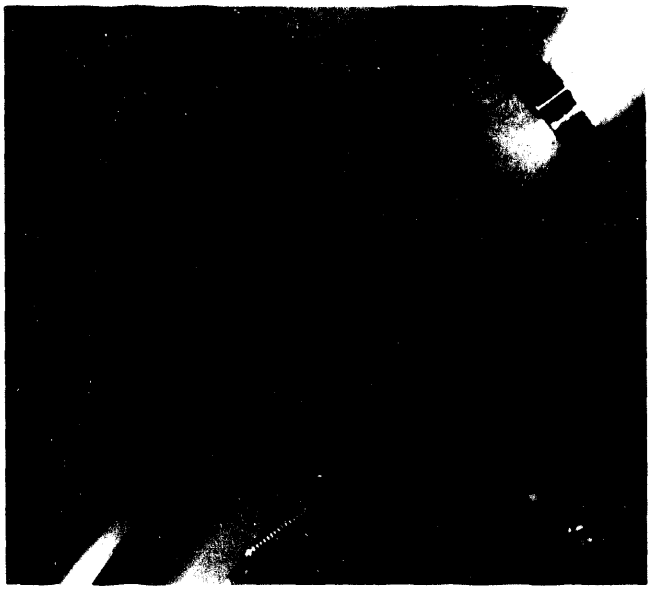


■ *Python seal applied to AT-400R container*

Cobra seal

The cobra seal is a passive fiber-optic loop seal consisting of a clear, polycarbonate seal body and a loop of fiber-optic cable. Installation is effected by looping the cable ends through or around the object to be sealed and terminating the loop in the seal body. At installation, a unique pattern is created on the seal face at the ends of the fiber-optic bundle. This pattern is photographically recorded. Verification of seal integrity after installation is accomplished by comparison of an image obtained at the time of verification with that obtained at installation. Seal images are recorded with a still video photographic verifier and can be printed for manual comparisons or displayed on a video monitor.

■ *Cobra seal during application to AT-400R container*



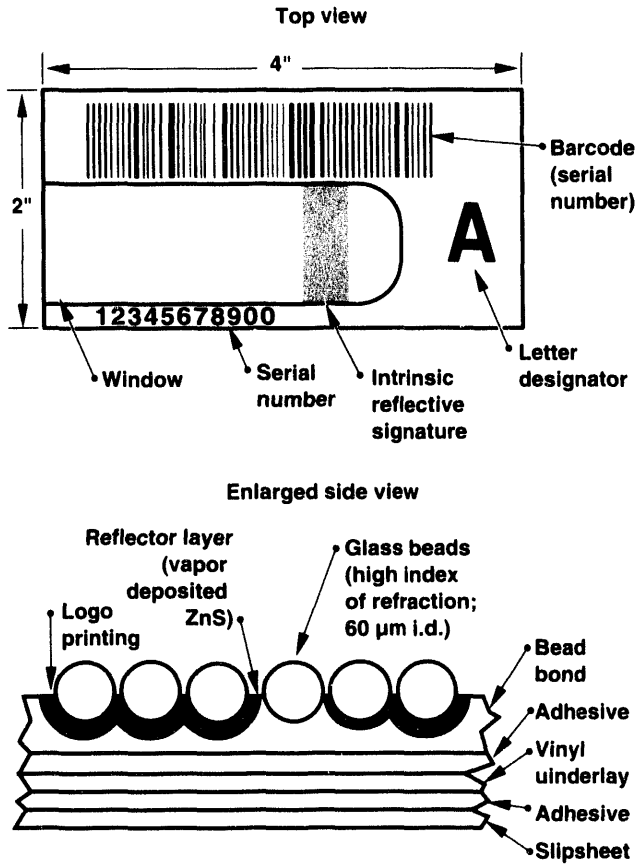
■ *Cobra seal applied to DOT 6M container*

■ *Cobra seal verification reader*

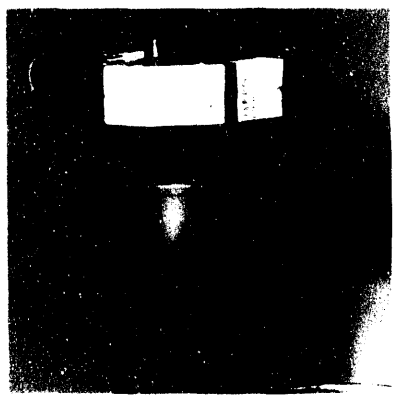
Tamper tape

A tamper tape is an adhesive-backed label that possesses various tamper-indicating, transfer-resistant, or counterfeit-resistant properties. Commercial tamper tapes are composed of multiple layers of various polymers, papers, patterns, devices, or other materials—all mixed with layers of adhesives. Tampering activities can easily cause observable changes in tape structure, such as separation of layers, discoloration, or bubbling. Designs have incorporated material based on coated glass beads embedded in a brittle bonding layer that, in the event of tampering, would be disrupted and cause distortion of a logo pattern reflected from a layer beneath the beads; printed serial numbers and accompanying bar codes; and an adaptation of reflective particle tagging technology, which makes use of materials containing optically reflective particles to generate complex signatures.

■ *Tamper tape seal applied to AT-400R container*



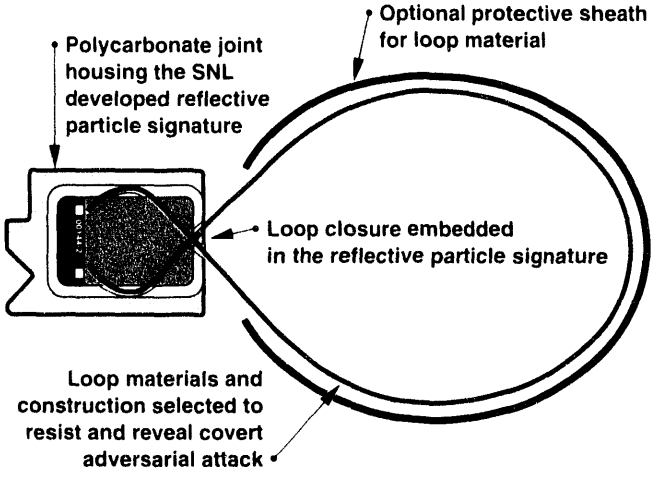
■ *Tamper tape seal component parts*



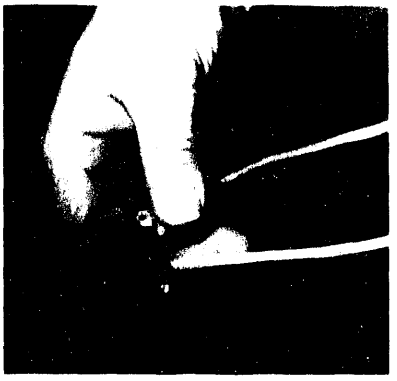
■ *Tamper tape seal applied to DOT 2R container*

Secure loop inspectable tag/seal (SLITS)

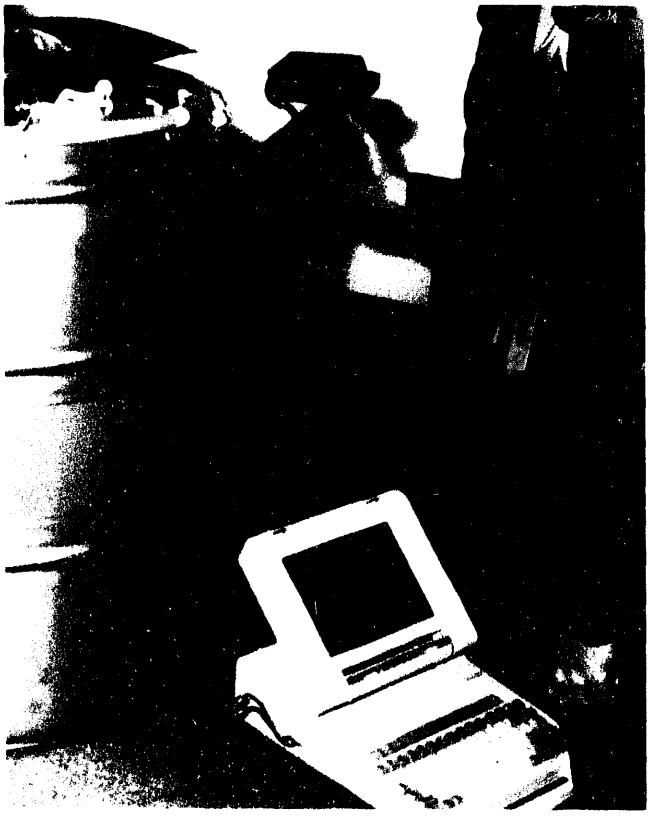
The SLITS is a loop tag and/or seal that allows high-confidence, on-site, tamper determination. SLITS incorporates a loop that, at installation, is wrapped around the item to be secured, and whose ends are then firmly attached to an optically clear seal (joint) block. The loop ends are embedded in an epoxy/reflective particle mixture within the block. As the epoxy hardens, the positions of the reflective particles and loop fibers become fixed and create a unique optical pattern when illuminated. The materials composing the loop make tampering, such as splicing, readily apparent. The seals are highly resistant to seamless chemical bonding and facilitate both tactile and visual inspection. The identity and integrity of the seal inside the joint block are established by correlation of video images taken at the time of inspection with images taken at the time of construction of the tag/seal. Correlations are performed automatically by a video recording system.



■ *SLITS seal component parts*



■ *SLITS seal applied to DOT 6M container*

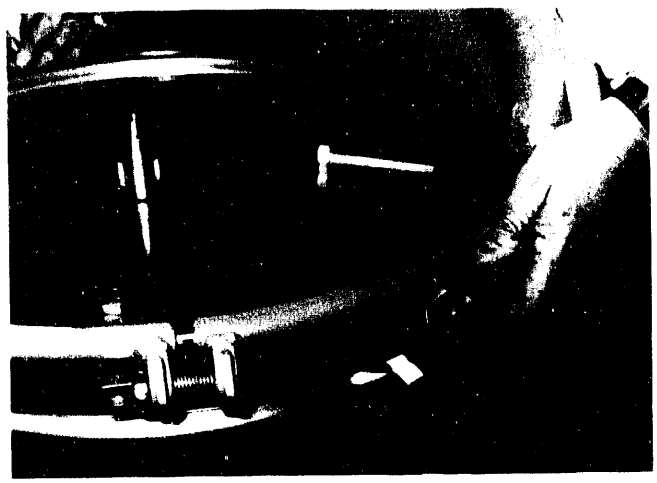


■ *SLITS seal verification reader*

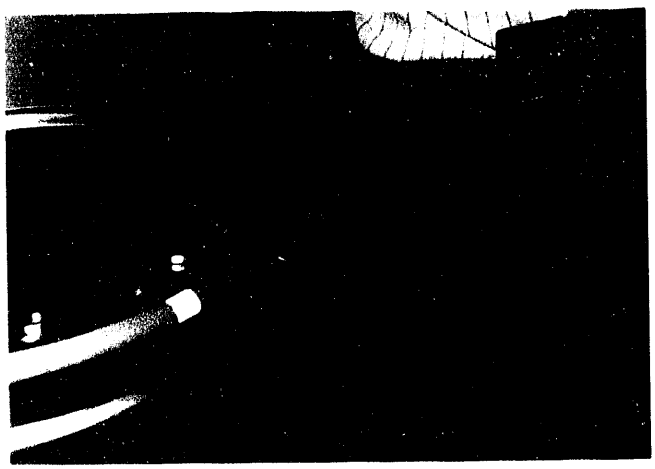
Bolt and loop electronic identification devices

Electronic identification devices (EIDs) are electronic tags that are attached to accountable objects. To authenticate the identity of a tag, a small hand-held reader is used to send a random number to the tag for encryption. The tag's encryptor encodes the received random number using internal keys. A response that is unique to the internal keys is then transmitted back to the reader. Foreknowledge of a tag's keys permits verification of a correct match of tag input and output data. The heart of the electronic tag is a microprocessor chip that holds the encryption keys and communicates with integrated tamper sensors and with the outside world. EIDs have been fabricated as a bolt-type tag and as a fiber-optic-type seal. The bolt-type tag consists of an EID mounted on a unit that can be screwed onto the bolt. Attempted tampering or transfer of the bolt is recorded. The fiber-optic-type seal is a device that performs the same function as the bolt tag, but employs a fiber-optic loop seal that can strung through one or several containers.

■ *Bolt-type EID applied to DOT 6M container*



■ *Fiber-optic EID seal and verification reader applied to DOT 6M container*

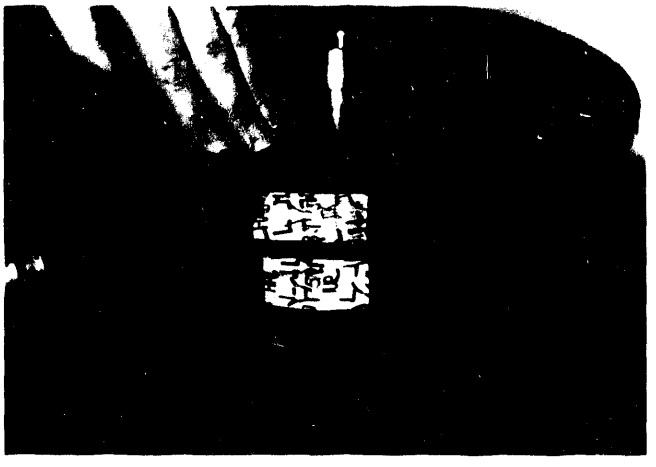


■ *Bolt-type EID verification reader*

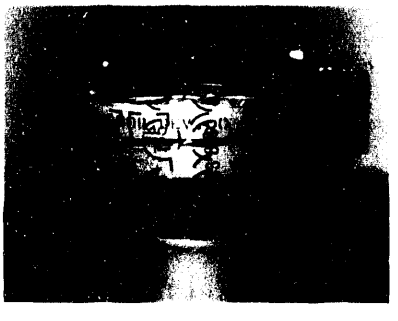
Shrink-wrap seals

Shrink-wrap seals are typically prepared using two layers of a clear thin film that are wrapped around the object to be sealed. When heat is applied the layers of shrink film having differing ink patterns tighten non-uniformly around the object being protected and in many cases conform to its surface. The spatial relationship between the patterns on each layer is unpredictable for each seal. It is the random shrinkage of the overlapping patterns that forms a unique fingerprint for the seal, which precludes removal and replacement with an identical seal.

■ *Shrink-wrap application procedure*



■ *Shrink-wrap seal applied to AT-400R inner container*



■ *Shrink-wrap seal applied to DOT 6M inner container*

DATE
FILMED
5/19/94
END