SAND2015-4251C

TAMPER-INDICATING ENCLOSURES, A CURRENT SURVEY

Heidi A. Smartt and Zoe N. Gastelum
Sandia National Laboratories, Albuquerque, NM, USA

Abstract:

Tamper-indicating technologies are critical elements of verification regimes, used extensively as part of containment and surveillance (C/S) equipment and to support Chain of Custody (CoC), thus providing confidence that equipment, information, and materials of concern remain uncompromised by adversaries. Active or passive, these technologies can indicate penetration either through recognized openings such as hasps (referred to as Tamper-Indicating Devices (TIDs)), or through panels or entire volumes (referred to as Tamper-Indicating Enclosures (TIEs)). Research on TIDs has been more prevalent than on TIEs, although both are equally significant for tamper indication. Technologies have become available that could aid adversaries in attacks against both TIDs and TIEs, leaving the verification community at a disadvantage. This paper will review the current landscape of TIEs as they are applied in the verification community and address some of the associated challenges.

Introduction

A tamper-indicating device (TID) is a device designed to leave non-erasable, unambiguous evidence of access or entry. A TID has also been defined as a device that, "because of its structure, reveals violations of containment integrity"[i] in which TID "containment integrity" can refer either to the TID's body or the actual enclosure opening mechanism to which the TID is attached. TIDs are used in international safeguards as part of a broader containment and surveillance (C/S) regime to provide "physical evidence of tampering with C/S or other safeguards equipment"[ii] or in arms control to support Chain of Custody (CoC).

While TIDs are well-suited to be applied over hasps or other enclosure openings, they are not able to provide evidence of an adversary by-passing that opening completely, for example by drilling through the side of an enclosure. Tamper-indicating enclosures (TIEs), on the other hand, are intended to detect precisely those scenarios. TIEs are defined as "enclosures that… [result] in physical evidence of [a] tamper attack."[iii] TIEs can be used as containers in order to provide more complete tamper-indication coverage for the contents, or can alternatively serve as the body of a TID as an additional tamper-indicator.

TIEs can be classified into various categories, depending on their function, verification method, or other characteristics. This paper seeks to define the scope of TIEs, and provide an overview (not meant to be comprehensive) of currently available TIE technologies for safeguards and arms control as understood through various categorization schemas. Note that the categorization can be highly overlapping. We will also discuss advantages and disadvantages of TIE approaches at a high level.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2015-XXXXC

TIE Scale of Use

TIEs can be incorporated into a verification system at various sizes or scales. For the purposes of this paper, we will describe these scales of use in three categories: TIEs as TID or equipment bodies, TIEs as monitored item enclosures, and TIEs as rooms.

TIEs as TID or Equipment Bodies

There are several scales at which TIEs can be used. At the smaller end of the spectrum, TIEs can be used as the housing for TIDs (where often the end of a fiber optic or wire terminates in loop type TIDs) or other equipment (such as surveillance technology) to provide additional tamper detection. We make this distinction because some TID bodies do not have TIEs as an integral part of their structure. Examples of TIEs as TID or other equipment bodies include:

- TID/equipment with hematite embedded, which upon penetration into material would cause irreversible disturbances in the particle distributions.

Figure 1: Cobra 5 Seal with Embedded Hematite. Photo courtesy Sandia National Laboratories.

- TID/equipment using difficult to replicate material or patterns in body such as swirled plastics or, patterned composites.
- TID/equipment using frangible materials such as ceramic or glass. Frangible materials break into fragments rather than retaining cohesion and thus a tamper attempt is prone to result in difficult-to-reassemble fragments. Sandia National Laboratories' and Savannah River National Laboratory's Ceramic Seal,[iv] and the Glass Seal under development with IAEA, are examples of TIDs with frangible materials (Figure 2).

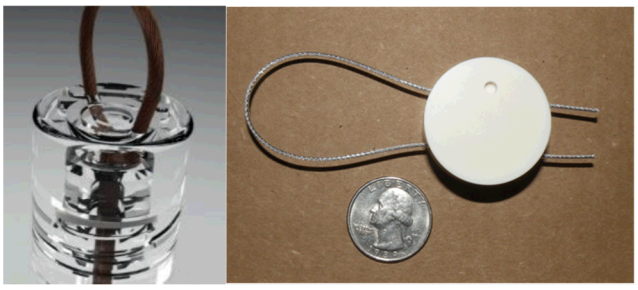

Figure 2: (Left) IAEA Prototype Glass Seal[v]; (Right) Sandia National Laboratories' and Savannah River National Laboratory's Ceramic Seal

- TID/equipment using active or passive fiber optic strands within body walls, for example Canberra's Electronic Optical Sealing System (EOSS seal) and DCM-C5 camera (Figure 3). Optic fibers are thin strands made of glass or plastic that can transmit light from one end to the other, across long lengths and curves. By incorporating optical fibers into the walls of an enclosure, cuts or replacements of the fiber can be detected via a stoppage of transmission in light from one end of the fibers to another.
- TID/equipment using anodized aluminum, which is produced by applying an electrical or chemical process to aluminum, thus producing a layer of aluminum oxide on the material that has a different texture and crystal structure than the material below. Cuts or other disruptions to a container made of anodized aluminum should be apparent due to the show-through of the aluminum layer from below, and the disruption of the oxide layer on the surface. Examples include the DCM-C5 camera (Figure 3) and the Remotely Monitored Sealing Array (RMSA).

Figure 3: DCM-C5 constructed using Anodized Aluminum. Image courtesy Canberra.

TID/equipment using special coating or paint, such as Savannah River National Laboratory's transparent coating that is excited by ultraviolet (UV) light. (Figure 4: Ceramic Seal illuminated with UV Light Revealing Fluorescent Coating (Savannah River National Laboratory)

-).

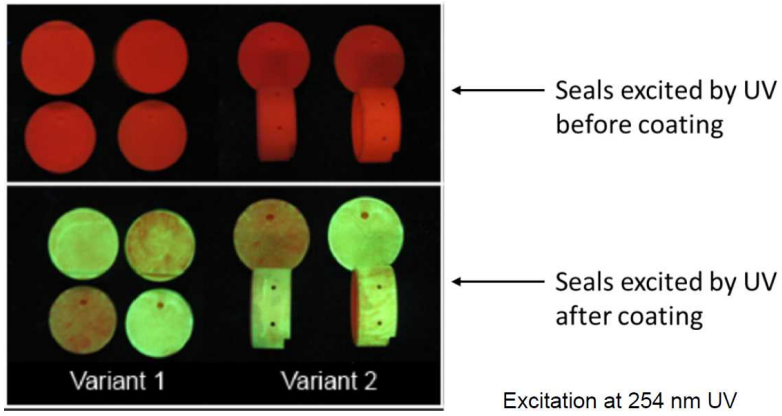

Figure 4: Ceramic Seal illuminated with UV Light Revealing Fluorescent Coating (Savannah River National Laboratory)[vi]

TIEs as Monitored Item Enclosures

The enclosure surrounding the monitored item (equipment cabinet, nuclear material storage container), over which C/S or CoC is required, may serve as a TIE. Combined with a TID on the mechanical opening, having the monitored item's enclosure itself as a TIE provides additional assurance that it was not penetrated via a non-traditional opening (such as drilling through the side). The method of implementing a TIE for an item depends on whether the item enclosure is facility-owned or inspector-owned. In the case that the item enclosure is facility-owned, the approaches may be limited due to standardized enclosures or limitations on applying exterior coatings or enclosure modifications. Inspector-owned enclosures can be customized. Examples of TIEs at the monitored item enclosure-level include:

- IAEA cabinets which are painted using a powder process, making attempts to repair a tamper more evident[vii].

Figure 5: IAEA Equipment Cabinet. Picture courtesy Pacific Northwest National Laboratory.

- Monitored item enclosure on which eddy current verification is conducted. Conductive material enclosures have a unique signature that can be determined from variations due to magnetic permeability and material conductivity in the enclosure. Any cutting, drilling, plugging or re-welding will change these properties. Eddy current is useful in particular for facility-owned item enclosures where modifications or exterior coatings may be limited.
- Application of elemental X-ray fluorescence (XRF) compounds onto surfaces and subsequent reading of those XRF signatures.

Application of special materials around the item enclosure, such as fiber optic cables or tamper-indicating shrink wrap. Tamper-indicating shrink wrap consists of sheets of film that are printed with differing ink patterns. The monitored item is enclosed with multiple continuous layers and a heat source is applied. A reference photograph is taken for authentication during subsequent inspections (see

- Figure 6).

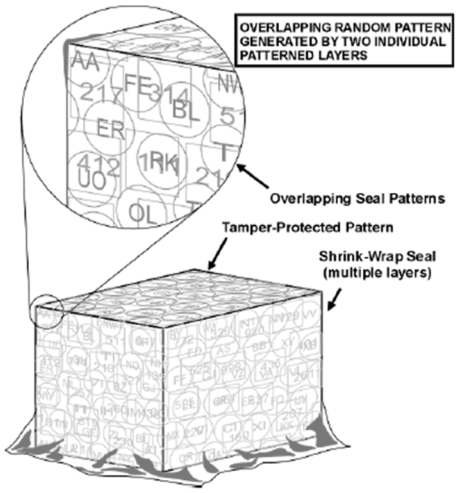

Figure 6: Tamper-indicating shrink wrap. Picture courtesy Sandia National Laboratories.

TIEs as Rooms

At a larger scale, a room can serve as a TIE. If the verification objective is to retain confidence that the walls, floor, and ceiling of the room have not been tampered with since first assessed, tamper-indicating coatings (or other scalable technologies) could be applied to these surfaces, and additional TIDs applied to entry or exit points. Flash thermography is another method that could be used to verify room integrity. It uses active standoff thermal inspection technology to help establish the physical integrity of equipment and structures.[viii]

If the verification objective is to confirm that a room has not been entered, microwave sensors that send microwave beams to receivers and record any interruption in the transmission of those beams, or infrared sensors that sense changes in heat either emitted by a body or blocked/disrupted by a person (or other object) can be deployed. However, as approaches in which the environmental state can be reestablished, these approaches require authenticated event logging.

Functional Characteristics

In addition to scale of use, TIEs can be classified by their functional characteristics, that is, the mechanism by which they indicate tamper of an enclosure. For the purposes of this paper, the three categories of TIE functional characteristics are shell integrity indicators, event assessment or recording devices, and internal environment monitors.

Shell Integrity Indicators

Shell integrity indicators are TIEs that indicate a breach of an outermost shell (whether that is a TID body, other equipment, a monitored item's enclosure, or a room). A shell integrity indicator can be verified with visual inspection to determine if the shell indicates disruption, or can be verified using specialized equipment. Examples of shell integrity indicators include:

- Anodized aluminum, discussed previously. The DCM-C5 (shown in Figure 3), Remotely Monitored Sealing Array (RMSA), and other equipment used by the IAEA often use this material.
- Specialized coatings that are difficult to replicate or reapply upon tamper, for example the Ceramic Seal coatings developed by Savannah River National Laboratory (such as shown in , above).
- Fiber optic wrapped containers and fiber optic panels. Canberra's DCM-C5 camera and the EOSS seal utilize this method.
- Tempered glass or ceramic have also been described as a shell integrity indicators, because they will shatter when disturbed. Both are frangible materials, as described above.
- Eddy current readers and tamper-indicating shrink wrap, as discussed above.

Event Assessment or Recording

Event assessment or recording TIEs record, either actively or passively, whether or not an enclosure has been penetrated. Examples of event assessment for TIEs include:

- Conductive tamper planes such as used in the Ceramic Seal.

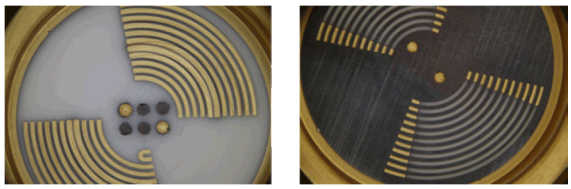

Figure 7: Conductive Tamper Planes on the Ceramic Seal Cap.

- Conductive fabric (such as Oak Ridge National Laboratory's Whole Container Seal) in conjunction with nodes measuring resistance can indicate tamper if the fabric is penetrated.

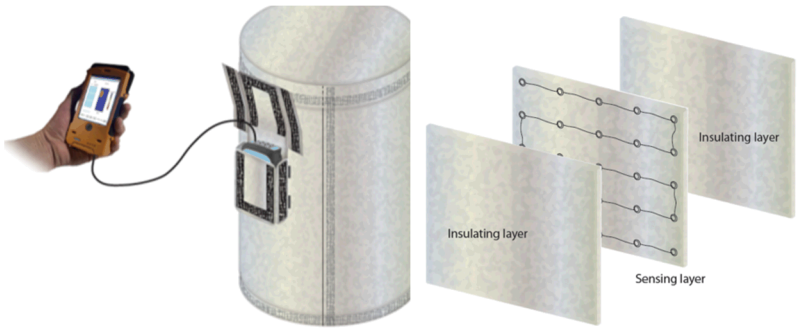

Figure 8: Conceptual Design of Oak Ridge National Laboratory's Whole Container Seal.[ix]

- Fiber optics inside an enclosure, for which penetrating the enclosure will interrupt the fiber.

Internal Environment Monitors

Internal environment monitors are devices that evaluate a key feature of the internal environment within an enclosure, with the assumption that a disruption to that state indicates a penetration of the enclosure. Examples include light sensors, vapor sensors, and pressure sensors. With these types of TIEs, either the environment must not be able to be reestablished, or the change in environment must be recorded and authenticated, i.e. provide non-erasable evidence. Further, the detection mechanism must be able to detect shell compromise of an enclosure. For example, pressure sensors can be used as internal environment monitors for TIEs only if the compromise of the shell of an enclosure would result in a change in pressure within the enclosure. Other examples of internal environment monitors include:

- For an enclosure that is always dark, a light sensor can be used to indicate the introduction of light from a penetration.
- Radiofrequency (RF) monitoring inside an enclosure can be used to detect changes in RF characteristics that would result from opening an enclosure.[x]

Verification Mechanism

TIEs can also be classified by their verification mechanism. These include visual inspection of specially designed enclosure materials, receipts and analysis of active sensor signals, or enclosure integrity verification via externally applied instruments.

Visual Inspection

Many TIEs incorporate special materials which rely on careful visual inspection to detect sophisticated penetrations or repairs. Visual inspection includes human eye, images and subsequent processing or comparison, or illumination in non-visible wavelengths that result in visual phenomena. TIEs that can be verified via visual inspection may consist of multiple layers of material in which a visibly different sub-surface layer is exposed with penetration (such as with anodized aluminum), change color when penetrated, imprint or disrupt a pattern or design when tampered (plastic with difficult to replicate designs, or with suspended materials), or simply shatter (glass or ceramic). Visual inspection can support the verification of TIEs constructed of specially designed materials, or the internal or external wrapping of a container (such as shrink wrap or passive fiber optic cable wrap that is interrogated with a light source).

Active Signals

TIEs that are verified through active signals rely on electric signals or messages from sensors that indicate an enclosure has been breached. Active signal TIEs include fiber optics, conductive tamper planes, monitored conductive fabrics, and environmental sensors such as light sensors, pressure sensors, or vapor sensors that act as volumetric monitors to detect a change in the enclosure that would indicate an opening. These types of signals tend to require electrical input to maintain

operations, the signal of which can be transmitted to monitoring stations or stored locally on the sensor.

Enclosure Integrity Verification Technologies

Enclosure integrity verification technologies refer to approaches that verify enclosures using active penetration-detecting technologies. Though the enclosures may be constructed from materials that would not be considered TIEs by themselves, these TIE approaches detect disruption in the material's continuity as compared to a previous interrogation. The verification technologies include, for example, eddy current and flash thermography.

Advantages and Disadvantages

Each TIE technology or method has advantages and disadvantages ranging from costs, complexity, scalability, power requirements, and ease of inspection, to name a few. The application itself will often dictate the TIE method. In this section, we discuss high level advantages and disadvantages of the TIE verification approaches and applications.

Scale of Use

If visual inspection will be used, smaller TIEs are generally easier to verify due to the reduced surface area, unless the tamper response is significant. More technically advanced methods such as using external verification equipment or active monitoring of an area can effectively maintain C/S or CoC over larger enclosures such as containers or rooms, though this usually requires a power source which may limit their applications. External verification and visual inspection of larger or fixed monitored items (containers or rooms) may have access issues, i.e. inability to verify backsides or undersides. In those scenarios, active systems have an advantage.

Functional characteristics

Many shell integrity indicators are excellent TIEs in their ability to provide evidence of tamper or penetration without requiring a power source or a verification mechanism beyond visual inspection with the human eye, assuming the tamper attempt is obvious enough to be discovered. These methods are typically simple conceptually and can be less expensive. However, their use in industrial environments such as that of a nuclear fuel cycle facility must also be considered, as the shell integrity indicators may become scratched, broken, or otherwise damaged as a result of normal operational activities.

Event assessment indicators may be useful in monitoring larger enclosures, but they require that the data be authenticated and the sensor not simply "reset" (i.e. that is provides non-erasable evidence). These methods are typically more complex and expensive, but can provide immediate automated and logged tamper detection. Internal environment monitors, which are useful in controlled settings

such as dark or pressurized environments, face similar challenges as event assessment for data authentication and non-erasable evidence.

Verification Mechanism

Visual inspection approaches are typically low cost and involve simple inspection concepts such as visually scanning an item for signs of tamper. Often no additional instruments are required, or if they are, may be standard type equipment such as a digital camera or UV light. Scalability depends on the technology or approach. The visual response of a tamper should be proportional to the size of the monitored item. For example, disruption of the position and orientation of hematite can be detected using a visual reader/image processing on a small scale, but would not be feasible on an entire wall or even large cabinet panel.

Active approaches can allow verification without inspector involvement or inspector presence, which can be useful for remote monitoring applications. Active approaches range in scalability, from small tamper planes inside of the Ceramic Seal, to enclosing large volumes with the Whole Container Seal (conductive fabric). Active approaches require power, however, and depending on application may be an issue. For instance, long periods between inspections, underwater environments, or facility requirements may preclude use of active approaches. Active methods may be more costly and complex as well.

As mentioned previously, approaches that interrogate enclosure integrity (eddy current and flash thermography) are particularly useful for existing facility-owned enclosures in which modifications may be limited. However, which technology is chosen depends upon the enclosure material (eddy current can only be used on conductive materials), size of the enclosure, and application (which, due to operator or host restrictions, may not allow active interrogation methods at all). Costs of these technologies are related to the interrogating equipment. Analysis may require a skilled inspector or post-interrogation analysis algorithms.

Conclusions

The current landscape of TIEs can be understood in a variety of contexts, depending on scale, functional characteristics, and verification mechanism. Though these groups may be a convenient mechanism for understanding broad categories, the classification of TIEs into these categories, or others, is neither mutually exclusive nor exhaustive. Indeed, there are differing opinions within the nonproliferation community about how TIEs should be understood.

The increasing importance of TIEs within the international safeguards and arms control verification communities may increase the focus on these technologies in the future, at which time it will become more imperative to find consensus on TIE definitions and categorizations.

Acknowledgements

The work described in this paper is funded by Sandia's Laboratory Directed Research & Development funding. Special thanks to Karl Horak for his initial thinking and organization on this topic.

---

[i] Garcia, Mary Lynn. The Design and Evaluation of Physical Protection Systems. Sandia National Laboratories, 2001.
[ii] "Tamper Indication" IAEA Safeguards Glossary 2001 Edition. International Nuclear Verification Series, No. 3. June 2002. http://www-pub.iaea.org/MTCD/publications/PDF/nvs-3-cd/PDF/NVS3_prn.pdf, accessed 02 April 2015.
[iii] Black, Billy D. "Survey of High Security Tamper-Indicating Enclosures" July, 1991. SAND-91-156.
[iv] Zamora, David L., Romero, Juan A., Thomas, Maikael A., Walker, Charles A., Peterson, Kenneth A., and Smartt, Heidi Anne. "First Prototype of Intrinsically Tamper Indicating Ceramic Seal (ITICS)." In the Proceedings of the Annual Meeting of the Institute of Nuclear Materials Management, July 2012.
[v] International Atomic Energy Agency, "Workshop on Sealing, Containment, and Authentication Technologies: Announcement Annex (General Technical Requirements)." Available at: http://www-pub.iaea.org/MTCD/Meetings/PDFplus/2011/43123/43123_AnnexLeaflet.pdf
[vi] Photo courtesy Savannah River National Laboratory, in: Smartt, Heidi A., Krementz, Daniel, Kuhn, Michael J., "Advanced Technologies for Safeguards Communications Current Research on Containment Technologies for Verification Activities: Advanced Tools for Maintaining Continuity of Knowledge." Presented at the 2014 Symposium on International Safeguards: Linking Strategy, Implementation, and People. 20-24 October 2014. Available at: http://www.iaea.org/safeguards/symposium/2014/home/eproceedings/sg2014-papers/000138.pdf
[vii] Schanfein, Mark, "International Atomic Energy Agency Unattended Monitoring Systems." In Nuclear Safeguards, Security, and Nonproliferation, ed. James E. Doyle. 2008.
[viii] Correa, Ernest M., Shepard, Steven, Chaudhry, Bharat B., Bartberger, Jack C., Cates, James, Trujillo, A., Merkle, Peter M. "Active Thermal Standoff Inspection for Physical Authentication." In the Proceedings of the Annual Meeting of the Institute of Nuclear Materials Management, July 2010.
[ix] See Smartt et, al. 2014.
[x] Pickett, Chris A., Tolk, Keith M., Keel, Frances, and LaMontagne, Steve. "Results from the 2010 INMM International Containment and Surveillance Workshop focused on Concepts for the 21st Century." In the Proceedings of the Symposium on International Safeguards: Preparing for Future Verification Challenges. 1-5 November, 2010, Vienna Austria. Available at: https://www.iaea.org/safeguards/symposium/2010/Documents/PapersRepository/099.pdf