A SYSTEMS APPROACH TO TAMPER PROTECTION

W. C. Myre
M. J. Eaton
Sandia National Laboratories, Albuquerque, New Mexico, USA

CONF-800315--18

MASTER

Abstract

Tamper-protection is a fundamental requirement of effective containment and surveillance systems. Cost effective designs require that the tamper protection requirements be considered early in the design phase and at the system level. A discussion of tamper protection alternatives as well as an illustrative example system is presented.

1. Introduction

In the design of equipment to meet the objectives of an international safeguards system, it is essential that the data provided an inspector accurately represent the true state of affairs in the safeguarded facility.[1] For equipment that is to remain unattended for long periods of time, it can be a difficult endeavor to ensure that the equipment is operational at all times and has not been tampered with. In fact, the requirements for equipment reliability and tamper protection can be major contributors in the design process, suggesting basic design strategies that might otherwise not have been chosen. The difficulty of meeting these requirements often dictates that the various safeguards elements be highly interdependent. Thus, the design of an individual piece of equipment should not progress independently of the other elements to be used in the complete system.

The goal of tampering is to modify the operation of a system so that unauthorized acts can be performed without fear of timely detection of those acts. Overt tampering is undertaken without concern for the concealment of evidence that tampering has taken place. On the other hand, covert tampering involves efforts to leave no obvious evidence that the system has been defeated.

In this paper the tamper-related terminology is defined as follows:

Tampering - The act of interfering with safeguards related equipment or data with the goal of preventing the safeguards system from performing its intended function.

Tamper Indicating - The capability to report or record a tamper attempt.

Tamper Resistant - The capability to impede, but not necessarily indicate, a tamper attempt.

Tamper Protection - The application of devices and techniques to ensure the validity of data, the integrity of equipment and to indicate the cause of failures.

Design of the tamper protecting features of unattended instruments can be difficult since the adversary (1) has considerable time, (2) knows, or can know, the design details of the instrument, and (3) has access to nearly unlimited resources to achieve his purpose. In well designed international safeguards system, tamper protection is accomplished by the combination of tamper resistant and tamper indicating features coupled with careful observation by an inspector.

2. Approach

The tamper protection requirements of a system are determined during the preliminary design phase and are dependent on the specific application. The desired level of tamper protection is designed into each system element. The interdependence of tamper protection techniques and inspection frequency is of particular importance. For a given tamper protection technique, the likelihood of detection typically increases with more frequent inspector presence.

The many different types of tamper indicators in use can be categorized into three groups--passive, active and state-of-health monitoring. The most effective passive techniques usually require time consuming examination of a "fingerprint" of some sort resulting in significant inspection verification time. However, these passive techniques can be very effective in establishing intent during an investigation triggered by a more easily read active system. Active techniques such as tilt switches and cover switches are usually easy to read; however, they may be more prone to false alarms. State-of-health monitoring techniques such as self-test circuits or polling schemes are also easy to read but suspicions of component reliability may lead to ambiguous interpretations of tamper indication. The level of tamper protection capability will be determined by the type and number of techniques selected. An optimum system designed to detect tampering by a dedicated adversary will very likely include a mixture of all three types of indicators.

Component reliability can become a significant issue in the arena of tamper protection. Most systems have a defined operating range where satisfactory performance can be statistically assured through careful design, component selection and product acceptance testing. When systems are deliberately subjected to environments beyond the defined operating or handling limits, tampering can be disguised as poor component reliability. Techniques need to be included in the tamper protection design, such as temperature labels or dosimeters, to ensure that the safeguards components have not been subjected to destructive operating environments. In addition, the various classes of failure modes must be addressed and, insofar as possible, the system must be designed to fail in the least objectionable modes. For example, system failures should not be obvious to the diverter but must be easily recognizable by the inspector.

Role of Inspector

The total IAEA safeguards system is strongly dependent upon human activities.[2] Verification of data recorded by safeguards instruments, physical inventories, and of material flows all depend upon inspectors and the inspection effort. Evaluation of information provided by the state, collected during inspections and obtained from analytical samples often involves human judgment. The design of tamper protection features and equipment should recognize the importance of this human interface. Tamper protection subsystems should be easy for the inspector to install, inspect, and maintain. Any support equipment required for integrity verification or for information collection and readout should be small, easy to operate and portable.

Evaluation of information provided by tamper protection equipment can be placed in two categories. The first category of evaluation occurs during the facility inspection. Here, the inspector concludes that either tampering has not occurred or that due to some form of ambiguity, it is not possible to state that there has been no tampering. In the latter case, the inspector must attempt to gather additional information which may immediately or at some later time be used to clarify the ambiguity. The design of a tamper protection subsystem should consider this possible need for additional information and should provide specific guidance for use by the inspector. The second category of evaluation occurs after the inspection and possibly upon return to IAEA Headquarters. Examination of all information relevant to the facility and the particular inspection is completed. It is at this point that remaining ambiguities are resolved, and final conclusions are reached.

The choice of unattended instrumentation techniques also influences the inspector role. Unattended instrumentation systems currently in use are generally autonomous packages, in that each sensor package includes the capability to record and store data independently. For these systems, inspectors periodically retrieve all the data and inspect all the system components. A central recording system could replace some of the manual requirements for collecting data and monitoring autonomous packages. The choice between autonomous packages and a central recording system is based on such trade-offs as cost, the degree of tamper protection desired, the allotted annual inspector days specified in agreements for the facility, and the timeliness criteria.

Tamper Protection Locations

Tamper protection can be applied at many locations in a safeguards system. The contribution and vulnerability of each element must be considered. The following five locations address some of the major tamper protection considerations:

1. The coupling between a sensor or detector and the phenomenon being observed. For example, in an optimum system, radiation detectors should be able to sense the unauthorized placement of shielding around the detector, and CCTV systems must be able to detect scene substitution.

2. Environmental monitors. Radiation dosimeters and temperature indicators are examples of devices that will record the ambient conditions to determine if the components have been subjected to destructive operational environments.

3. Interconnecting control, power or data lines. Balanced bridge circuits, phase comparators and fiber optics transmission lines are examples of techniques that have been utilized to ensure data integrity between system components.

4. The remote data link that transfers data from local monitoring equipment to another location for review and processing. These data may be transferred through radio links, hardwire, or recorded on a storage medium and physically transported. Authentication and encryption are examples of techniques utilized in this area. Asymmetric encryption techniques show promise of being extremely useful and are likely to enhance the utility of real time remote monitoring systems.

5. Individual equipment enclosures. Anodized aluminum, prestressed glass, seals and microswitches are examples of techniques employed in tamper indicating enclosure designs.

Enclosures

Because enclosures are universal components of any tamper protection system, and their design principles apply to other portions of the system, they deserve closer examination. An enclosure (which may include closure devices, joints, surfaces, position and volume intrusion sensor), defines a physical boundary beyond which unauthorized access is detected.

Tamper protection enclosure designs have received considerable attention in national defense applications. For these applications the sensing of the tamper attempt is integrated with an immediate response to deny the use of the enclosure contents. Such systems are usually complex and expensive and have found little application in international safeguards.

Ideally, an enclosure should be simple, not prone to false alarms, and should reliably provide an unambiguous, easy to verify indication of tampering. However, this is generally difficult to achieve without using several tamper protection features. Active methods which are used with systems that have recording units may be used in conjunction with passive features such as prestressed glass. The recording of data from active devices can be either local, or remote as proposed in the RECOVER program. Even when remote recording is available, it is often necessary to have periodic local inspections to provide additional observations and readings.

One of the most difficult problems associated with enclosures is that of maintaining enclosure integrity while still having adequate provision for authorized access. Closure devices (locks and/or seals) are used to allow necessary operations such as film change, data removal and maintenance.

Surfaces may respond to penetration attempts by self-destruction (such as prestressed glass) or may simply have physical characteristics that are difficult to restore after disturbance. Joints must resist probing attacks which could be used to remotely defeat interior components. The combination of joint and closure device must resist disassembly without the proper tool whether that tool be code, key, or the removal of a seal by an authorized person. In passive containers, disassembly by other than proper procedure must leave tell-tale traces.

Position sensors typically are active devices such as a switch used to detect opening of a joint or tilt motion detectors used to sense movement of the entire enclosure. Such devices reinforce or augment surfaces and joints and prevent defeat by direct disassembly.

Volume intrusion detection methods have been extensively applied to plant physical security and potentially could be useful as a tamper detection method for enclosures. However, when methods such as tuned RF or acoustic cavities were examined in the past, little practical usefulness was found due to design complexities and false alarm problems.

Combined systems can be very effective. For example, a protective surface may be combined with a position switch that detects removal of that part of the surface. Defeat of the switch requires disruption of the surface which cannot be restored, but removal of the surface requires defeat of the switch.

Enclosures, as well as other components of a tamper protection system, tend to positively interact when integrated into a system. The extent of this interaction is best illustrated by the description of an example system.

3. Example System Description

An unattended video surveillance and recording system has been selected to illustrate some of the practical aspects of tamper protection.[4] This system (see Figures 1 and 2) is designed to collect video surveillance data from two remotely located video cameras. These cameras receive power and transmit signals via cables to the control electronics where the processing and recording of the signals occur.

This system is tamper protected in three major areas: camera housings; the cables to the cameras; and the control and video recording electronics inside a cabinet. The camera housings are machined from an aluminum tube and treated with a special coating. The rugged housing and special coating make it difficult to tamper with the housing without leaving detectable evidence. The tubular housing is easy to seal because threaded rings on the front and rear of the housing can be wire sealed to the mounting brackets on the housing. Temperature sensing labels, humidity sensing labels and radiation detectors are also installed inside the housing to indicate excessive environmental conditions. These detection methods, coupled with indications on the video records, provide evidence of tampering attempts.

The cables that connect the camera to the control cabinet are perhaps the most vulnerable part of this system. Without some type of protection it

would be possible to substitute video information on these cables without any indication of tampering. This system utilizes cable supervision which monitors for opens, shorts, and cable taps. Detection of such tamper attempts provides indicators that are recorded in the video signal. The RF multiplex signals utilized in the system also make it difficult to substitute video signals on the cables.

Short circuit protection is built into the camera power supply to prevent its destruction by intentional shorts in the camera power cables. The power supply returns to normal operation when the short is removed. During the time period that camera power was shorted, a circuit within the cabinet reinserts video sync so that video recordings can continue to be made of the tamper flags generated by the system. A video presence detector within the circuitry looks for the video and distinguishes the difference between the lack of video from the camera and the possibility that the camera had been covered with cloth.

The cabinet is tamper protected to provide protection for the control and recording electronics which must be accessed for installation, maintenance and other operations. Tamper protection is provided by a combination of cabinet seals, automatic door locks, surface finish, and tamper switches. The doors are protected by tamper trim to block cabinet access of probe-like devices designed to change switches which significantly modify operation. The trim also protects the tamper switches which monitor the opening and closing of the door. The cabinet is monitored for environmental tampering by enclosing temperature labels, humidity labels and radiation detectors.

The system electronics monitors the active tamper functions and inserts tamper data into the video signals. Thus, the video information contains letter designations which inform the inspector about tamper signals. Interpretation of this record along with actual physical evidence would permit an inspector to make a determination as to whether tampering has occurred.

The battery backup power supply provides for continued tamper protection during power outages at the facility being monitored. The frequency and duration of power outages are recorded for use in detecting tampering via control of the main power source.

Video signals are provided to a slave recorder in a separate tamper protected cabinet compartment located above the main electronics cabinet. Since it is planned that non-IAEA personnel will have access to this cabinet and its electrical interfaces, protection has been provided on all power control and video signal lines going to the slave recorder. These lines are fused and zener diode protected so any attempts to inject higher voltages down into the system to cause failures would be met by clamping of the high voltage and blowing of the fuses. Blown fuses are an indication of tampering with these control lines to destroy the integrity of the main system.

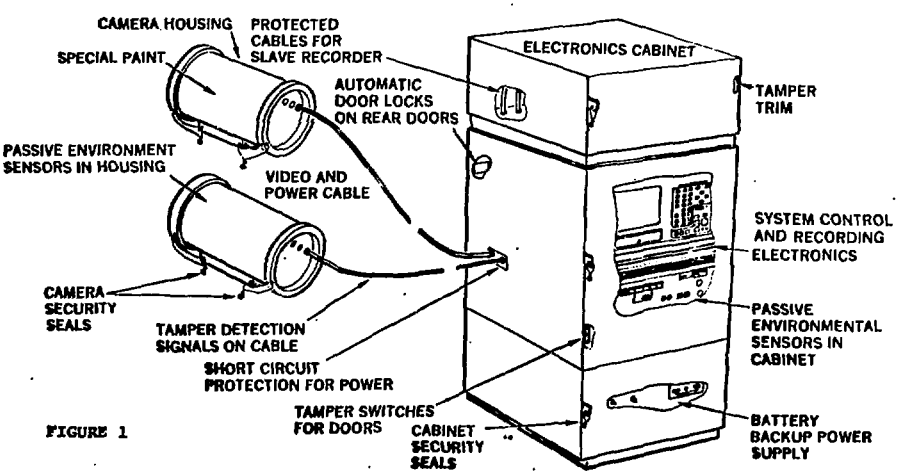

FIGURE 1

4. Summary

As illustrated by the description of the example system, attempting to tamper protect even a moderately sized system can require a significant effort. It is extremely important that the various tamper protection features be properly balanced and synergistic effects be utilized to enhance total system capability. With the increase in the number and types of safeguards instruments being installed in nuclear facilities, tamper protection can be expected to receive an increasing amount of attention. When tamper protection is given adequate attention early in the design phase, effective systems can be designed.

5. References

1. Dilworth, Secord, Meagher and Associates Limited, "Development of Safeguards Procedures for Heavy Water Moderated and Cooled Power Reactors with Continuous Refueling", February 1968, IAEA 519/RB.
2. C. Buchler, "International Safeguards: A Profession with a Future", 20th INMM Proceedings, Albuquerque, NM, July 16-18, 1979.
3. F. Prokoski, et al, "Development of Surveillance Devices with Remote Verification Capability, 1st Annual Symposium, ESARDA, Brussels, Belgium, April 25-27, 1979.
4. C. S. Johnson, Unattended Video Surveillance Systems for International Safeguards, 20th INMM Proceedings, Albuquerque, NM July 16-18, 1979.

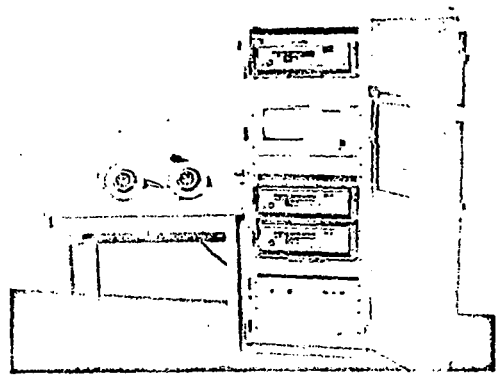

FIGURE 2