PNNL-11407
UC-515

Optical-Based Smart Structures for Tamper-Indicating Applications

P. Sliva
N. C. Anheier
K. L. Simmons
H. A. Undem

November 1996

Prepared for
the U.S. Department of Energy
under Contract DE-AC06-76RLO 1830

Pacific Northwest National Laboratory
Richland, Washington 99352

DISCLAIMER

Summary

This report is a compilation of several related projects performed from 1991 through 1996 concerning the design, construction, and application of optical-based smart structures[a] to tamper-indicating and sensing secure containers. Due to several influences, the projects were carried through to varying degrees of completion. Cancellation of the overall project at the client level motivated the authors to gather all of the technology and ideas about smart structures developed during these several projects, whether completed or just conceptualized, into one document. Although each section individually discusses a specific project, the overall document is written chronologically with each successive section showing how increased smart structure complexity was integrated into the container.

The first project presented in this report, which represents the basis of all of the related projects, was initiated by the need of the U.S. Department of Energy (DOE) to find a more cost effective method of securing nuclear materials or related items of high value either in storage or transport. Although other methods of securing these items existed, all-composite, lightweight containers that monitored in real-time did not. The initial demonstration container and the next container, a secure video system to remotely monitor factory operations, proved that the concept of optical fiber-based tamper-indication would work. The tamper-indicating window became of interest because it allowed visual inspection of a container's contents or the radioactive contents of a room to be inventoried without having to enter the room. A second tamper-indicating container for storing and shipping radioactive materials, in this case special nuclear material from dismantled weapons, was initiated as a way to reduce visual inspections at DOE storage facilities. This next-generation container had the ability to communicate its status in real-time. It became apparent as the complexity of the smart structure increased, especially with the communication aspect, that tamper-indicating containers had applications beyond storing and transporting nuclear materials. Interest grew within the U.S. Department of Defense (DoD) of using smart containers for shipping, storing, and prepositioning high-value material. As a result, the authors received several requests to write proposals to design and construct smart intermodal-type shipping containers.

This report provides information on the five projects that were initiated involving optical-based smart structures. These projects include the first demonstration container, the second container for secure video applications, smart windows, the next-generation container with communications, and the large, intermodal smart shipping containers.

- A prototype secure container was prepared that used continually monitored optical fiber as the smart structure. A small (~7.6 cm x 10.2 cm x 12.7 cm), matchbox-shaped container, consisting of an inner drawer within an outer shell, was fabricated from polymer resin. The optical fiber was sandwiched between additional non-optical, strength-promoting fibers and embedded into the polymer. The additional non-optical fiber provided strength to the container, protected the optical fiber from damage, hid the fiber, and acted as a decoy. The optical fiber was wound with a winding density such that a high probability of fiber damage would be expected if the

---

(a) Smart structure, by general definition, is a system comprised of smart materials and other components that is able to respond to external stimuli in an intelligent manner. Fiber optic (or channel waveguide) is the basis of the smart structure for tamper-indicating containers and windows because it can sense external stimuli and also carry the resultant signal to the microprocessor for response.

container was penetrated. The inner drawer and outer shell were wound with optical fiber that optically coupled when the two halves were joined to form a continuous optical pathway. Electronic circuitry located in the base of the inner drawer sent and received an infrared signal through the fiber several times a second (20 Hz). For demonstration, when the drawer was opened, interrupting the fiber loop and creating a container breach, an alarm beeper was activated. The beeper could be turned off using an infrared remote control. When the drawer was re-closed, the alarm circuitry automatically reset so that any subsequent breach again set off the beeper.

- A tamper-indicating container was prepared to secure a video system that uses actively monitored optical fiber as the smart structure. Because the video system was already adapted to a steel container, an all-composite, fiber-wound container was not constructed. Additionally, because the steel container had several limiting features, an all-composite, fiber-wound lining could not be prepared as a single shell and inserted into the steel container. Instead, optical fiber was wound around six polyurethane foam panels and assembled inside the steel box. Holes in the container for the video camera lens were made secure by winding spiral disks of optical fiber, placing them around each hole, and splicing the fiber to the remainder of the wound panel. Electronic circuitry was designed and prepared that sent and received an infrared signal through the optical fiber. The electronics system was designed to activate an alarm beeper if a fiber was compromised or an attempt was made to remove the secure container's lid. The electronics package performed as designed and although functionally limited, provided the possible electronic functionalities that can be built into the structure.

- A project was initiated to create channel waveguides first on and then within clear polymers for tamper-indicating window applications. Channel waveguides are linear regions of slightly higher (than their surroundings) refractive index capable of propagating a light signal much in the way a fiber optic transmits light. Using procedures closely resembling those for creating microelectronic circuitry, channel waveguides were written in polymers spin-coated on clear polymer substrates. Varied channel waveguide "circuitry" was written on several substrates to demonstrate the methodology and possibilities. Being able to write circuitry beyond simple linear patterns opened the possibility of creating sensors on the substrate surface in addition to tamper-indication. At project end, a precise method of coupling light into the channel waveguides was being developed. All that remained was to create the sandwich structure to protect and hide the channel waveguides.

- A tamper-indicating composite container was designed for the transport and storage of special nuclear material removed from dismantled weapons. In addition to the optical fiber-based tamper indication designed into previous smart containers, the container had two unique embedded sensors. The first was a scintillating fiber embedded in the lid that when placed in a neutron field, reacted with the neutron field to produce light, which was transmitted through the fiber and detected by solid-state photomultiplier tubes. This sensor would detect the removal of the lid, removal of the source, or human presence near the container. The second sensor employed Bragg sensors (gratings) in an embedded optical fiber traversing the lid near each of the 12 bolt holes to create a unique (up to) 12-point stress signature once the bolts are tightened. It would be extremely difficult to reproduce the stress signature. Radio Frequency (RF) communication was used to monitor the container's status in real-time.

- At the time of these projects, there was a need to advance the state-of-the-art in intermodal shipping containers for military and commercial applications. Because of this need, a next generation tamper-indicating, smart shipping container was designed and conceptualized in

several proposals written to various military agencies. At the time of this report, one of the proposals was selected for funding. This container would sense light, internal moisture (humidity), motion, and temperature (internal and external). The container would be robust for shipping and field environments, lightweight, waterproof, sling capable, and configured for handling by standard forklifts. Similar to the previous containers designed and constructed by the authors, the intermodal container would provide physical security for the contents and detect, in real-time, container breaches and general container health (e.g., physical integrity of walls, corners, and doors). The container would include a control system that was self-contained, self-powered, and provided global positioning capability. All of the sensor and global positioning information, container health, and inventory movement would be automatically uploaded to an RF tagging system that could be externally interrogated while in transit (e.g., automated crane systems) and in the field (e.g., field personnel with hand-held readers or satellite uplink).

Smart structure complexity increased with each new container even though the basis for tamper-indication remained essentially unchanged. Optical fiber as the smart material allowed for the addition of other discrete sensors, fiber optic-based (e.g., secure windows, radiation, stress) or otherwise (e.g., moisture, temperature, motion). All of the containers were designed and constructed so that the optical fiber-based smart structure was an integral part of the container. At the time of this report, compared with all other methods of providing tamper-indication for secure containers, the smart containers designed, developed, and constructed in these projects are the only tamper-indicating containers in which the *container itself* provides the tamper indication.

Acknowledgments

The authors recognize Kurt Stahl and Ross Gordon who played key roles in the first few years of our smart materials projects. The authors also thank Debra Sunberg, Richard Craig, and Mary Bliss who, for most of the projects, provided all of the expertise and performed most of the experiments involving optical fiber transmission. Sergey Kucheryavyy developed many of the channel waveguide writing techniques for creating secure windows. Hal Undem has been the consummate program manager; his role in our success cannot be overstated. Except for the secure video system project, which was funded by Sandia National Laboratory (SNL), and the intermodal shipping container proposals, which were funded internally, all of the projects associated with this report were funded by DOE's Office of Non-Proliferation and National Security (NN-20).

Acronyms and Abbreviations

ALARA	as low as reasonably achievable
ASTM	American Society for Testing and Materials
DER	Dow Epoxy Resin
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy
FY	fiscal year
GPS	global positioning system
IC	integrated circuit
ISO	International Standards Organization
LED	light-emitting diode
OTDR	optical time domain reflectometer
PNNL	Pacific Northwest National Laboratory
RF	radio frequency
rpm	revolutions per minute
SNL	Sandia National Laboratory
TETA	triethylene tetramine

Contents

Figures

Tables

1.0 Introduction and Background

This report is a compilation of several related projects performed from 1991 through 1996 concerning the design, construction, and application of optical-based smart structures[a] to tamper-indicating and sensing secure containers. Due to several influences, the projects were carried through to varying degrees of completion. Cancellation of the overall project at the client level motivated the authors to gather all of the technology and ideas about smart structures developed during these several projects, whether completed or just conceptualized, into one document. Although each section individually discusses a specific project, the overall document is written chronologically with each successive section showing how increased smart structure complexity was integrated into the container.

The first project presented in this report, which represents the basis of all of the related projects, was initiated by the need of the U.S. Department of Energy (DOE) to find a more cost effective method of securing nuclear materials or related items of high value either in storage or transport. Although other methods of securing these items existed, all-composite, lightweight containers that monitored in real-time did not. The initial demonstration container and the next container, a secure video system to remotely monitor factory operations, proved that the concept of optical fiber-based tamper-indication would work. The tamper-indicating window became of interest because it allowed visual inspection of a container's contents or the radioactive contents of a room to be inventoried without having to enter the room. A second tamper-indicating container for storing and shipping radioactive materials, in this case special nuclear material from dismantled weapons, was initiated as a way to reduce visual inspections at DOE storage facilities. This next-generation container had the ability to communicate its status in real-time. It became apparent as the complexity of the smart structure increased, especially with the communication aspect, that tamper-indicating containers had applications beyond storing and transporting nuclear materials. Interest grew within the U.S. Department of Defense (DoD) of using smart containers for shipping, storing, and prepositioning high-value material. As a result, the authors received several requests to write proposals to design and construct smart intermodal-type shipping containers.

This report provides information on the five projects that were initiated involving optical-based smart structures. These projects include the first demonstration container, the second container for secure video applications, smart windows, the next-generation container with communications, and the large, intermodal smart shipping containers.

The first smart structure constructed was a small, matchbox-like container that was a successful feasibility demonstration. This container was comprised of densely wound optical fiber embedded in a polymer shell. A laser diode pulsed light through the fiber and a piezoelectric buzzer alarmed if the container shell was compromised or the container was opened.

The second secure, or tamper-indicating, container was constructed to securely house a video camera system and contained six optical fiber wound panels, each with its own laser diode light system. Interrogating each panel separately permitted isolation of a container breach. Camera lens

---

(a) Smart structure, by general definition, is a system comprised of smart materials and other components that is able to respond to external stimuli in an intelligent manner. Fiber optic (or channel waveguide) is the basis of the smart structure for tamper-indicating containers and windows because it can sense external stimuli and also carry the resultant signal to the microprocessor for response.

holes were made tamper-indicating by circularly winding optical fiber around each hole and splicing both fiber ends to the panel fiber to complete the optical circuit. The original video system windows were comprised of tempered glass with a sensor attached. An attempt to break through the glass would result in its completely shattering, causing the sensor to trigger an alarm. Searching for a better way to secure the video camera windows led to the concept of smart windows.

The goal of the smart windows project was to develop a clear, polymer window with channel waveguides running through it that would transmit light. It was envisioned that the window could be integrated into a fiber-wound, tamper-indicating container, wall, or door when see-through capability was needed. A two-step development plan was chosen: 1) to write channel waveguides in a polymer coated on a clear substrate and 2) to write channel waveguides directly into the polymer subsurface. At the end of the two-year project, step one was almost completed.

The third container being developed was for storing and transporting neutron-emitting sources such as special nuclear material from dismantled weapons. It had the typical features of the earlier containers such as composite construction and embedded optical fiber for tamper-indication. In addition, this container was to have radio frequency (RF) communication and a unique composite lid that utilized both embedded fiber optic Bragg sensors for tamper-indication of tightened bolts and embedded scintillating fibers for neutron detection. This project was at the design stage when the overall program at the client level was canceled.

Similar to the smaller tamper-indicating containers constructed and/or designed, a large intermodal shipping container was conceptualized and designed. Several proposals to construct a tamper-indicating smart intermodal shipping container, including two with unique cooling systems, were marketed to the military. At the time of this report, one of the projects had been selected for funding and the authors were waiting on the funding disposition.

2.0 Tamper-Indicating Demonstration Container

2.1 Introduction

The objective of this study was to demonstrate optical fiber/polymer matrix smart structure properties through fabrication of a small, secure container; identify potential problems associated with design and fabrication; and ascertain application and growth potential of optical fiber/polymer matrix smart structures into additional areas.

Smart materials and structures are part of a rapidly evolving, multidisciplinary approach to using a material's intrinsic properties or combining materials to achieve inherent intelligence (Rogers 1989; Ahmad et al. 1990). Smart materials may be defined as materials that possess intrinsic properties capable of responding and adapting to external stimuli. The material's intelligence may be the result of its composition, processing, microstructure, presence of defects, or conditioning. Smart structures may be comprised of integrated smart materials and/or more discrete components such as actuators or sensors which, in combination, provide the required intelligence.

Optical fibers have been the basis of advanced polymer composites to prepare intelligent structures (Claus 1991). Optical fibers are small, are immune to electromagnetic interference, are lightweight, can be embedded in other materials, have an adjustable composition, and can operate in harsh environmental conditions. Optical fiber-based smart structures have the ability, via embedded or attached optical fiber (the smart material) and the associated electronic circuitry, to monitor the polymer's physical integrity and structural behavior during use. The unique ability of optical fiber to act as a signal transmitter as well as to modulate a propagating optical signal as a response to external stimuli has led to numerous applications of optical fiber-based smart structures. Although capable of detecting electrical and chemical phenomena, optical fiber sensors have been developed primarily for determining strain, thermal expansion, and vibration of structural components.

Non-optical glass or polymer fibers are typically embedded into polymer structures to enhance strength and toughness. Replacing a portion of the structural fiber with optically conducting fiber permits fabricating robust, optically-active structures such as secure containers. Secure containers are optical fiber-based smart structures that offer the ability to continually or passively monitor the integrity of the container walls (shown conceptually in Figure 2.1). Continually monitored, secure containers monitor in real-time, with container breaching activating the smart structure. Smart structure activation can lead to numerous consequences within the container depending on the specific application of the container, the size of the container, and the complexity of the accompanying electronics. At a minimum, smart structures can be given the ability to recognize and record container breaching. Difficulty in defeating the secure container depends on the smart material's stealth and the smart structure's complexity, which can be provided by the smart material being incorporated into the container walls with additional, non-active decoy material.

2.2 Experimental Approach

The secure container chosen for demonstration was comprised of three parts: optical fiber, fiber reinforced polymer matrix, and an electronics package. The project was completed in three phases. The first project phase was to design the container and electronics and determine a suitable

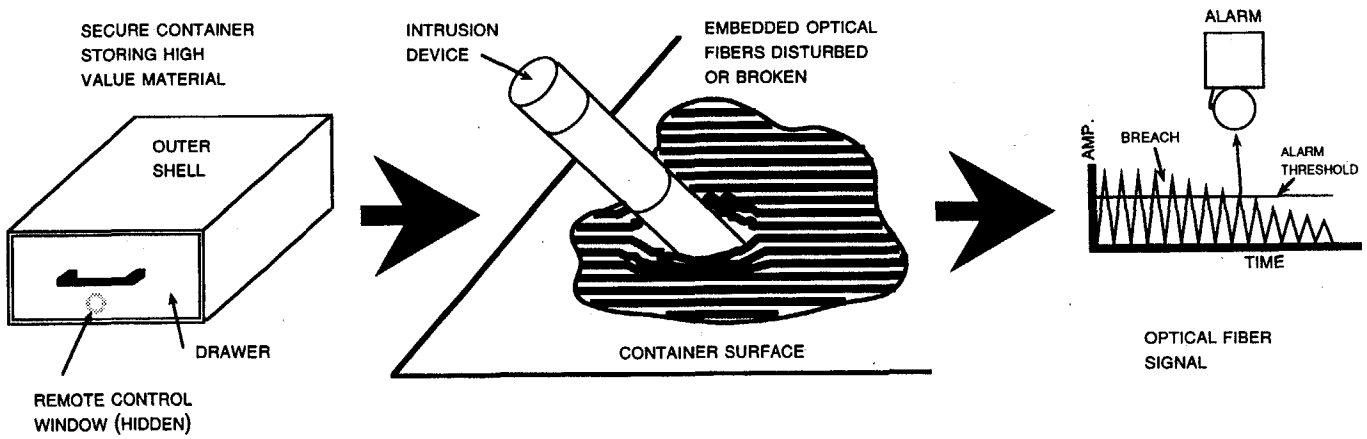

Figure 2.1. Optical Fiber-Based Smart Secure Container Conceptual Operation

optical fiber for embedding into the polymer matrix. The second phase was to fabricate the container without optical fiber to evaluate the fabrication process, assemble the electronics package, and evaluate optical fiber performance in the candidate epoxies. The final project phase involved fabricating the container with optical fiber, connecting the electronic circuitry, and testing.

2.2.1 Optical Fiber

Characteristics of the optical fiber were chosen for the secure container application. The fiber was to have a glass core and cladding (buffer optional), be multimode, have an overall diameter as small as possible, have minimal loss of optical signal upon bending, be able to transmit (in the near infrared) up to a kilometer with minimal loss of optical signal, be compatible with the polymer matrix, and be relatively inexpensive. Commercial-grade optical fiber was obtained from Polymicro Technologies Inc., the characteristics of which are listed in Table 2.1. The fiber obtained had a silica-based core and cladding and a protective polyimide buffer.

A series of tests were performed in order to determine the effect of embedding the optical fiber in a polymer. A known length of fiber, typically a few meters, was coiled and placed into the bottom half of a 500-ml polyethylene bottle. The fiber ends were cleaved and attached to a spectrophotometer (U.O.P. Guided Wave, Inc. Model 100 Spectrophotometer) that transmitted light pulses over a wavelength range of 350 to 1000 nm. The spectrophotometer measures transmittance as a function of time and wavelength. An ultraviolet/near infrared transmissive fiber was used as the standard reference cable. A transmittance measurement was taken on the coiled fiber (representing time zero) and then the polymer poured over the fiber to embed it. Transmittance measurements were taken on the fiber at approximately 10-15 minute intervals until the polymer cured.

Three different epoxies were prepared for fiber embedding: 1) Dow (Dow Chemical Company) Epoxy Resin (DER) 332 epoxy resin with 10 parts per hundred triethylene tetramine (TETA) (Kodak Chemical Company); 2) DER 332 epoxy resin with 40 parts per hundred Jeffamine (Texaco Chemical Company) T-403 hardener; and 3) DER 332 epoxy resin with 80 parts per hundred Versamide (General Mills Chemical Company) 140 hardener. The first two hardeners produced rigid epoxy after curing, the Jeffamine taking longer to cure than the TETA. Longer

Table 2.1. Characteristics of the Optical Fiber Used in Fabricating the Secure Container*

- Composition: Pure Silica/Doped Silica (Core/Cladding)
- Buffer Composition: Polyimide
- Core/Cladding/Buffer Outer Diameters: 100 μm/110 μm/125 μm
- Transmission Range: 380-2500 nm
- Operating Temperature: To 400°C
- Ultra-low OH^- Core
- Step Indexed
- Radiation Resistant
- High Laser Damage Threshold

* Obtained from Polymicro Technologies Inc.: Fiber FHZ100110125.

curing times are associated with less shrinkage; therefore, it was expected that the Jeffamine-containing epoxy would result in lower shrinkage. The Versamide is a polyamide hardener that keeps the epoxy semi-flexible after curing.

Because the optical fiber would make numerous bends when wound into the container, a series of tests were performed on the optical fiber to determine the loss in transmission when the fiber was bent. One end of a known length of optical fiber was attached to an optical time domain reflectometer (OTDR). The remaining fiber was bent over a series of mandrels with radii of 3.5, 1.3, 1.0, and 0.6 cm at wavelengths of 650 and 850 nm and the signal attenuation measured. The container was operated at 850 nm, and 650 nm was used as a check.

2.2.2 Container Design and Fabrication

The container consisted of a five-sided drawer that slid into a five-sided outer shell. Both the shell and drawer were plastic composites consisting of glass reinforcing fiber (carbon or Kevlar fiber could also be used) in a polymer resin matrix. The two container parts used a combination of reinforcing mat and filament wound, unidirectional fiber. Optical fibers were filament-wound within the reinforcing layer with a spacing close enough that attempts to breach the container wall damaged them.

Mold designs for the drawer are shown in Appendix A (Figures A.1 and A.2). A combination of reinforcing mat, reinforcing fiber, and optical fiber were wetted with polymer and wrapped on the mold mandrel shown in Figure A.1 to a thickness of approximately 0.25 cm. The ends of the optical fiber were inserted into Teflon tubing to keep them clean for later attachment of connectors. The polymer was allowed to cure and then the bottom plate of the mold removed. Reinforcing mat was applied to the bottom of the drawer and around the cured material (still on the mold). The assembly was inserted into the mold cavity (shown in Figure A.2) to provide a fixed outside shape for the part. After the polymer was cured, the part was carefully removed from the mold. Similar steps were followed to produce the shell. The mold for the shell is shown in Figure A.3.

2.2.3 Electronics Package

The secure container's electronics package was designed to provide a basic example of the functionality that could be built into such containers. Depending on the container application, circuitry could be designed and miniaturized, for example, to reduce power consumption, provide telemetry, and initiate a range of responses. Therefore, the secure container circuitry demonstrated in this study should be viewed as a starting point, instead of an end point. The electronic circuitry designed was capable of being embedded; however, it was decided to place the circuitry in the bottom of the drawer for viewing and easy access for changes. The circuitry implemented an optical"pitch-catch" scheme. A block diagram and schematic are shown in Appendix B, Figures B.1 and B.2. An infrared light-emitting diode (LED) launched (pitches) pulses of light into the embedded optical fiber. The pulses were approximately 500 microseconds wide and were launched at a rate of approximately 20 Hz. When the optical fiber path was uninterrupted (drawer was closed and embedded fiber winding was unbroken or undisturbed), the pulses arrived at the receiving (catch) end and were detected by a photodiode. The signal was amplified and shaped, and fed to a missing pulse detection circuit. The missing pulse circuit produced a logic 0 signal as long as the prescribed pulses were detected as expected. However, if one or more of the pulses did not arrive, due to fiber

breakage or an open drawer, a logic 1 was output by the missing pulse detector. In the present circuit, the logic 1 level caused a piezoelectric buzzer (mounted to the circuit board) to sound. Since the pulses were expected at a 20 Hz rate (period of 50 milliseconds), any breach lasting longer than 50 milliseconds would be detected. The circuitry also included a remote control detector/demodulator, remote control logic, and a "valid transmission" indicator LED. Four AAA batteries powered the circuit and provided sufficient capacity for approximately 168 hours (7 days) of operation.

Infrared remote control of the circuit was implemented in order to demonstrate its feasibility. The remote control gave the capability to turn off the piezoelectric buzzer during a breach. The infrared LED in the hand-held controller emitted a burst of light pulses which constituted a unique identification address. The encoded light pulses were detected by a phototransistor, with appropriate optical filter, that was mounted on the inside face of the drawer. The pulse stream was amplified, shaped, and decoded. If the decoded identification address matched the expected address, the transmission was considered valid and a signal was sent to a logic circuit that turned off the buzzer. Subsequent transmissions from the remote controller toggled the buzzer on and off as long as the breach condition remained. When the optical fiber path was re-established, as when the container drawer is closed, the circuit automatically returned to its default mode, wherein any subsequent breach would cause the alarm to sound. If the transmission was received when there was no optical fiber breach, the transmission was ignored. This arrangement ensured that the circuit would always sound the alarm when the fiber loop was broken, eliminating the possible situation where the alarm did not sound when the container was opened due to its being remotely turned off during a previous demonstration.

2.3 Results and Discussion

2.3.1 Optical Fiber

All of the epoxies chosen caused significant loss in signal transmittance through the optical fiber during curing over the wavelength spectrum tested. There was little difference in responses observed between epoxies. The change in transmittance as a function of wavelength and time for optical fiber embedded into TETA-hardened epoxy is shown in Figure 2.2. The change in transmittance shown is typical of all the epoxies, including the longer-curing Jeffamine. The first scan taken is represented by the top of the thick upper curve at a relative transmittance of 16-17. Each successive scan decreased in relative transmittance. The bottom of the lower curve represents the last scan taken - seven hours from when the epoxy was initially poured over the optical fiber. The relative transmittance decreased to ~12, representing a signal attenuation of 25%-30% over the meter tested (850 nm was used as the reference).

During curing, epoxies shrink, which ultimately translates to compressive stresses being exerted on the optical fiber. The non-compliant polyimide buffer only serves to translate the load to the optical fiber. The resultant high optical signal losses from fiber strain were unacceptable because even the small container being fabricated may contain up to 100 m of optical fiber. In order to reduce or eliminate straining the optical fiber, a 25 μm layer of silicone (General Electric Silicones, GE RTV 615) was coated onto the optical fiber. Silicone is a very compliant polymer compatible with most epoxies and allows the optical fiber to essentially "float" in the silicone coating. Figure 2.3 shows the change in transmittance as a function of wavelength and time for silicone-coated optical fiber embedded in Jeffamine-hardened epoxy. The relative transmittance curve shown

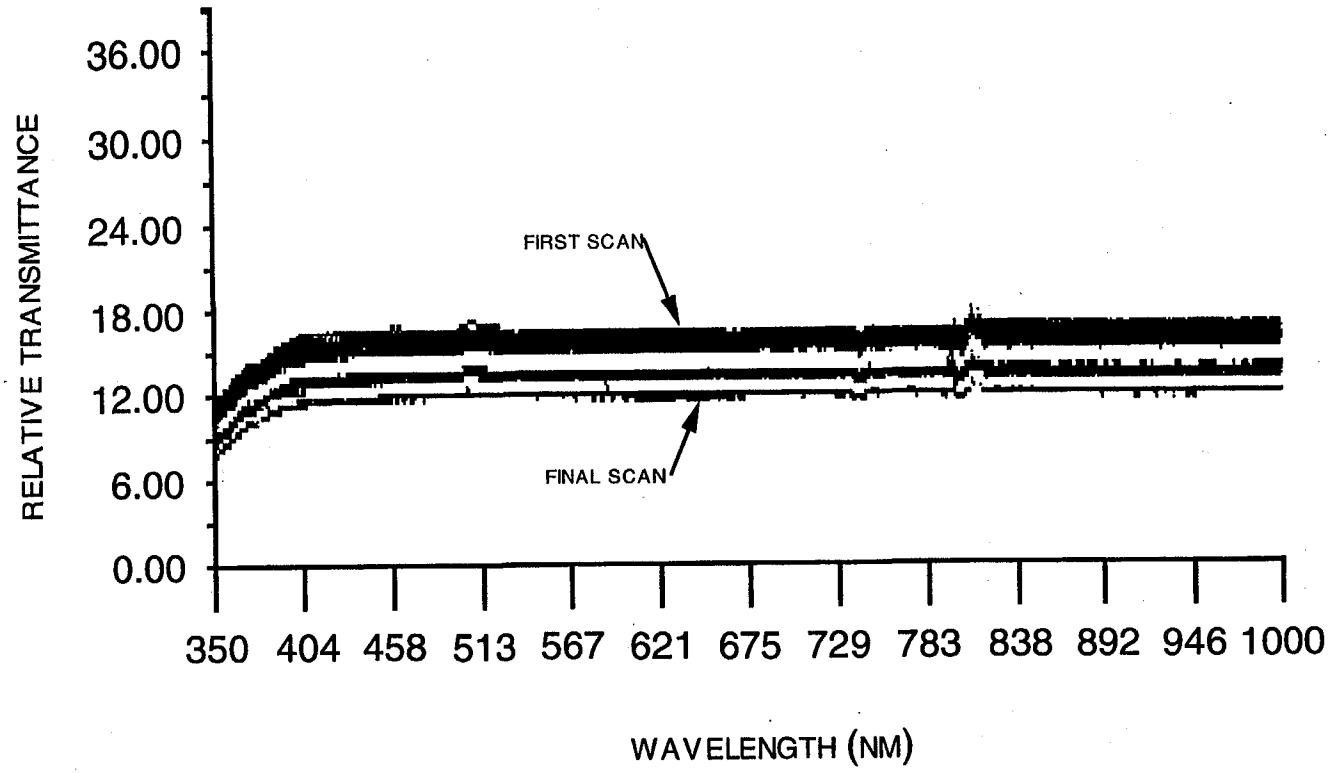

Figure 2.2. Change in Transmittance with Wavelength and Time of Optical Fiber (Polymicro Technologies FH100110125) Embedded in Epoxy (DER 332/TETA) During Curing. Sixty scans were made over seven hours.

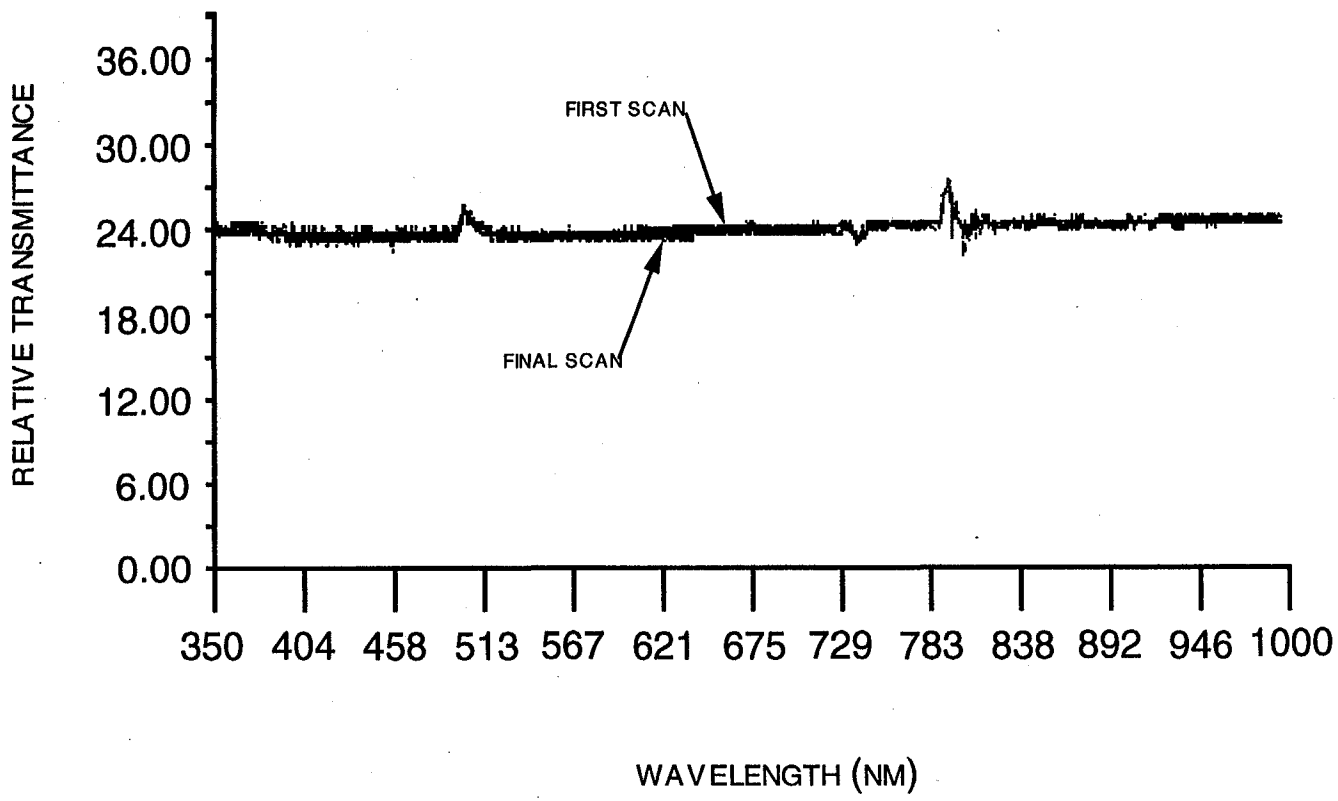

Figure 2.3. Change in Transmittance with Wavelength and Time of Optical Fiber (Polymicro Technologies FHZ100110125) Coated with Silicone Embedded in Epoxy (DER 332/Jeffamine Hardener) During Curing. A minimum of 42 scans were made.

represents 42 hours of scanning, with the very bottom of the curve representing the last scan. The overall relative transmittance loss at 850 nm was essentially zero. Because the epoxy hardened with Jeffamine resulted in similar signal attenuation in the uncoated optical fiber, it was assumed that the reduced signal attenuation was due to the silicone coating absorbing the stresses caused by epoxy shrinkage. Additional work would need to be done to further reduce transmittance losses if larger secure containers are to be realized.

Results of the bend tests are given in Table 2.2. As expected, the signal attenuation increased as the fiber was bent to a smaller radius. A bend radius of 3.5 cm was considered too large to be practical for the present container size. The signal attenuation at a bend radius of 1.3 cm is acceptable for the container size and the transmission capabilities of the fiber. Larger containers with more bends may require varying the fiber and increasing the bend radius to minimize signal attenuation.

2.3.2 Container Fabrication

Three problems were encountered during fabrication of the prototype secure container. The major problem was removing the filament-wound outer shell from the mold. The shell must be able to slide easily from the mold to minimize damage. To facilitate removal, the outer shell mold was remachined with a 3° taper, the mold split, and a wedge inserted to assist in removal of the part. Diagrams of the modified outer shell mold with the inserted wedge are given in Figures A.4 through A.7 (Appendix A). No further difficulties in part removal were experienced.

Several centimeters of free fiber must be available at the two fiber terminals of both the outer shell and drawer after fabrication to provide adequate length for attaching connectors. It is difficult to keep the fiber ends completely resin free while the parts are wound. This problem was resolved by winding plastic film over one end of the fiber and threading the other fiber end under the film after the winding was completed. Resin was then painted over the fiber to avoid contact with the protected ends.

The original molds were designed to create channels on both sides of the drawer to contain the optical fiber connectors so that they would uncouple when the drawer was removed (see Figure A.3). Difficulty in attaching (embedding) the fiber connectors in the two channels and the limited workscope led to the decision to not have the connectors uncouple for the first prototype container (see redesigned mold in Figure A.4). Consequently, for demonstration purposes, audible signal activation (i.e., simulated penetration) required the manual separation of optical fiber connectors. The logistics of attaching the fiber connectors were to be resolved during the next program phase.

2.3.3 Electronics

In order to simplify the drawer design, no optical window for the infrared on/off remote control was provided. The remote control optical pulses must pass through the drawer front wall, which was comprised of embedded optical and strength fibers, before reaching the phototransistor. Although operable, the associated optical absorption and scatter limited the remote control range to several centimeters. Increasing the distance of remote control operation was to be undertaken in the next program phase.

Table 2.2. Signal Attenuation (in decibels/bend) from Bending Optical Fiber Used in Fabricating a Prototype Smart Secure Container*

Mandrel Radius (cm)	Wavelength (nm) 650	850
3.5	NL#	NL
1.3	0.02 db/bend	0.04 db/bend
0.95	0.04	-----
0.63	0.08	0.06

* Polymicro Technologies, Inc. Fiber FHZ100110125.
\# NL = no apparent loss.

The container used four AAA batteries capable of powering the electronics for approximately 168 hours (7 days) of operation. Battery life is the limiting factor for any portable smart structure. A "sleep mode" could be introduced that shuts off the batteries during periods of inactivity. The electronics could then be reactivated by one of several methods, for example, container movement, surface interaction, or remote control.

2.4 Applications

The work was performed to demonstrate the capabilities of optical fiber smart structure technology and to serve as a basis from which to expand smart structure capabilities. Electronically active secure containers such as the one fabricated in this study could be expanded to almost any size with careful selection of optical fiber, container design, and compatible electronics. Large containers for shipping, field use, or storing stationary objects could also be prepared with a passive system (without active electronics), with container integrity being checked periodically with an OTDR. Polymer matrix adaptability permits the fabrication of complex-shaped containers and allows additional smart structures to be embedded. Having all of the container's components embedded increases container ruggedness and security.

Smart structure electronics could be adapted and expanded to perform almost any function. For the container prepared in this study, tampering with the optical fiber triggered a buzzer. Capacitors, telemetry, destructive devices, or sensors could also be activated by the triggering mechanism. Electronics could be expanded to include real-time recording of container intrusion, remote activation, and communication with other smart structures.

The concept of smart materials fabricated from optical fibers has application beyond secure containers. Wall panels could be prepared in a manner similar to a secure container wall, only on a larger scale. Panels could be prepared that join and interlock so that the resultant wall becomes a single unit. Temporary secure buildings and limited access areas could be created in this manner.

The concept of polymer-embedded optical fiber-based smart materials developed in this study is also adaptable to sensors. Chemical sensors could be prepared by embedding an optical fiber array into a polymer sheet that is then coated with another polymer sensitive to the specific chemical. As the sensitive coating comes in contact with the chemical, it swells which places pressure

on the optical array. Changes in the optical fiber refractive index could be detected through light attenuation. Special pressure sensors could also be designed using the same concept, with the pressure being exerted directly on the embedded optical fiber. The chemical or pressure sensors could be single, stand-alone units, or be part of a secure container wall.

2.5 Conclusions

The prototype secure container prepared in this work is an example of an optical fiber-based smart structure. Several fabrication problems were resolved. The electronics package performed as designed and although functionally basic, revealed the possible electronic functionalities that could be built into optical fiber smart structures. The primary limitation to electronically active portable structures continues to be battery life.

The knowledge gained from fabricating the secure container could be applied to other secure containers, smart wall structures, and pressure-based sensors. Through judicious selection of materials and fabrication methods, a host of optical fiber-based smart structures could be prepared.

3.0 Optical Fiber-Based Secure Container for Secure Video Applications

3.1 Introduction and Objectives

3.1.1 Introduction

Optical fibers have been the basis of advanced polymer composites used to prepare intelligent structures. Optical fibers are small, immune to electromagnetic interference, are lightweight, can be embedded in other materials, have an adjustable composition, and can operate in harsh environmental conditions. Optical fiber-based smart structures have the ability, via embedded or attached optical fiber (the smart material) and the associated electronic circuitry, to monitor the polymer's physical integrity and structural behavior during use. The unique ability of optical fiber to act as a signal transmitter as well as to modulate a propagating optical signal as a response to external stimuli has led to numerous applications of optical fiber-based smart structures. Although capable of detecting electrical and chemical phenomena, optical fiber sensors have been developed primarily for determining strain, thermal expansion, and vibration of structural components.

Non-optical glass or polymer fibers are typically embedded into polymer structures to enhance strength and toughness. Replacing a portion of the structural fiber with optically conducting fiber permits fabricating robust, optically-active structures such as secure containers. Secure containers are optical fiber-based smart structures that offer the ability to continually, intermittently, or passively monitor the integrity of the container walls. Continually monitored secure containers monitor in real-time, with container breaching activating the smart structure. Smart structure activation can lead to numerous consequences within the container, depending on the specific container application, container size, and the complexity of the accompanying electronics. At a minimum, smart structures can be given the ability to recognize and record container breaching. Difficulty in defeating the secure container depends on the smart material's stealth and the smart structure's complexity, which can be provided by the smart material being incorporated into the container walls.

Sandia National Laboratory (SNL) was preparing a field-worthy stationary surveillance video system that was housed in a rectangular, six-sided, metal box with a hinged lid. It was imperative that the metal box be secure even with camera lens viewing ports, vent holes, and power/connection cabling ports machined into it. It was also important that the video system be easily accessible when necessary. It was not necessary that the box security system be impenetrable, only that it be tamper-proof.

Pacific Northwest National Laboratory (PNNL) has prepared secure containers by filament winding optical fiber around a preform and then embedding the fiber in a polymer matrix via resin transfer molding. In this manner, a secure container was prepared that uses continually monitored optical fiber as the smart structure. A small matchbox-shaped container consisting of an inner drawer within an outer shell was fabricated from polymer resin. The optical fiber was sandwiched between additional non-optical, strength-promoting fibers and embedded into the polymer. The additional non-optical fiber provided strength to the container, protected the optical fiber from damage, hid the fiber, and acted as a decoy. The optical fiber was wound with a winding density such that a high probability of fiber damage would be expected if the container was penetrated. The inner drawer and outer shell were wound with optical fiber that optically couples when the two halves are put together

to form a continuous optical pathway. Electronic circuitry located in the base of the inner drawer sent and received an infrared signal through the fiber several times a second. For demonstration, when the drawer was opened, interrupting the fiber loop and creating a container breach, an alarm beeper was activated. The beeper could be turned off via an infrared remote control. When the drawer was re-closed, the alarm circuitry automatically reset so that a subsequent breach again set off the alarm.

PNNL was contracted by SNL to design and fabricate a similar optical fiber-based secure container that would be compatible with both the video camera system and its metal box. Work began in August 1993 under a time constraint to finish the container as soon as possible. This time constraint, and especially the limitations introduced by the metal box design, influenced many decisions during design and fabrication. Differences in the actual secure system fabricated compared with the design that would have been implemented without the metal box limitations are noted throughout the report.

3.1.2 Objectives

The objectives of the study were to fabricate a secure container compatible with the SNL video system and the metal box, including securing the perimeter of round openings and the lid; identify potential problems associated with secure container design and fabrication; and ascertain advantages and disadvantages of the secure container and its potential.

3.2 Secure Container Fabrication

A Hoffman metal box was received from SNL in August 1993. A 2.5-cm diameter hole was machined into the front for power cabling by PNNL. The two 5.1-cm holes for the video camera lenses were to be machined into the metal box lid by SNL at a later date. A separate grouping of 15 small air vent holes, 1 mm in diameter, was machined into one side of the box by PNNL per SNL's request. The convention used throughout the report to label top, sides, etc. is as follows. If the metal box was positioned with the lid opening up and away from you (the hinge horizontal), the bottom was against the floor, the back was the side under the hinge, the front was opposite the back, the two sides were the other two vertical sides of the box, and the lid was the top.

The secure container consisted of two parts: 1) a series of panels comprised of optical fiber wound around polyurethane foam and 2) an electronics package. The project was completed in three phases. The first project phase was to design the container and electronics and determine a suitable optical fiber for filament winding. The second phase was to wind a test panel to evaluate the winding process (especially related to optical signal transmission), and assemble the electronics package. The final project phase involved winding the panels, final assembly, and testing. Container fabrication is presented in order of the phases presented above.

3.3 Phase 1: Secure Container Design, Electronics Package Design, and Optical Fiber Selection

3.3.1 Secure Container Design

Designing and fabricating the secure container as a new concept without constraints would involve filament winding optical and strength-enhancing fibers into a rectangular, five-sided preform followed by resin transfer molding to embed the fiber. This composite box plus a similarly fabricated lid, both molded to size, would replace the metal box, which was considered an integral part of the video system housing package. If the constraint of fabricating a secure container involved beginning with a simple metal box with a hinged lid, a secure container exactly like the one indicated above could be fabricated and inserted into the metal box and under the lid as a "secure liner." However, the secure liner method could not be used for the secure video application due to a feature of the metal box. The opening under the lid had a lip around the perimeter that overhung the box interior. This feature precluded creating a second, optical fiber-wound container that could be slipped into the metal box as a lining. Consequently, the secure lining for the metal box had to be fabricated in six parts (i.e., panels) so that each panel could be positioned properly on the bottom or under the lip to assure security. The secure container lid panel was designed to be optically coupled via two pin connectors to side-wall panels so that jarring or opening the lid would trigger the alarm.

The secure holes required for the video system presented a special design and fabrication problem for the secure container. Simple filament winding in only one direction, like that chosen for the panels, did not allow any of the panel area adjacent to the hole to be covered by fiber unless winding was performed in multiple directions (envision infinite straight lines tangent to a circle). Optical fiber windings in different directions to secure the hole would result in an unacceptable build-up of fiber near the edge of the hole from overlap and require at least a 50% increase in fiber length. Consequently, alternative methods of winding the holes were pursued. The accepted design and method was to wind a separate fiber into a spiral to create a fiber "disk" tens of centimeters in diameter. The inner diameter of the fiber spiral equaled the hole's diameter. Extra fiber was left at either end of the spiral for direct splicing to the remaining wound fiber on the panel.

3.3.2 Electronics Package Design

Preparing the secure container in separate parts provided an opportunity to create an electronics package that allowed each panel to be monitored individually if desired (a composite container may have used only two fiber loops– the box and the lid). Consequently, seven circuits were prepared, one for each panel and a spare. Although the video system will in practice have access to external electrical power, the secure container circuitry was designed with battery power for demonstration purposes. A detailed circuit description follows.

The circuit was powered by four C batteries connected in series to provide a total of 6 volts. An on/off switch was inserted immediately following the battery so that when the switch is off, no current flows. A 1N4003 diode placed in series with the switch provided protection against incorrect battery polarity and also dropped the battery voltage by approximately 0.7 volts. The resulting 5.3 volt level was used for Vss (the supply voltage) throughout the rest of the circuit. Integrated circuit (IC)9 is a low-power DC-DC converter which was configured to output -12 volts. The -12 volt output voltage appeared on pin 5 of IC9 and was used as Vee (laser diode voltage supply) for the laser diode drivers, IC1-IC7.

IC10 is a CMOS dual-timer chip which was used to generate pulses with 9 milliseconds duration and 10% duty cycle. The 5 volt amplitude pulses appeared at pin 9 of IC10. IC8 and IC11 were non-inverting buffer/driver chips which provided an interface between the CMOS 556 (IC10) and the TTL-based IR3C01 laser diode drivers (IC1-IC7). After being buffered by IC8 and IC11, the pulses were connected to pin 5 of IC1-IC7. These seven IC's were laser diode drivers, which drove the Seastar #CL-100-10 laser diode modules (the actual laser diode housed in the CL-100-10 was a Sharp LT015MD). The laser diodes, TX1 through TX7, had a built-in photodiode which could be used to monitor and stabilize the output power of the laser diode, providing stability over a wide range of ambient temperatures. The IR3C01 made use of the built-in photodiode for this purpose, and also provided a "soft start" function which protected the fragile laser from being destroyed due to current overload caused by power supply spikes, etc. The output power level of each laser diode was set by its associated 100K potentiometer. When the signal on pin 5 of IC1-IC7 was TTL high, the laser was turned on and operated at the pre-set power level. When pin 5 went low, the laser was turned off.

After traversing the optical fiber, the optical pulse arrived at the Seastar CP-100-10 photodiode receiver, RX1-RX7. The receiver module contained a Fujitsu FID08T13TX silicon photodiode. The signal current from the photodiode was applied to pin 6 of the combination op-amp/comparator LM392, IC12-IC18. Pin 6 was the inverting input of the op-amp. The op-amp was connected in a transimpedance configuration which converted the photocurrent into a voltage via the feedback resistor between pins 6 and 7 of the IC. The signal at pin 7 was a 9 milliseconds, positive voltage pulse with an amplitude corresponding to the intensity of the laser light arriving at the photodiode. This voltage pulse was applied to the inverting input (pin 2) of the comparator portion of IC12-IC18. The 200KΩ and 100KΩ resistors form a reference voltage of 0.002*Vss against which the voltage pulse was compared. The comparator was an open-collector output device, which was pulled up to Vss by a 330KΩ resistor. If the voltage pulse was greater than 0.002*Vss (approximately 10 mV with fresh batteries), the comparator output went to zero volts. When the voltage pulse was less than the reference voltage, the comparator output went to 5 volts. Therefore, the signal at pin 1 of IC12-IC18 was an inverted version of the original modulation signal from IC10. Note that DIP switches S1-S7 were used to disable the output of IC12-18, respectively, by grounding the output stage of the comparator thereby keeping the signal at zero volts regardless of the optical signal present at the corresponding photodiode.

IC19 was a 4075 CMOS triple three-input OR gate. The outputs of the comparators were applied to the inputs of the OR gates in such a way as to give a low logic level at pin 10 only when all seven of the comparator outputs were simultaneously low; if any or all of the comparator outputs were high, pin 10 would go high. Due to the signal inversion at the comparator, in the absence of light the comparator signal was a high logic level. Therefore, if one or more of the fiber optic loops was broken, pin 10 of IC19 would always remain high, even when the signal from the unbroken loops went low as their optical pulse was detected. If no fiber loops were broken, or if all broken or inactive loops were disabled using S1-S7, pin 10 of IC19 output a pulse train which was at a high logic level for 81 milliseconds and a low level for 9 milliseconds, which was an inverted version of the original modulation signal from IC10. Pin 10 of IC19 was connected to a "missing pulse detector" circuit implemented by Q1 and IC22. The output of the missing pulse detector appeared at pin 3 of IC22. This signal would remain at a high logic level only as long as pulses arrived continually from pin 10 of IC19. Thus, if one or more of the fiber optic loops was broken, the missing pulse detector saw a steady high logic level as opposed to a pulse train, and the logic level at pin 3 of IC22 went low.

The output logic level from pin 3 of IC22 was fed to a logic section consisting of IC20 and IC21. IC20 was a 4011 quad 2-input NAND gate and IC21 was a 4013 dual D flip-flop. The function of these two IC's was to implement a reset capability which silenced the piezoelectric buzzer

when a fiber loop was open, as is often desirable when demonstrating the function of the secure container. As long as the reset switch (a momentary normally open switch) was left open, this logic section inverted the output of the missing pulse detector, with a low logic level appearing at pin 4 of IC20 when the container was not breached, and a high logic level when one or more fiber loops was open. Pin 4 of IC20 was connected to a piezoelectric buzzer excitation circuit consisting of the buzzer and Q2. A high logic level on pin 4 of IC20 caused the excitation circuit to oscillate, sounding the buzzer. When one or more fiber optic loops was open and the buzzer was sounding, a momentary closure of the reset switch applied a high logic level to the clock input of the flip-flop (IC21), which caused the output of IC20 (pin 4) to change level, thereby silencing the buzzer. Subsequent closings of the reset switch effectively toggled the output (pin 4) of IC20, which in turn toggled the buzzer on and off. The reset switch was ignored if it was pressed when none of the fiber optic loops was open. In addition, if the buzzer had been silenced by the reset circuit, the buzzer was automatically "re-armed" when the optical signal was re-established so that subsequent container breaches would always sound the alarm, regardless of the reset state the circuit was previously left in.

3.3.3 Optical Fiber Selection

Optical fiber characteristics were chosen based on the secure container application. Each panel would require from 500 to 900 m of fiber of which 50 to 100 m would be in bending mode; therefore, signal attenuation had to be minimal. The fiber was to have a large glass core and cladding, be multimode, have an overall diameter including buffer of 250 μm or less to meet the client's secure spacing requirement, have low bending loss characteristics, be operational in the near-IR to minimize attenuation, be compatible with the silicone polymer used for coating the fibers, and be relatively inexpensive. Commercial-grade optical fiber was obtained from Corning Incorporated that met the requirements, the characteristics of which are listed in Table 3.1.

After filament winding around the polyurethane panels, the fiber was painted with silicone (Dow Corning Silastic 932 RTV [Dow Chemical Company]) to bond it to the panel and for general damage protection. A test was performed in order to determine the effect of having the optical fiber in contact with the curing silicone. Often solvents in polymer resins will attack fiber buffer coatings and polymer resin shrinkage (or expansion) can induce strains in the fiber causing signal losses. The latter phenomena was observed in previous secure containers fabricated using epoxies at PNNL.

For the test, a known length of fiber, typically a few meters, was coiled and placed into the bottom half of a 500-ml polyethylene bottle. The fiber ends were cleaved and attached to a spectrophotometer (U.O.P. Guided Wave, Inc. Model 100 Spectrophotometer) that transmitted light pulses over a wavelength range of 350 to 1000 nm. The spectrophotometer measures transmittance as a function of time and wavelength. An ultraviolet/near infrared transmissive fiber was used as the standard reference cable. A transmittance measurement was taken on the coiled fiber (representing time zero) and then the silicone poured over the fiber to embed it. Transmittance measurements were taken on the fiber at approximately 10-15 minute intervals until the silicone cured.

The change in transmittance as a function of wavelength and time for the Corning optical fiber as-received and after embedding into Dow Corning silicone is shown in Figure 3.1. The as-received scan is represented by the upper curve and the lower curve represents the last scan taken approximately 23 hours from when the silicone was initially poured over the optical fiber. The change in relative transmittance observed at 850 nm (~4%) is within experimental error (3%-5%), indicating negligible signal attenuation over the 5 m of fiber tested. Negligible transmission loss was

Table 3.1. Optical Fiber Characteristics*

- Composition: Silica/Silica (Core/Cladding)
- Graded Index
- Buffer Composition: Acrylate
- Core/Cladding/Buffer Outer Diameters: 100 μm/140 μm/250 μm
- Operating Temperature: -60°C to 85°C
- Effective Index of Refraction: 1.51 @ 850 nm
- Attenuation at 850 nm: 3.6 db/km
- Cost: $0.33/m

* Obtained from Corning Incorporated: Fiber 100/140 CPC3.

expected because silicone is a very compliant polymer unlikely to induce strains in the fiber and the acrylate buffer was expected to be quite resistant to chemical attack from the acetic acid used as the solvent.

Because the optical fiber will make numerous bends when wound into the container, a series of tests were performed on the optical fiber to determine the loss in transmission when the fiber is bent. One end of a five meter length of optical fiber was attached to an OTDR. The remaining fiber was wound over a series of mandrels with radii of 0.64, 1.0, 1.2, and 1.4 cm and the signal attenuation measured at a wavelength 850 nm. A new length of fiber was cut for each test.

Results of the bend tests are given in Table 3.2. As expected, the signal attenuation increased as the fiber was bent to a smaller radius. The signal attenuation did not reach an acceptable value until a bend radius of 1.4 cm. It should be noted that in the process of investigating attenuation losses in the wound panels by mandrel bending testing, a variety of candidate fibers were similarly tested with a 1.4-cm bend radius. The original fiber chosen (Corning 100/140 CPC3) was found to be the best performer.

Table 3.2. Percent Signal Attenuation from Bending Five Meters of Corning Optical Fiber* Around Mandrels of Graduated Radii

Mandrel Radius (cm)	Percent Attenuation
1.4	<1%
1.2	30%
1.0	30%
0.64	70%

* Fiber 100/140 CPC3.

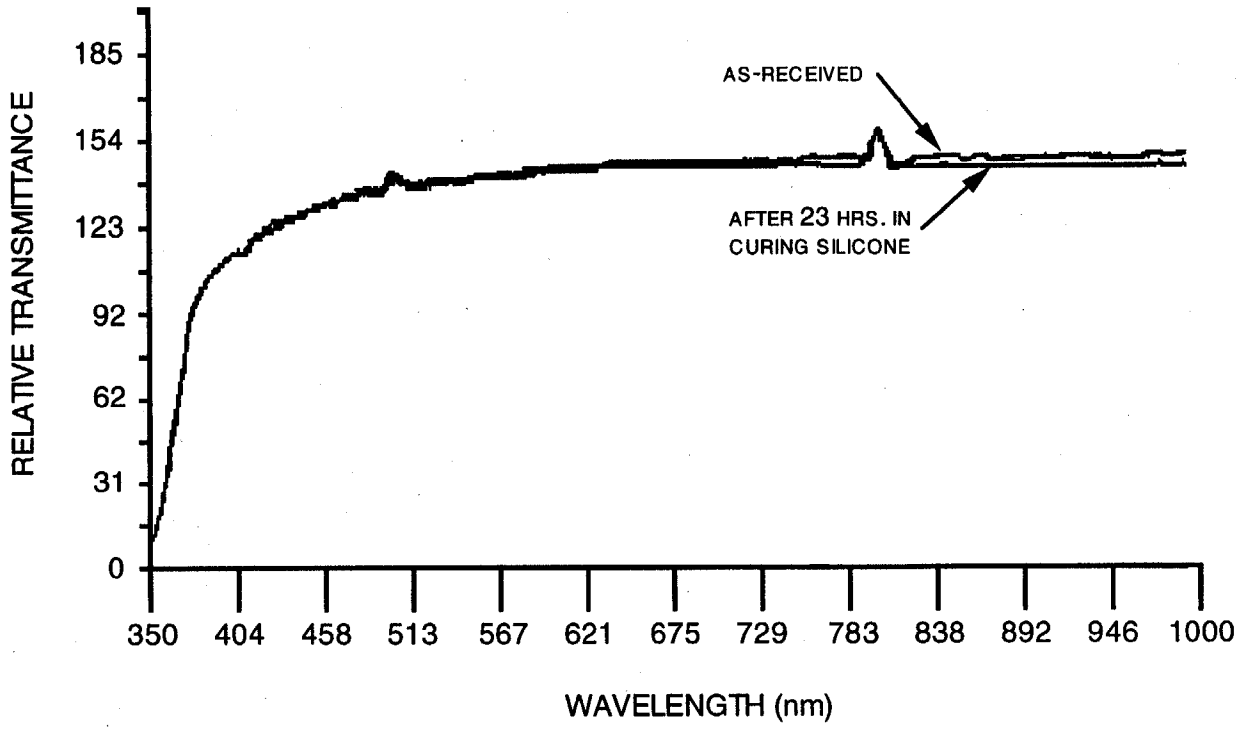

Figure 3.1. Change in Relative Transmittance as a Function of Wavelength of Optical Fiber (Corning Incorporated 100/140 CPC3) As-Received and After Embedding in Curing Silicone (Dow Corning Silastic® 932 RTV) for 23 Hours

3.4 Phase 2: Filament Winding of a Test Panel and Electronics Package Assembly

3.4.1 Filament Winding of a Test Panel

The test panel consisted of optical fiber wound around an 18 lb/ft^3 polyurethane foam core. The polyurethane foam core was used because it was readily available. Lighter, less dense polymers for the panels would have been preferable to help keep the containers as light as possible. A test panel was fabricated by machining a block of 2.86-cm thick polyurethane foam to an approximate size of 30 by 50 cm. The shorter sides were machined to create a semi-continuous curve 2.86 cm in diameter. The panel was mounted in a filament winding machine to allow it to be freely rotated about the transverse axis. The fiber was wound onto the panel and held in place with a light coating of silicone. The panel contained approximately 640 m of fiber plus several meters of fiber left at either end for connection. The test panel is shown in Figure 3.2.

The wound fiber was tested with an OTDR at 850 nm. Results indicated that almost all of the signal was being lost within the first 100 m. After verifying that the phenomena was real and the test results valid, the leading potential cause of the losses was considered to be strains introduced into the fiber during the winding process. After an additional two to three test panels were wound, a procedure was established to reduce signal attenuation by minimizing pulling and twisting of the fiber during winding. However, decreasing the tension on the fiber resulted in a looser, less acceptable winding. To maintain fiber alignment, the rounded edges of the polyurethane foam were remachined concave to allow a 2.86-cm diameter threaded nylon rod to be attached in lieu of the rounded foam edges. The threads acted as spacing guides for the fiber. Panels wound with this configuration showed an acceptable level of signal attenuation over the entire fiber.

3.4.2 Electronics Package Assembly

The electronics were assembled per the schematic diagrams given in Appendix C. The circuit was point-to-point soldered on two prototype style circuit boards. The boards were mounted on an aluminum sheet metal enclosure which was attached to the back and side of the box. This enclosure served to protect the circuitry as well as the optical fiber leads. No serious problems were encountered during assembly and testing. Correct circuit function was confirmed by unplugging, individually or in combination, each panel's optical fiber connection at the laser source and/or detector receptacle, simulating a fiber break. The battery life was determined to be approximately 4 days at continuous operation. When the batteries become discharged, the circuit's failure mode is to continuously sound the buzzer even when no fiber breaks are present.

3.5 Phase 3: Panel Winding, Final Assembly, and Testing

3.5.1 Panel Winding

Six separate panels were wound using the procedure described above for the final test panel. Threaded nylon rods were bonded to the edges of the foam core on opposite sides to provide spacing grooves for the optical fiber and eliminate fiber overlap. The spacing between adjacent threads was 488 μm. The fibers have an outer diameter of 250 μm so the space between fibers was 238 μm.

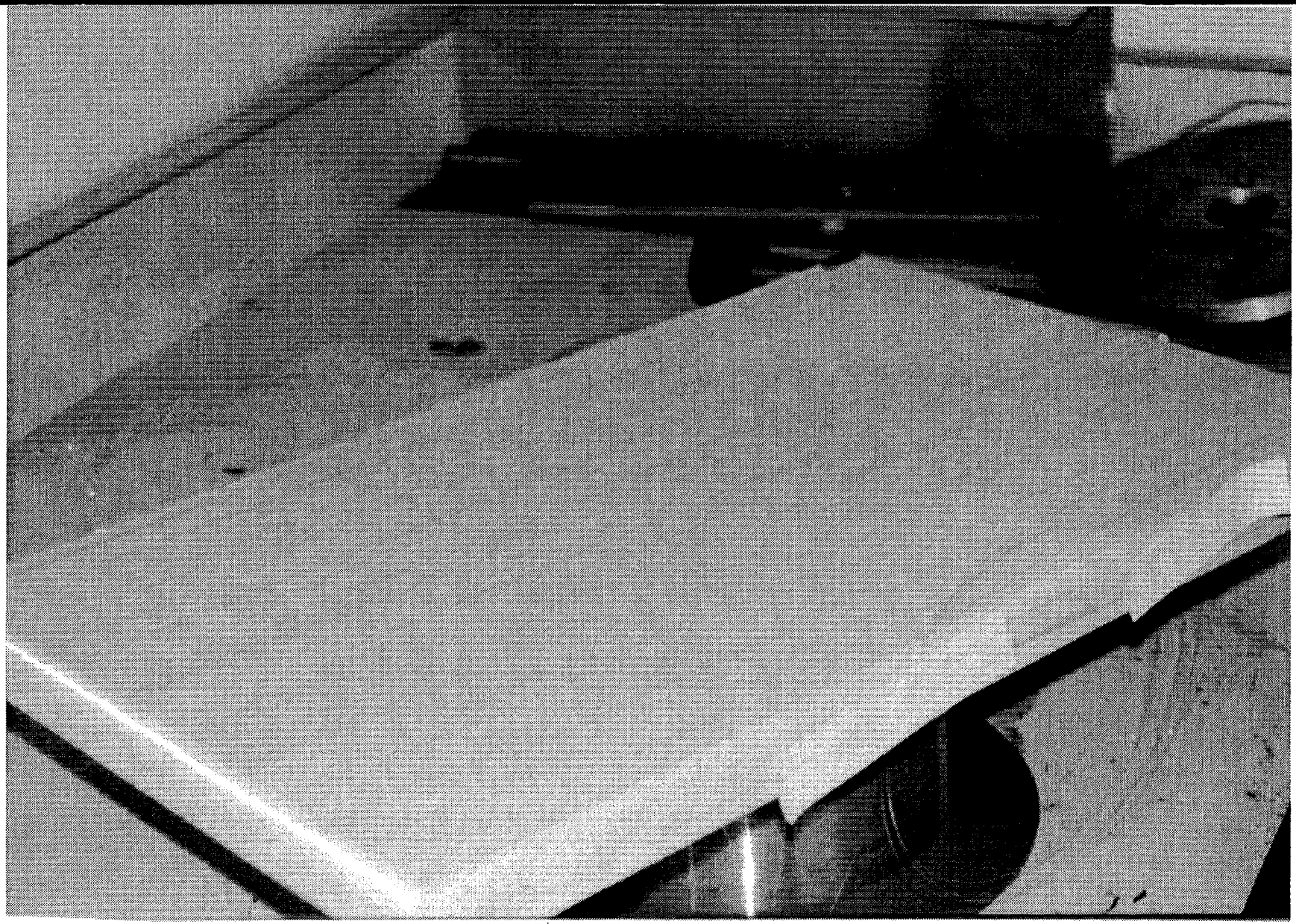

Figure 3.2. Test Panel Comprised of 650 m of Corning Incorporated 100/140 CPC3 Fiber Wound Around Polyurethane Foam (30 cm x 50 cm x 1.4 cm)

The optical fiber was wound around each 2.86-cm-thick panel in one continuous length. The sizes of the six panels and the approximate fiber quantity required to wind them were as follows (using the panel labeling convention given in first paragraph of Section 3.2):

- side, 2 each - 50 by 30 cm - 640 m
- front, 1 each - 44 by 30 cm - 580 m
- back, 1 each - 44 by 30 cm - 545 m
- top, 1 each - 44 by 44 cm - 805 m
- bottom, 1 each - 44 by 44 cm - 831 m.

The front and back panels were wound vertically and the side panels were wound horizontally. This arrangement allowed a rounded edge to abut a flat face so that there was no gap between the panels. The top and front panels had through-holes that required special treatment to assure that the optic fibers covered the entire panel except for the holes. Since the fiber was wound in only one direction, each hole left an uncovered band the same width as the hole. Figure 3.3 shows the band left after the top panel was wound.

Spiral wound fiber was used to cover the space around the holes. These spiral disks were wound using a fixture with a hub the same diameter as the hole and two plates spaced 76 μm wider than the fiber diameter. Spokes were cut into the two plates to provide access to the fibers so that they could be bonded in place with silicone adhesive. When the adhesive was cured, the spirals were removed from the fixture intact without unwinding. The top panel had two holes on the same center line. Two spiral disks, 25 cm in diameter, were wound to secure the holes. These disks were large enough to overlap each other and the panel edges so that there were no unprotected areas on the panel. The disk wound for the front panel was 13 cm in diameter to surround the single hole. The unfilled gap on the front panel not covered by the disk was filled with angled windings. The spiral windings were optically coupled in series with the flat windings in each panel. The spiral disks wound and mounted to secure the two holes in the top panel are shown in Figure 3.4.

Holes in the side panel for air ventilation were small enough (1-mm diameter) to allow the fiber to be flexed around pins placed through the foam panel. After the fibers were bonded in place, the pins were removed to leave an air passage through the panel. These holes matched the holes drilled into the metal box.

3.5.2 Final Assembly

The completed panels were coated with Dow Corning Silastic 932 (black) RTV to protect the fibers from damage and to hold them in place. The panels were then arranged in the metal box so that there was less than a 250-μm gap between panels at the corners. During this step the fiber ends were routed to the bottom rear of the box where they were connected to the electronic couplers. After the panels were positioned in the box, they were lined on the inside with 0.6-cm thick polyurethane foam to provide additional fiber protection and a surface to bond to for internal structures. A similar lining was bonded to both faces of the top panel (i.e., the lid) and strap handles attached so that it could be easily attached and removed. Figure 3.5 shows the inside of the completed box with the electronics mounted in the aluminum housing and Figure 3.6 shows the top panel (lid) in place. Optical continuity was attained between the top panel (lid) and the rest of the secure container by bonding two sets of optical mating connectors to the lid and the secure container walls. In this manner, the alarm would sound not only if a panel was breached, but also if an attempt was made to remove the lid.

Figure 3.3. Top Panel Showing Band Not Covered By Optical Fiber Resulting from Winding Around the Holes

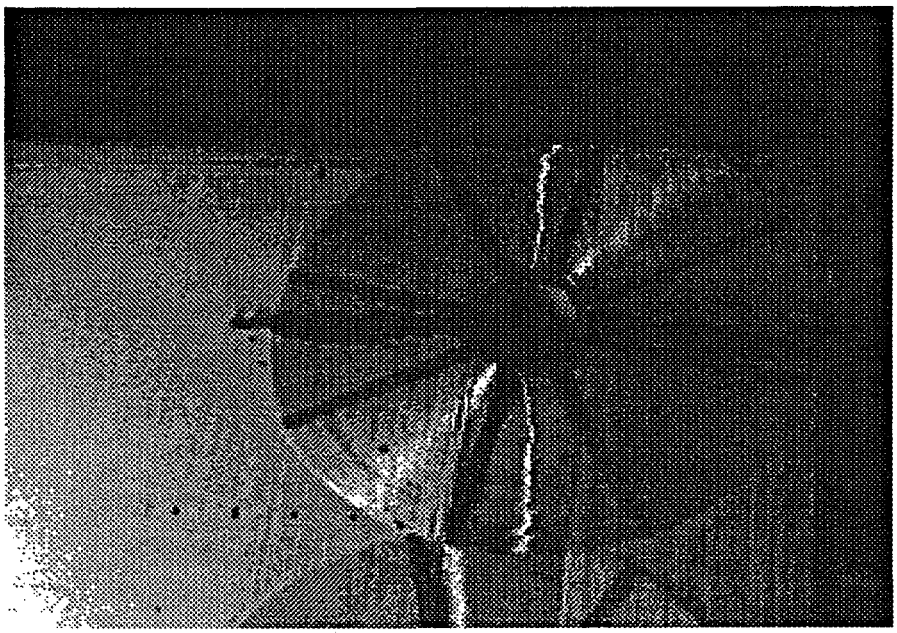

Figure 3.4. Top Panel Showing Spiral Disks Securing Each Hole Mounted over the Flat-Wound Fiber. The dark lines are silicone rubber on either side of the fiber disk used to bond the fibers together. Holes are 5-cm diameter.

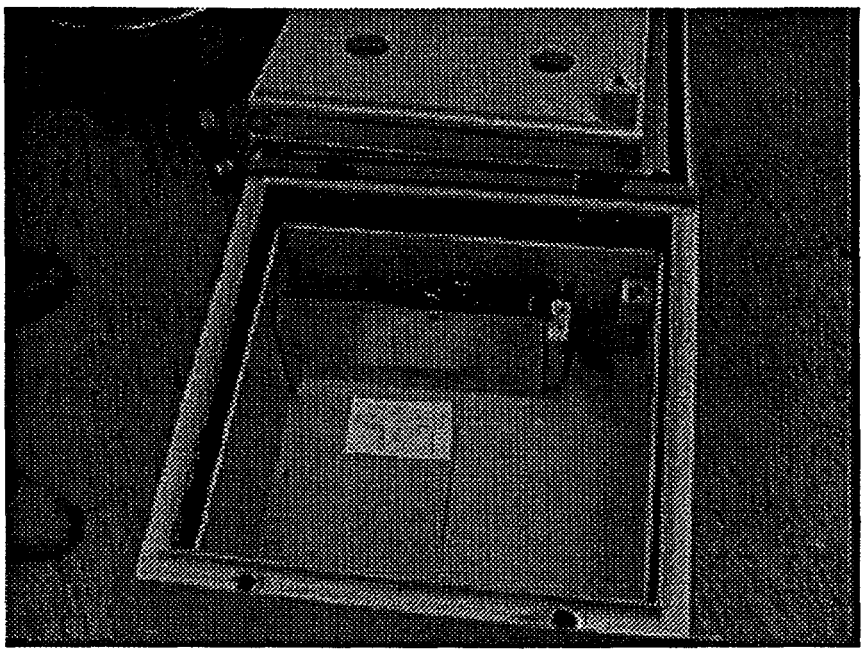

Figure 3.5. Interior of Completed Secure Container Showing Interior Polyurethane Lining Bonded over Optical Fiber-Wound Panels. Electronics are assembled in the aluminum housing.

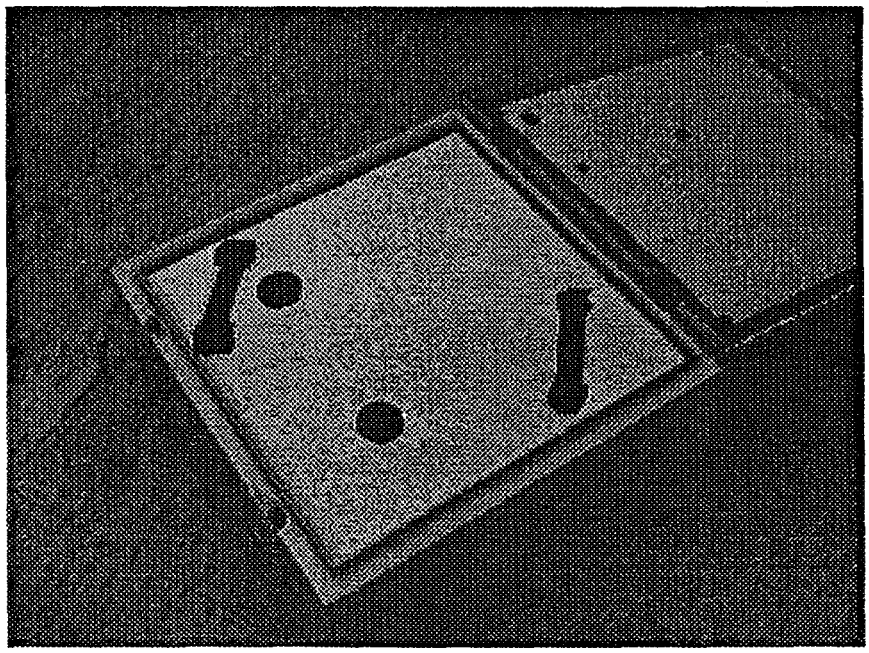

Figure 3.6. Top Panel (Lid) in Place Showing Video Camera Lens Holes

The various features of the individual panels which make up the box caused some of the panels to have less optical attenuation than others. Therefore, in some cases it was possible to drive more than one panel per laser diode. This is the reason that, even though seven laser diodes are provided, only four were used. When shipped from PNNL, the panels were connected as follows:

circuit #4: top
circuit #5: right side
circuit #6: back-left side
circuit #7: front-bottom.

Panel location designation was given in the first paragraph of Section 3.2.

The optical fibers were terminated with ST style connectors. The fibers were epoxied into the connectors and subsequently polished to an optical quality finish. Most of the fiber connectors were accessible in the electronics enclosure. The exceptions were the connectors associated with the two windows in the top panel. Since each of these windows was wound separately, they had to be connected in series with the top panel. These connections were buried in a cavity within the box lid, so were not accessible. There were 14 connectorized fibers accessible in the electronics enclosure– two for each of the six panels, plus two for the circle winding around the hole in the front panel. These connectors were identified by a black marking on the blue rubber strain-relief of each connector. The meaning of the marks is as follows:

T = top (lid) panel
R = right panel
Back = back panel
F = front panel
FCirc = front hole circle
B = bottom panel.

When panels were linked in series, as was the case with circuits #6 and #7, the interconnections were mounted to the electronics enclosure plate. If access to the electronics or optical fiber connections was needed, caution was necessary in handling the enclosure since several of the optical fibers protruding from the back corner of the box were rather short– as short as 15 cm or so. Therefore, the enclosure plate should be carefully laid over onto the bottom of the box, not pulled away from the box walls.

3.5.3 Testing

Testing performed on the completed secure container was a check of the electronics and removing the lid to activate the buzzer.

3.6 Container Features

The present work was performed to demonstrate the feasibility of fabricating an optical fiber-based secure container to house a video camera system. Electronically active secure containers such as the one fabricated could be constructed to almost any size with careful selection of optical fiber, container design, and compatible electronics. Secure containers could also be prepared with passive systems (without active electronics), with container integrity being checked periodically with an

OTDR. If constructed as a single-walled composite container of optical fiber wound and molded into a polymer matrix, complex-shaped containers could be fabricated. Compared with the video system secure container prepared from wound foam panels, embedding the optical fiber and the container's components in a polymer matrix increased its ruggedness and security.

The secure container's electronic circuitry was designed to demonstrate a basic example of the functionality that could be built into such containers. The possibilities are really only limited by the space and electrical power available. For instance, if power consumption is not an issue, the laser diodes could be operated continuously rather than in pulsed mode, which would greatly increase the speed of response (which was limited by the pulse repetition rate to approximately 90 milliseconds) in detecting a container breach. The circuitry could be powered by the same AC source which powers other instrumentation within the box.

The secure container's electronic circuitry could be adapted and expanded to perform almost any function. For the secure container prepared for the SNL video system, tampering with the optical fiber or lid activated a buzzer. Discharging capacitors, telemetry, destructive devices, mechanical action, writing of information to an EEPROM, and sensors are just some of the responses that could also be activated by the triggering mechanism. Electronics could be expanded to include real-time recording of container intrusion, remote activation, periodic interrogation, and communication with other smart structures. Depending on the container application, circuitry could be designed and miniaturized, for example, to reduce power consumption. The secure container circuitry demonstrated in this study should be viewed as a starting point, instead of an end point.

The secure container prepared as-is as a component system provided excellent flexibility in design and fabrication. The multiple-panel design allows the flexibility of preparing panels differently and if desired, of monitoring each panel separately. Having fibers present on both sides of a panel doubles the chances of detecting intrusion.

Disadvantages of the wound foam panel approach include added weight (the secure container doubled the weight from 32 to 67 lbs) and loss of space inside the container for the video system. The insulating qualities of the foam decreases heat transfer, making it more difficult to cool the video electronics. The secure container as-prepared was not completely compatible with the as-prepared video system mounting brackets. However, the incompatibility was the result of designing the video system apparatus prior to constructing the secure portion of the metal box. Secure container side panels had to be 2.86-cm thick which used all of the space available under the metal box lip, precluding the use of the video system mounting brackets. If designed as an integrated system, preparing compatible video and secure components is considered a minor task.

The study undertaken by the PNNL Secure Container Team had three objectives. The first objective was to prepare a secure container compatible with the SNL video system, including securing the round openings (holes) and lid. This objective was met except for having the secure container be completely compatible with the as-prepared video camera mounting apparatus. However, it was concluded by both SNL and PNNL that the shortcoming was due to designing the video system apparatus prior to constructing the secure portion of the metal box. The second objective was to identify and overcome problems associated with secure container preparation. The most difficult problem encountered was securing the holes which was resolved by winding spiral fiber disks around each hole. A considerable amount of time was also spent learning to wind the panels so that the fiber would not be stretched or twisted. The final objective was to determine the pros and cons of the secure container prepared. Although the objective was met to fabricate a secure container, without

the constraints placed on construction, the panel method would not have been chosen. Instead, a composite secure container of optical fiber embedded into a polymer matrix would have been prepared.

4.0 Smart Tamper-Indicating Windows

4.1 Introduction and Objective

4.1.1 Introduction

Incorporating secure, tamper-indicating windows into secure containers was envisioned as a means of providing flexibility to a secure container system where visibility into or out of the container was desired. Container security is provided through optical fiber embedded into the container walls; window security is provided through optical channel waveguides written into the polymeric window. Optical fiber in the container wall can be coupled directly into the window waveguides creating a continuous optical path. An infrared light pulse generated at one end of the optical fiber traverses the continuous optical path in the window and either continues back into the optical fiber or is interrogated at the terminus. A break in the light path at any point, either in the fiber or the window, interrupts the infrared signal which triggers an alarm or other device.

Channel optical waveguides are written in a polymer sheet using an ultraviolet laser fabrication technique. A focused laser beam is scanned across the polymer sheet to photoinduce regions of higher index of refraction. These continuous, high-refractive index regions effectively support a propagating radiation mode. An array of waveguide channels can be written at various spacing densities as small as a few microns, depending on the degree of security required. Because the channel waveguides can be written very precisely by the laser, the waveguides can be written into curved and uniquely-shaped windows. Interrupting the transmission of any one of the waveguides, such as when the window is broken, cut, or scored, is similar to breaking an optical fiber and would be sufficient to trigger an alarm or some other mechanical or electronic response mechanism.

Channel waveguides are virtually invisible and, if non-visible light is used, they are unobtrusive and difficult to locate. The waveguide pattern and line density can be tailored to the application. For example, to secure 2-cm diameter spheres would require a grid line density slightly smaller than 2 cm. Secure windows also permit tagged (e.g., bar coded) inventory in a secure room to be interrogated with a laser tag reader without having to enter the room. In a "retrofit" manner, waveguides written on an adhesive-backed, flexible film can be placed over existing windows to provide (additional) security.

The waveguides written into a window can also act as sensors to heat, chemicals, vibration, etc., depending on the window polymer, the waveguide pattern, and the associated electronics. For example, a waveguide channel can be branched at the edge of the window with each channel branch located on either side of the window pane. Light travelling through the channel will be split into the two channels and be detected on the opposite edge of the window. An external stimulus on one side of the window pane (for example, a hand on the window) will cause a difference in the waveguide conditions between the two sides of the window. Electronic circuitry detects differences in transmitted light intensity and/or phase between the two sides.

4.1.2 Objective

The objective was to build, demonstrate, and test a smart window that contains invisible channel waveguides that propagate a light signal. The smart window can provide: 1) tamper-indicating "see-through" capability for rooms and structures storing special nuclear material and

other high-value items and 2) sensing capability. The light signal through the polymer provides information about the "health" of the window (broken, cracked, being stressed) and environmental conditions on either side of the window.

4.2 Scientific Basis and Approach

Channel optical waveguides are created (or "written") in a polymer by selectively raising the polymer's refractive index in narrow, continuous channels within the window. A focused laser is used to write the channels, which can be as small as a few microns in cross-section. The laser's energy is used to alter the polymer's molecular bonding, typically through cross-linking. The refractive index of the cross-linked areas is raised less than 0.1%. However, the difference in refractive index is enough for the channel to act exactly like an optical fiber embedded in the polymer. Light will propagate within the high(er) refractive index region by reflecting at the lower refractive index interface. Because channel waveguides can be written very precisely by the laser, the waveguides can also be written into curved and uniquely shaped windows.

There are two methods for creating channel waveguides. The first method, which is less complicated, is to coat a glass or polymer substrate with a photoactive polymer film, followed by selective exposure by the laser. The exposed areas cross-link and the unexposed areas are removed with a solvent, leaving behind the channel waveguides. This process is very similar to that used by the electronics industry to create circuitry on printed circuit boards. With the channel waveguides exposed on the surface, they offer little resistance to wear or tampering unless covered or sandwiched between two substrates. The second method to create channel waveguides is to start with a photoactive polymer; a polymer doped with a photoinitiator or a photorefractive material. An example would be a sheet of doped Plexiglass. Exposure to a focused laser will cause cross-linking or dimerization, leading to a refractive index increase. Focusing the laser beneath the polymer sheet surface will "bury" the channel waveguides beneath the surface. Optical circuitry can also be written in this manner.

Light can be coupled into the window via optical fiber attached at the window's edge. An infrared light pulse generated at one end of the window will follow the channel. The channels will be invisible to the observer because of the use of infrared light and because the difference in refractive index is very slight. Interrupting the light transmission of any one of the waveguides, such as when the window is broken, cut, or scored, is similar to breaking an optical fiber and would be sufficient to trigger an alarm. Similarly, waveguides written into a window can also act as sensors to heat, chemicals, vibration, etc. For example, a waveguide channel can be branched at the edge of the window with each channel branch located on either side of the window pane. Light travelling through the channel will be split into the two channels and be detected on the opposite edge of the window. An external stimulus on one side of the window pane, for example a hand on the window, will cause a difference in the waveguide conditions between the two sides of the window. Electronic circuitry can detect the differences in transmitted light intensity and/or phase between the two sides, and trigger an alarm.

4.3 Experimental

Based on the literature (McFarland et al. 1991; Frank et al. 1991; Beeson et al. 1992), it became apparent that writing waveguides directly into a polymer was going to require a complete understanding of the laser system parameters and how they affect channel waveguide characteristics.

Another realization was that substrate preparation and procedures to characterize the written channels needed to be optimized. The most economical and timely way to determine this information was to write channel waveguides in polymer films coated on substrate surfaces.

A commercially available photosensitive polyimide polymer, Ultradel, was obtained from Amoco Chemical Company and spin-coated on the substrate using an Integrated Technologies, Inc., model P-6000 spin coater. The substrate was first cleaned with acetone and then vacuum chucked to the spin coater and spun at 3000 rpm. 5 mL of the Ultradel 9120D was applied and the substrate was spun at 500 rpm for 30 seconds, then at 2500 rpm for 60 seconds. The substrate was removed and baked for 5 minutes at 100°C. This process resulted in a uniform polyimide film thickness of 4.5 μm.

The film-coated substrate was placed on a stage computer controlled in both horizontal directions ("X" and "Y" directions) and exposed to ultraviolet light from a computer-controlled focused laser. Any "circuitry" geometry desired was written into the software program that controlled the laser. Other than basic linear channels needed for tamper-indication, channels were designed to converge and diverge, corner, and bend. The ability to control the channel geometry provided the basis for creating various sensors. Table 4.1 gives the laser parameter settings.

The complete process for creating a tamper-indicating window is depicted in Figure 4.1. Photosensitive polymer was spin-coated on different substrates (glass, silicon) and exposed to a focused laser beam. The unexposed polymer film was washed away to leave behind the channel waveguides. At this point in the process, since the waveguides were exposed, they were more easily characterized, allowing the laser parameters to be more clearly defined. To complete the window, a polyimide cladding material was spin-coated over the waveguides and a cover window was placed over the cladding to create a "sandwiched" structure. Light was launched into polished or cleaved waveguides faces at the window edges.

4.4 Results and Discussion

Once the writing parameters and workable ranges were identified, channel waveguides were written routinely on both glass and silicon substrates. Silicon substrates were used because they are well characterized and provided a reliable, flat surface to test coating and waveguide writing methods. Optical losses as low as 0.3 dB/cm at 1300 nm are possible using the Ultradel polyimide. Typical cross-section dimensions for a channel waveguide were 4 μm high by 10 μm wide. Figure 4.2 shows a scanning optical microscope photograph of a 2X2 coupler channel waveguide.

At the time of this project, a precise method for coupling light from an optical fiber into a waveguide was being developed. The channel waveguide end faces had to be the right geometry and of high optical quality in order to minimize optical coupling losses. Additionally, a means of connecting the optical fiber to the substrate was required. A diamond wafer saw was used to cut off the ends of the substrate, resulting in workable channel waveguide termini.

Table 4.1. Laser Parameters for Writing Channel Waveguides in Spin-Coated Photosensitive Film

Exposure Scan Rate: 1-5 mm/sec
Laser Exposure Energy Density: 300-900 mJ/cm^2
Laser Spot Size: typically 5-10 microns
Laser Wavelength: Ultra-violet multiline (333.6-363.3 nm)
Laser Type: Coherent Innova 90 argon-ion laser

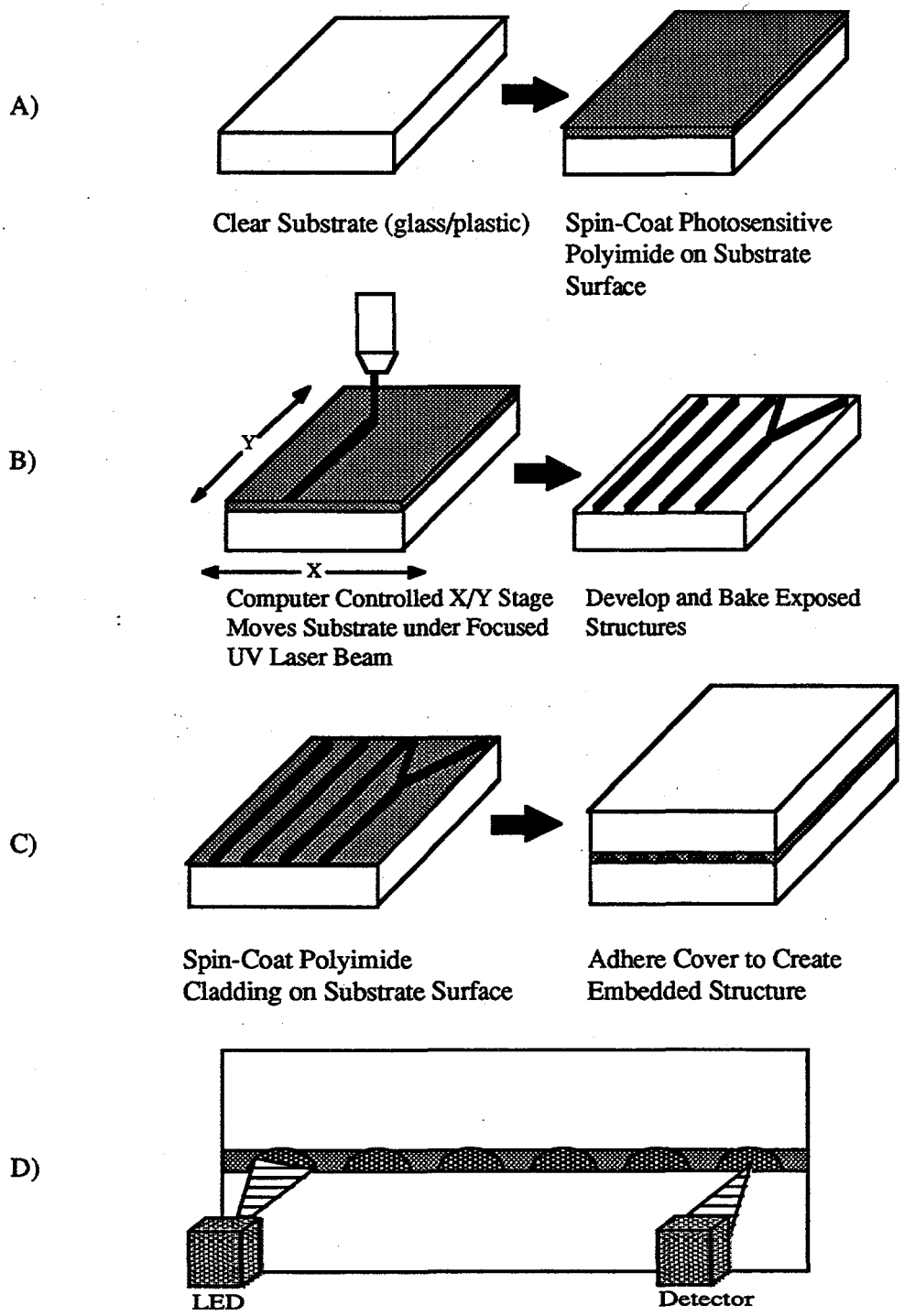

Figure 4.1. Process for Creating Tamper-Indicating Windows Depicting A) Coating on Clear Substrate, B) Forming Waveguide Circuitry, C) Creating the Embedded Circuit, and D) Coupling Light in and out of the Window

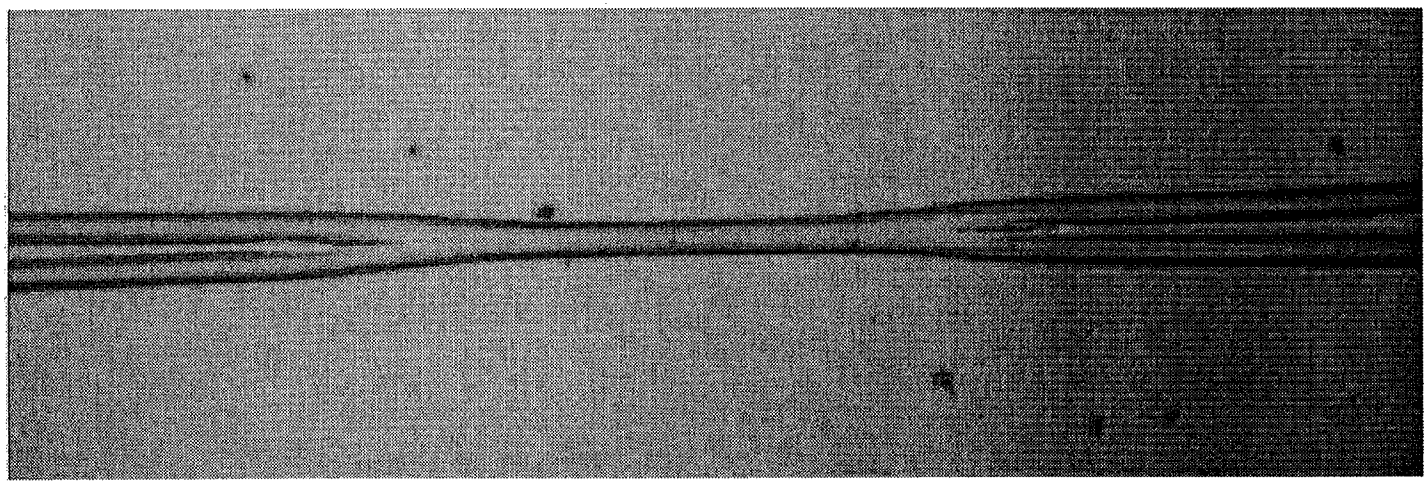

Figure 4.2. Microscopic Image of a Rib Waveguide 2x2 Coupler in Polyimide on BK7 Glass Substrate

4.5 Applications

Often it is advantageous to be able to see the contents of a container or room, for example, to periodically inventory the items or simply verify their presence, without having to open the container or open the door to the room. However, using a conventional window may not be possible because security is compromised. A smart window in the form of a "sandwich" structure with the channel waveguides located between two polymer sheets (the focus of this work), a polymer sheet such as Plexiglass, or a polymer film retrofit to an existing window provides the security via the light passing through the invisible channel waveguides inside the window. A conceptual tamper-indicating window in a door frame is depicted in Figure 4.3. Breaking, cutting, or bending the window causes a change in the light signal, which then signals an alarm. A single channel waveguide can be split at the window's edge and divided into two channels just under either window face. Pressure and temperature differences on either side of the window can be sensed and measured. The window's sensing capability adds to its security aspects by detecting the presence of, for example, a hand on the window.

Users include those responsible for both domestic and international safeguards of special nuclear material and other high-value items. When used with any radioactive materials and components, a tamper-indicating window can provide dose minimization for workers doing special nuclear material inventory by allowing visual inspection from a distance. Tamper-indicating windows can be used to make museum cases or, as a film, applied to existing windows to provide security.

With respect to sensing uses, an article about smart windows appeared in *Aviation Week and Space Technology Magazine* (Proctor 1995). Interest in smart windows has since come from Naval Air Systems Command at Wright Patterson Air Force Base, and the U.S. Coast Guard. The Air Force is interested in writing a channel waveguide around the perimeter of an aircraft canopy to detect stress cracks in the canopy's edge and near stress points like bolt holes. The Coast Guard is interested in writing channel waveguides in Plexiglass windows used in domestic "sightseeing" submarines to detect stress development and help determine window life.

4.6 Conclusions and Further Studies

We have proven through the work to date that channel waveguides are feasible and it is not difficult to envision the last few steps of coating the waveguides and creating a sandwich structure. However, the next step is to move from the substrate surface to writing waveguides in-situ in a photosensitive polymer. An entirely new set of laser writing parameters will have to be identified and defined, substrate composition and distribution of the photosensitive dopant must be fully characterized, and a new method of coupling the light from an optical fiber will need development.

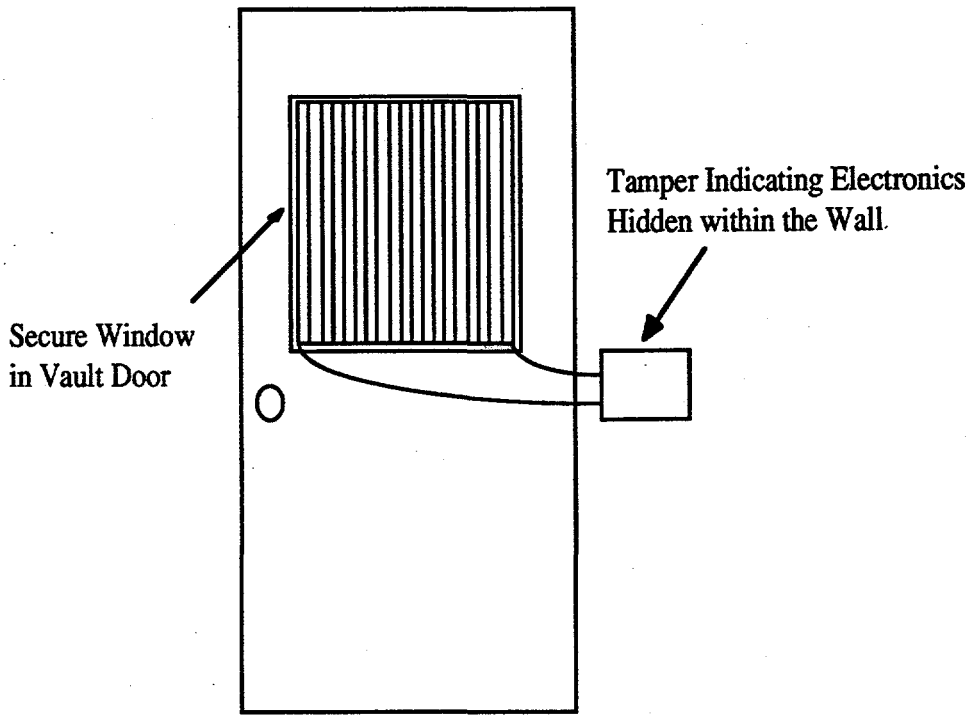

Figure 4.3. Tamper-Indicating Secure Window in a Door Application. Vertical lines show position of the channel waveguides; the actual window would be clear.

5.0 Smart Container for Transport and Storage of Neutron-Emitting Sources

5.1 Introduction

The proposed work extends the secure, tamper-indicating container concept to developing a neutron-sensing, tamper-indicating, all-polymer composite container for storing special nuclear material. To develop and verify the technological concept, an existing container presently being certified for storage and transport of neutron-emitting sources was chosen. This container is the AT-400R ("R" stands for Russian version).

Containers such as the AT-400R are designed to meet standards for transportation and storage; they provide only a modest level of tamper-resistance. The proposed smart container will provide the ability to monitor in real-time, either during transport or storage, the presence of the container contents and provide additional container tamper indication through optical fiber sensors in the lid. For demonstration purposes, the objective of the proposed work was to construct and demonstrate a smart lid for the AT-400R (however, we are not proposing a substitute lid/container for the existing AT-400 program). A conceptual view of the proposed smart container is shown in Figure 5.1.

5.2 Technical Approach

The AT-400R is comprised of two stainless steel containers, one within the other. The container of interest to the proposed work is the outer container. The outer container (herein called the container) is approximately 72.6-cm high and 50.8-cm in diameter. The lid would then be slightly less than 50.8 cm in diameter. The side of the container has an inner and outer wall with foam in between. The wall is approximately 5.1-cm thick. The lid rests on the 5.1-cm wide lip created by the inner and outer walls. The lid is held in place by 12 bolts that fit through holes in the lid and screw into threads tapped uniformly around the lip.

Sensors in the lid would perform two functions. Neutron-sensing optical fiber (developed at PNNL by Bliss et al. 1995a,b) embedded in the lid would monitor the presence of the nuclear device. The lid would also employ Bragg sensors (gratings) in an embedded optical fiber traversing the lid near each of the 12 bolt holes to create a unique (up to) 12-point stress signature once the bolts are tightened. To meet both inspection requirements and As Low As Reasonably Achievable (ALARA) concerns, the container would be radio frequency tagged so that remote interrogation is possible. Container status could be monitored continuously or periodically, depending on protocols.

The neutron sensor would be comprised of scintillating fiber coupled with commercial fiber wound into the lid. Additional neutron sensing fiber could be embedded in the container wall to increase sensitivity to the source. Approximately 1 m of scintillating fiber would be wound into the lid in a circular pattern. This active fiber, along with chopped structural fibers, would be embedded in polymer by resin transfer molding. The light pulse created in the scintillating fiber by interaction with the neutrons would be detected by solid state photomultiplier detectors embedded in the container wall. A selective threshold would be created by the electronics. If the light received by the detectors was outside the threshold because the lid was removed, the source was removed (through a hole cut in the container wall), or a person moderated the neutron flux by standing near the

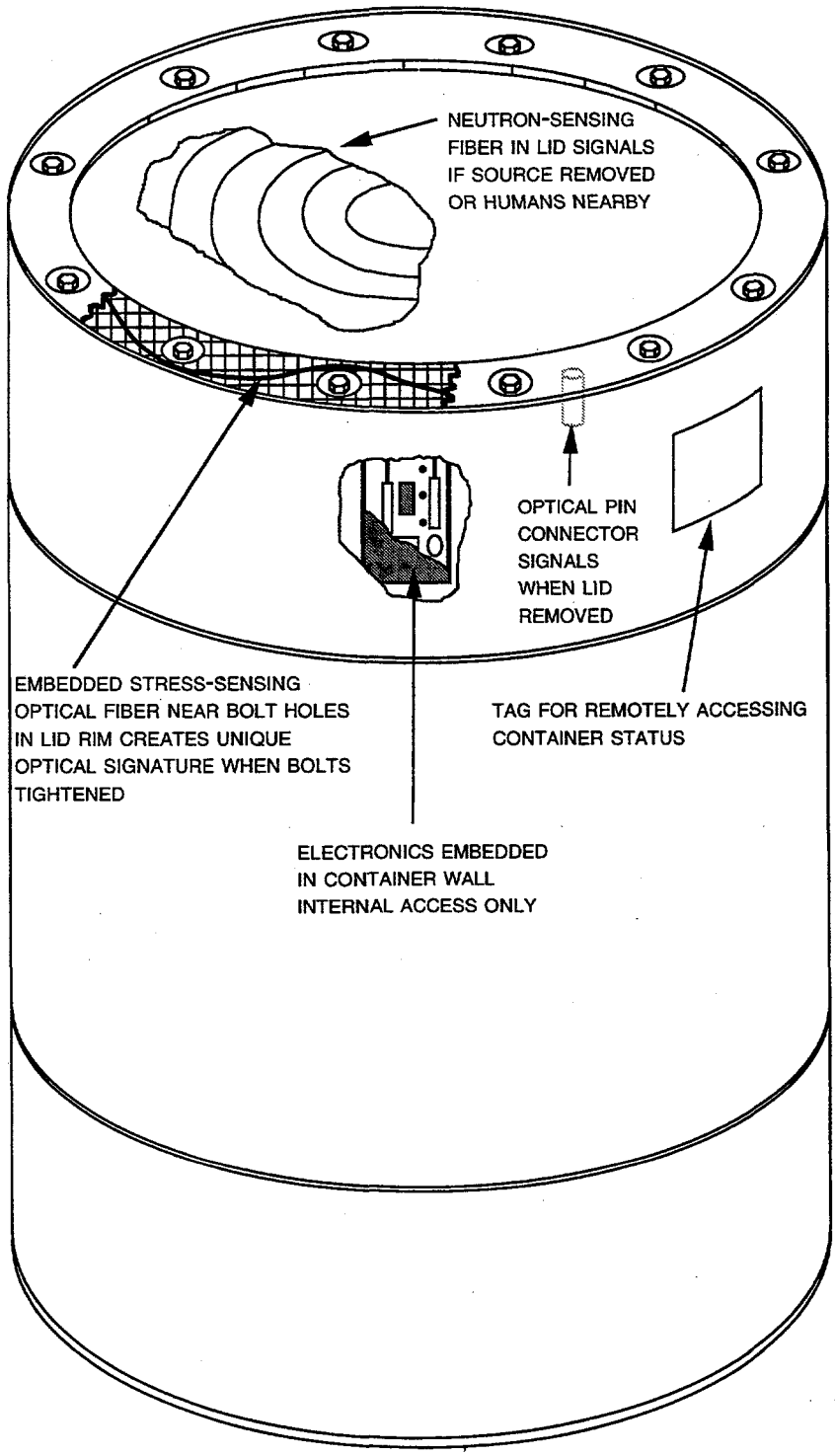

Figure 5.1. Smart Container for Storing and Shipping Neutron-Emitting Materials. This figure shows embedded sensors, electronics, and real-time RF communication.

container, an alarm would be triggered. The exact response to the alarm would be dictated by safeguard requirements.

The tamper-indicating sensor that traverses the outer rim of the lid would use the 12 bolts to create a unique fingerprint. The optical fiber would incorporate near each hole in the lid Bragg gratings that could detect microbending in the fiber. As each bolt is tightened, stresses would build up in the surrounding polymer and be transferred to the embedded optical fiber. Microbends in the fiber would cause wavelength shifts when the fiber is remotely interrogated with a light source. The resultant unique fingerprint recorded at each of the 12 bolt holes could be recorded for each container and checked periodically.

5.3 Experimental

Due to the cancellation of the overall program at the client level, the project was terminated at about the start of the experimental stage. A few prototype lids without the neutron-sensing fiber were prepared to check the molds and radiation-hardened electronics were located. For completeness, the prepared experimental matrix is described as follows.

To develop and test the neutron-sensing portion of the lid, the goal was to prepare a polymer composite lid containing the scintillating fiber, with several meters of either fiber end left outside the molded lid. A series of experiments using the original stainless steel container was devised to test the fiber sensitivity in the container configuration. A sealed neutron source would be placed in the inner container and that container placed into the outer container. The polymer lid with the embedded scintillating fiber would replace the regular stainless steel lid. The fiber termini would be connected to two solid-state photomultiplier tubes and the photon signal from the fiber monitored as a function of time to determine signal stability. The follow-on experiment would incorporate the remaining electronics to determine and test a threshold setting for the photon signal based on statistical neutron counts. After setting a threshold value, the resultant signal change would be monitored as the lid was slowly raised to increase the distance from the neutron source or a moderator brought within close proximity of the container.

The primary concern in using a polymer for the container was that polymers tend to creep over time. In order for the Bragg sensors in the lid to work, stresses introduced into the polymer by initially tightening the bolts must remain constant until the bolts were loosened (authorized or otherwise). Otherwise the microbends in the embedded fiber would relax to their initial state and the Bragg gratings would shift to their original positions, causing wavelength shifts in the light signal. The result would be a false positive signal that the bolts had been loosened.

Polymers could be made less compliant by adding chopped fibers, powders of certain inorganic compounds, and inorganic microspheres. A series of polymer samples were to be prepared using several candidate stiffener additives, followed by American Society for Testing and Materials (ASTM) creep testing. Final testing would involve embedding a Bragg sensor into a polymer sample, placing the sample in a known stress field, and monitoring the response of the sensor as a function of time and different atmospheric conditions.

5.4 Applications

The neutron sensing container received interest from the U.S. Department of Energy, Richland Operations Office (DOE-RL). Spent fuel from the Hanford K-Basins will eventually be placed in canisters for long-term storage on-site. In the storage facility, each canister will be lowered into a ground-level concrete cylindrical hole. It is envisioned that the cover over each concrete hole holding a canister could be a "smart lid" designed to verify presence of the spent fuel and provide tamper indication in real-time. An RF tag on each lid would be interrogated by a reader that is hard wired to a manned command post for continuous monitoring.

Because the container is self-contained and self-powered, it is ideal for shipping situations. Again, an RF tag on the container's exterior can be interrogated for the container's status by a local reader (e.g., in the truck or each rail car). This information can then be telemetered to a command center.

An interesting feature of this smart container that was not considered in the original sensing package is its ability to identify human presence. This was first noted by Bliss and coworkers (Bliss 1996) while developing a plutonium storage monitor. It is probable that a person standing next to a container would provide enough moderation or absorption for the scintillating fiber photon count to exceed threshold value and cause an alarm. This feature adds an extra level of security to the total system.

6.0 Smart Shipping Containers/Modular Buildings

6.1 Introduction

The same sensors, electronic components, and embedded tamper-indicating fibers applied to smaller smart containers can be extended to the large (8 x 8 x 40-ft) shipping containers that are presently the standard for commercial and military shipping. These intermodal containers have become the standard for worldwide shipping of both military and civilian cargo. For the military, tracking the shipment and placement of their vast inventory of material is formidable, which during conflict also becomes critical. In addition to knowing the cargo's location at all times, protecting that cargo is equally important. Cargo losses from accidents, mishandling, mislocating, and theft while the loaded container is being stored prior to shipment, during shipment, and once deployed are considerable. The civilian market is worse, primarily from theft of resalable, high-value goods.

The authors wrote/co-wrote several proposals to the military to develop a smart intermodal International Standards Organization (ISO) shipping container. One of those proposals, to the DoD Physical Security Equipment Working Group, was selected for funding in FY97. At the time of this report, the authors are waiting for disposition of that proposal and a similar proposal written to the Army Research Office to develop a smart, passively cooled shipping container. The following conceptual description of smart shipping containers is excerpted mostly from those two proposals.

6.2 Smart Intermodal Shipping Container

6.2.1 Introduction

There is a need to advance the state-of-the-art in shipping containers for military applications. Inadequacies of intermodal shipping containers were demonstrated during the Gulf War where the movement of strategic material was delayed because shipping containers had to be manually searched and sorted. The movement and handling of shipping containers between modes also created delays and the potential for mishandling. ISO containers must be compatible with all forms of loading, handling, and transportation methods, both private and military, and must also be functional in deployment conditions. Knowing the exact geophysical location of the container, its shipping status, contents inventory, and the health of the container and its contents is critical to military logistic coordination. Ready Reaction Forces must be able to deploy in hours. Placing their critical supplies in prepositioned smart containers would reduce their reaction time and give them greater flexibility to operate beyond supply lines. Once prepositioned in the field, there is no method available for field personnel to determine if the container's internal temperature did not experience an excursion and taint the contents, for example frozen blood plasma; if the container's contents underwent a severe shock during positioning, causing internal damage to sensitive electronic components; or if tampering occurred. A smart container would have immediate impact on timely and secure delivery of perishables, medical supplies, electronic equipment, and other high-value material in the field.

Current commercial shipping containers also lack "intelligence" that allow them to be automatically sorted and stacked by an automated crane system. The smart shipping container would have immediate impact on the timely delivery of perishable goods to remote destinations or disaster

areas without power. Additionally, the smart shipping container's ability to provide tamper indication and report sensor response in real-time has the potential to significantly reduce the high losses currently experienced in commercial shipping.

The Next Generation Smart Container is based on an intelligent sensor platform capable of continuous operation up to 6 months at a time on a single battery charge. The container would contain a fiber optic network for tamper-indication and container health monitoring such as damage to corners and edges. It would be self-contained and self-powered, would include an embedded microcomputer that accommodates remote interrogation of container states such as health and contents, would include a global positioning system (GPS) and an RF tagging system. The container would be hardened for shipping and field environments, lightweight, waterproof, sling capable, and configured for handling by standard forklifts. It would be able to be remotely prepositioned. The container would meet all ISO and intermodal transportation requirements. The container would be compatible with a fully automated cargo handling system, and would be able to interface directly with such a system to transmit information such as cargo inventory and destination.

6.2.2 Objective

PNNL proposed to develop the next generation tamper-indicating, smart shipping container that sensed: light, internal moisture (humidity), motion, and temperature (internal and external). The container would be robust for shipping and field environments, lightweight, waterproof, sling capable, and configured for handling by standard forklifts. The container would provide physical security for the contents and detect, in real-time, container breaches, either unauthorized or by mishandling, and general container health (e.g., physical integrity of walls, corners, and doors). The container would include a control system that is self-contained, self-powered, and provides global positioning capability. All of the sensor and global positioning information, container health, and inventory movement would be automatically uploaded to an RF tagging system that could be externally interrogated while in transit (e.g., automated crane systems) and in the field (e.g., field personnel with hand-held readers).

6.2.3 Demonstrated Technology

The innovative technology in the container is not related per se to the development of individual electronic components, sensors, materials, and cooling system, but in the challenge of combining existing systems and materials uniquely, resulting in an innovative, robust, lightweight, state-of-the-art, intermodal shipping container. The sensor platform, including the intelligence package, would provide the basis for other future smart containers and structures, both for military and civilian applications. These might include self-mobilizing containers that could preposition robotically such as a container deployed from an airplane that would preposition itself; fully interactive containers that could communicate information (such as contents and health) for streamlining loading and unloading of vessels; and smart shipping containers that would reduce contraband smuggling by sensing certain contents or by providing a history of the container's global position. Smart container construction would utilize lightweight, insulative materials to increase loads and aid thermal management.

The proposed work would result in the following deliverables: an enhanced electronics platform with associated sensors, fiber optic physical security and "health" network, GPS system, RF tagging, and microprocessor; a 20-ft., all-composite, fieldworthy prototype demonstration shipping

container; and a final report detailing the container design, construction, testing results, demonstration results, recommendations for changes/improvements, and estimated unit production cost.

6.2.4 Approach for Concept Demonstration

The proposed work has two primary goals related to the development of an intelligent sensor platform and a smart shipping container. The first is to demonstrate a sensor package capable of controlling all smart container functions and which is fully interactive under external interrogation. The second is to design and construct a full-scale container that demonstrates ISO and intermodal handling and transportation requirements for military and commercial applications.

Portions of the proposed work involve technologies that are more mature than others. It is the intention of the investigators to use available technology whenever possible; however, developmental work would be required, the extent of which depends on the requirements and specifications. The technical work could be divided into two tasks: task 1) sensor platform design and construction and task 2) container design and construction.

6.2.4.1 Task 1: Sensor Platform Design and Construction

The purpose of this task is to develop the electronics and sensors for the smart container. An onboard, smart sensor platform would be developed to provide detection of ambient light levels, interior moisture, interior and exterior temperature, and acceleration (motion). An embedded fiber optic network located in the container shell would provide physical security and detect container breaches, either unauthorized or by mishandling, and general container health (e.g., container corners, walls, and lid). A GPS receiver would provide geographic location information. The GPS receiver would be triggered by an accelerometer monitoring container movement. A microprocessor control and data acquisition system would be designed to read and store sensor values and control the power generation system.

RF tagging technology would be used to telemeter sensor data to a remote interrogator. When activated with RF energy, the transponder would modulate the contents of its memory buffer back to the interrogator. Once the signal is received and decoded by the interrogator, it would be converted into conventional ASCII characters for computer-based applications. Technology exists to develop a dynamic tag that interfaces with the onboard microcomputer within the container. Thus, data collected from the sensor suite could be remotely accessed by a hand held reader. RF energy is attractive for field situations because it is unaffected by smoke, rain, fog, dirt, mud, sunlight, or darkness.

In task 1, both off-the-shelf and customized sensors, RF tags and reader, and associated electronics would be integrated into a monitoring and highly integrated electronics platform for the smart container. This platform would provide the features listed above. The container and sensor platform would be designed to provide enhanced intelligence, while reducing weight, size, and electrical power requirements.

6.2.4.2 Task 2: Container Design and Construction

In task 2, a full-scale, fieldworthy demonstration container would be designed and constructed for testing shell and insulation materials, sensors, and electronics systems. This container

would feature a rugged, lightweight, polymer composite exterior shell and a polymer composite interior chassis that sandwiched a low thermal conductivity insulation. Embedded within the container walls would be a fiber optic matrix used to monitor the physical security and health of the container. The container would be designed such that sensors and electronic components would be protected, but also easily maintainable and interchangeable.

The container door would be monitored with a fiber optic pin connector so that each time the door is opened, at minimum the time and date is recorded. Entry access could require inserting a code prior to opening the door. If each item in the container is tagged, a perimeter may be created at the shipping container opening to automatically record the removal of that item from the container.

6.3 Smart Modular Storage Buildings

6.3.1 Introduction

Modular storage buildings are envisioned to be as large as full-scale shipping containers, except that they would be assembled from panels or modules. Figure 6.1 depicts the concept of a smart modular storage building. These buildings could be assembled in the field or in an unsecured area where a temporary secure enclosure was needed. They have an identical sensor platform as the large shipping containers described above, except that all of the sensors, electronics, communications, and power (except of course for the optical fiber in the panels) would be located in one modular unit. Each storage building would be comprised of several basic fiber-wound panels, a door panel, and a control panel. Building size would be determined by the number of modules connected; typical module size is envisioned to be approximately 1 m x 1 m.

6.3.2 Concept

Optical fiber could be wound or woven into predominantly two-dimensional flat mats similar to the way that non-optical glass fiber is commonly used to reinforce commercial polymer products such as large exterior automobile or minivan panels. A single optical fiber could be woven or wound and then embedded in a polymer matrix via the resin transfer molding process. The two ends of the optical fiber in the wall panel would be fitted with connectors on the panel edges so that when the panels are connected together, the optical fiber becomes continuous. Different panels created for walls, ceilings, corners, and doors could be fitted together in the field to create modular rooms/storage units/containers of various sizes. One special wall panel houses the power unit and the interactive electronics. A light signal generated either continuously or intermittently travels the entire length of fiber and is interrogated at the terminus. Any attempt to breach or disconnect panels would result in breaking the optical path, triggering a response. Door panels would be fitted with connectors that require the door to be closed to complete the optical path.

The wall panels may vary in thickness, depending on the application. The panels could be comprised of optical fiber and reinforcing fibers such as Kevlar and/or several inches of highly insulative materials could be contained within inner and outer panel shells. The panels may vary in size, again depending on the application. The panels are comprised of impact-resistant, high-strength, waterproof polymer resin. The fiber is typically commercial grade unless specifications require otherwise. For example, if radiation detection was required, neutron-detecting fibers could be incorporated or a "neutron-sensing" wall panel module incorporated into the structure. Fiber winding density in a panel is typically very high, but could be wound to higher densities if needed.

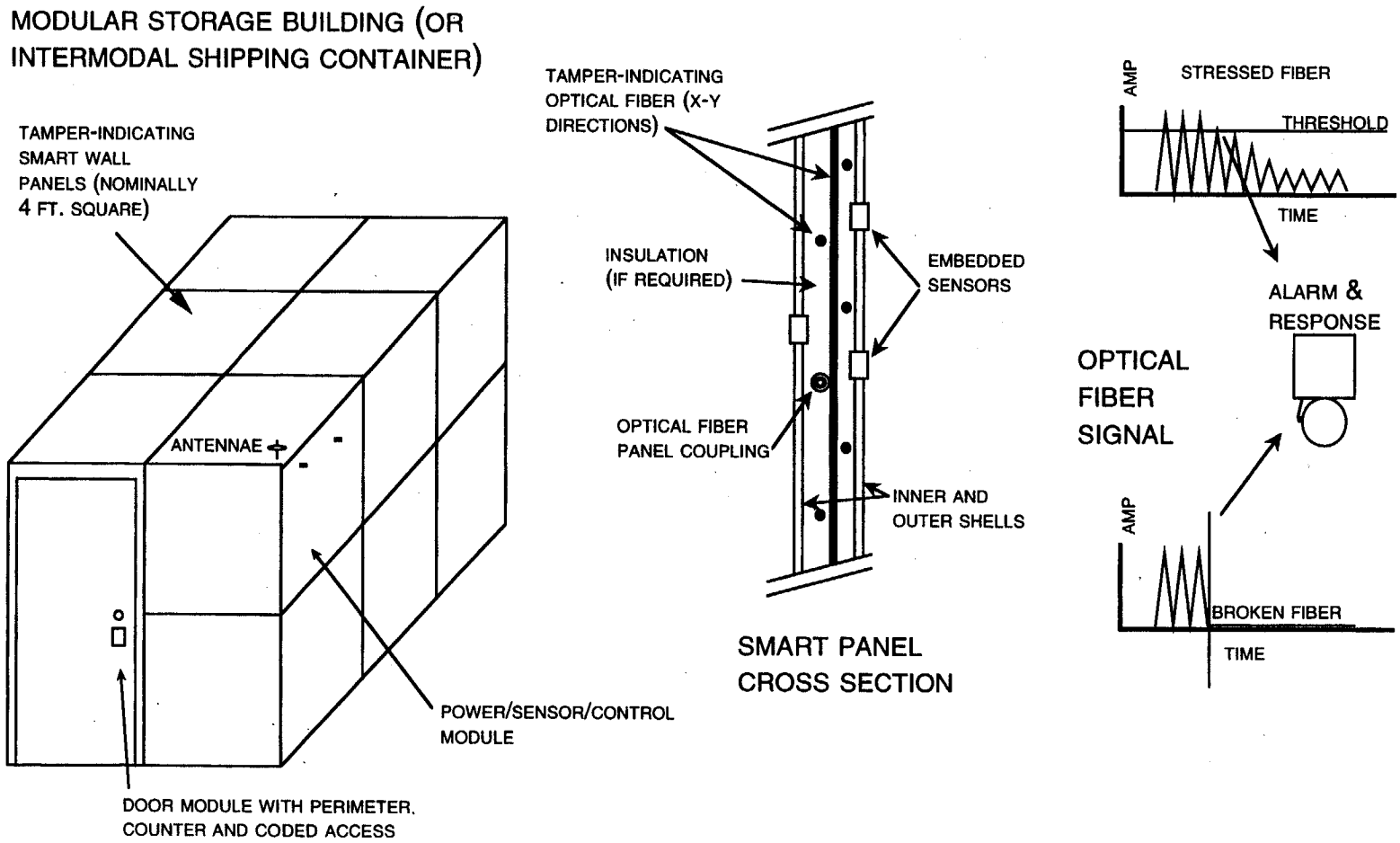

Figure 6.1. Conceptual Tamper-Indicating Smart Modular Field Container/Building or Intermodal Shipping Container

Electronics package features include tamper indication– the light signal through the fiber could be continuous or pulsed intermittently. An RF tagging/communication system permits items placed into the container/room to be inventoried and the inventory obtained from outside the container/room by interrogating an external RF tag with a remote reader. If the items in the room are individually tagged, a perimeter around the door could be created that automatically logs when an item entered or exited the room. The door itself is made secure by requiring a unique code to disarm the door alarm prior to entering. Response to tampering with, for example, a wall panel, unauthorized entry through the door, removing an item from the container/room, or any similar situation would vary, but at minimum, an alarm would sound.

Using optical fiber as the basis for tamper indication allows incorporating either fiber optic sensors or fiber optic compatible discrete sensors into the modular panels. For example, optical fiber containing Bragg sensors could be used to detect changes in stress, temperature, or vibration. Mentioned previously, fibers that detect the presence of neutrons could be integrated into the container. Coupling discrete sensors that measured, for example, moisture, light, and air composition is also possible. Many of the sensors not requiring a larger area to be effective could be incorporated into a single panel. Constructing a portable modular building involves the assembly of specific panels selected prior to deployment.

6.3.3 Applications

The key feature of this storage building is its modularity. The modules are small enough to be transported and could be assembled to almost any size building in the field. Modular storage buildings could be used for most situations where a temporary secure storage room was required. For example, there may be a need to temporarily secure a small area within a larger, unsecure area/building. Through communication between the modular building's RF tag and an interrogator located nearby, the modular storage building could be monitored continuously in real-time.

7.0 Conclusions and Lessons Learned

The prototype container, the secure video container, and smart windows were the three projects that provided experimental data and actual hands-on construction. In the first two container projects, we learned how to wind the optical fiber to reduce twisting and bending losses and how the fiber responded to embedding in polymer. For the prototype container, the fiber was sensitive to polymer shrinkage because the fiber buffer was very thin and noncompliant. The fiber showed minimal signal loss after the fiber was coated with silicone, a very compliant polymer. The fiber wound into the video container had a much thicker buffer and silicone rubber was used to embed the fiber; this fiber showed negligible signal attenuation. Both of these systems successfully used light from a laser diode to detect fiber breaches and/or lid removal. Electronics were kept simple and smart structure response was demonstrated with a simple piezoelectric buzzer alarm.

The smart windows project added another component to the tamper-indicating smart container concept. The goal was to first write waveguides on the surface of a substrate and then write them below the substrate surface in-situ. Writing channel waveguides into a photosensitive polymer on a substrate surface was successful using a computer-guided focussed UV laser. Channel waveguide structures of varying complexity were able to be replicated. Light was able to be coupled into the waveguides manually and at project end we were in the process of developing a permanent coupling method. The final step was to coat the channel waveguides with a second polymer and cover them to create a sandwich structure. It became apparent during the investigation that windows with channel waveguides could act as sensors in one of two manners. Being able to write almost any waveguide circuit into the photosensitive polymer was a direct lead to constructing discrete sensors directly on the window. Secondly, a smart window with embedded tamper-indicating channel waveguides would be able to sense environmental changes by comparing the light intensity and/or phase from different channel waveguides.

The final two projects, the container for storing and shipping special nuclear material and the intermodal shipping container/modular building, demonstrated the level of complexity possible with optical fiber-based smart structures. The special nuclear material storage/shipping container had two fiber optic-based sensors tied into the tamper-indication system, one for neutron detection and the other for stress detection. The intermodal container extended the tamper-indication function to health monitoring. Not only would the container detect breaches or open doors, the same system could also report damage to the container, which is critical for field deployments. Both of these containers utilized radio frequency communication to report the container's status, which initiated the possibility of real-time monitoring, even in remote situations.

Smart structure complexity increased with each new container even though the basis for tamper-indication remained essentially unchanged. Optical fiber as the smart material allowed for the addition of other discrete sensors, fiber optic-based (e.g., secure windows, radiation, stress) or otherwise (e.g., moisture, temperature, motion). All of the containers were designed and constructed so that the optical fiber-based smart structure was an integral part of the container. At the time of this report, compared with all other methods of providing tamper-indication for secure containers, the smart containers designed, developed, and constructed in these projects are the only tamper-indicating containers in which the *container itself* provides the tamper indication.

8.0 References

Ahmad, I., A. Crowson, C.A. Roger, and M. Aizawa. 1990. *US-Japan Workshop on Smart/Intelligent Materials and Systems.* In Proceedings of the March 19-20, 1990, conference, Honalulu, Hawaii, ed. Technomic Publishing, Lancaster, PA.

Beeson, K.W., M.J. McFarland, W.A. Pender, J. Shan, C. Wu, and J.T. Yardley. 1992. "Laser-written polymeric optical waveguides for integrated optical device applications." *Integrated Optical Circuits II*, SPIE Vol. 1794, pp. 397-404, SPIE, Bellingham, WA.

Bliss, M., R.L. Brodzinski, R.A. Craig, B.D. Geelhood, M.A. Knopf, H.S. Miley, R.W. Perkins, P.L. Reeder, D.S. Sunberg, R.A. Warner, and N.A. Wogman. 1995a. "Glass-fiber-based neutron detectors for high- and low-flux environments." In Proceedings *Photoelectronic Detectors, Cameras, and Systems*, San Diego, CA, eds. C.B. Johnson, Ervin, J. Fenyves, SPIE 2551, pp. 108-117, SPIE, Bellingham, WA.

Bliss, M. and R.A. Craig. 1995b. "A Variety Of Neutron Sensors Based On Scintillating Glass Waveguides." In Proceedings *Pacific Northwest Fiber Optic Sensor Workshop*, ed. E. Udd, SPIE Vol. 2574, pp. 152-158, SPIE, Bellingham, WA.

Bliss, M., R.A. Craig, D.S. Sunberg, and R.A. Warner. 1996. "Prototype Plutonium-Storage Monitor." *Journal of Nuclear Materials Management* 24(3):22-29.

Claus, R.O. 1991. *Proceedings of the Conference on Optical Fiber Sensor-Based Smart Materials and Structures.* Ed. Technomic Publishing, Lancaster, PA.

Frank, W.F.X., A. Schosser, S. Brunner, F. Linke, T.K. Strempel, and M. Eich. 1991. "Optical properties of waveguiding structures in polymers." *Nonconducting Photopolymers and Applications*, SPIE Vol. 1774, pp. 268-277, SPIE, Bellingham, WA.

McFarland, M.J., K.W. Beeson, K.A. Horn, A. Nahata, C. Wu, and J.T. Yardley. 1991. "Polymeric optical waveguides for device applications." *Integrated Optical Circuits*, SPIE Vol. 1583 pp. 344-353, SPIE, Bellingham, WA.

Rogers, C.A. 1988. *Smart Materials, Structures, and Mathematical Issues.* Ed. Technomic Publishing, Lancaster, PA.

Proctor, P. (compiler). 1995. "Secure Windows." *Aviation Week and Space Technology*, August 7, 1995.

Appendix A

Appendix A

Schematic Diagrams and Perspective Drawings of Molds Used for Fabricating the Optical Fiber-Based Secure Smart Structure Drawer and Outer Shell

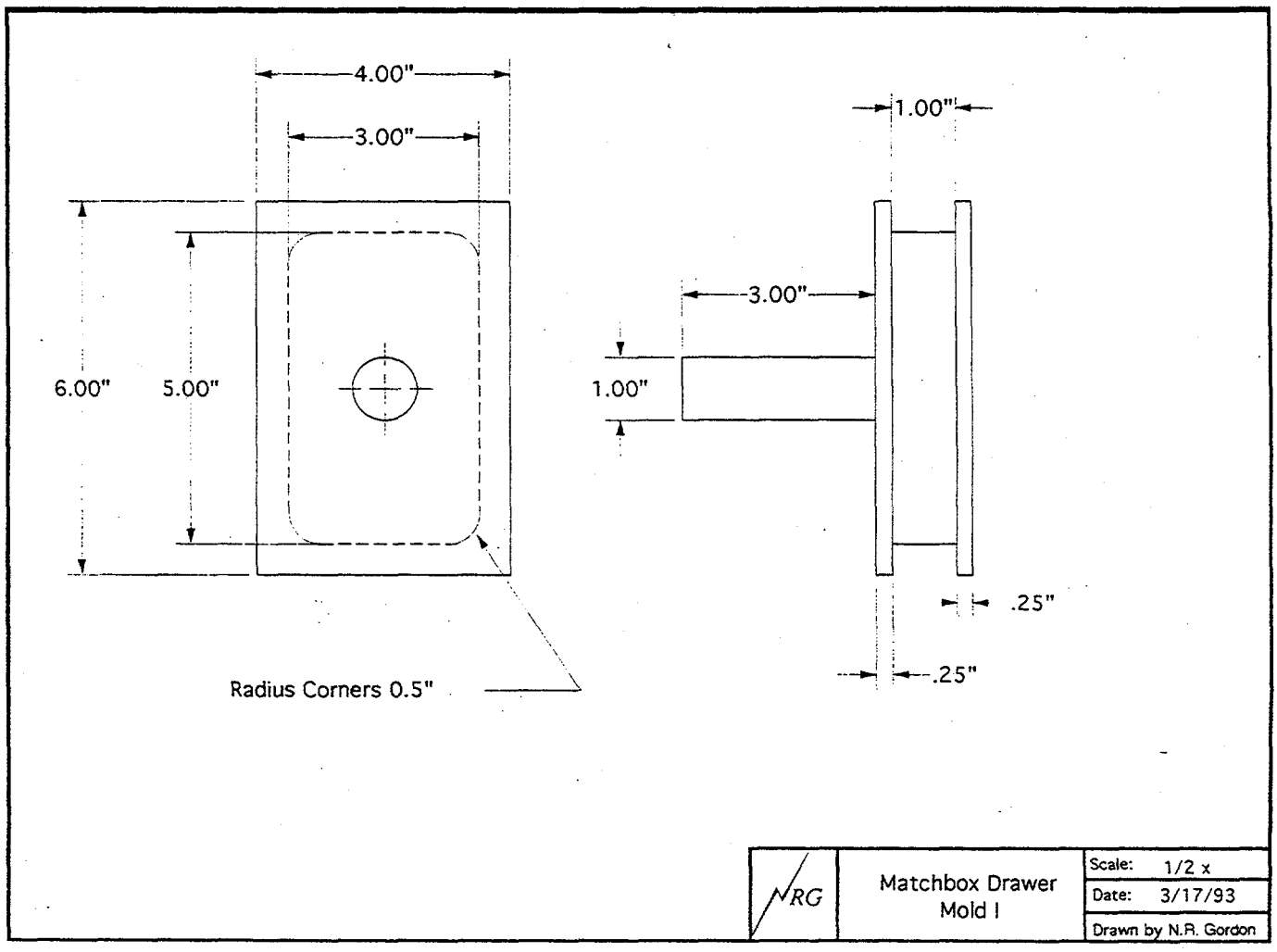

Figure A.1. Schematic of Secure Container Drawer Inside Mandrel

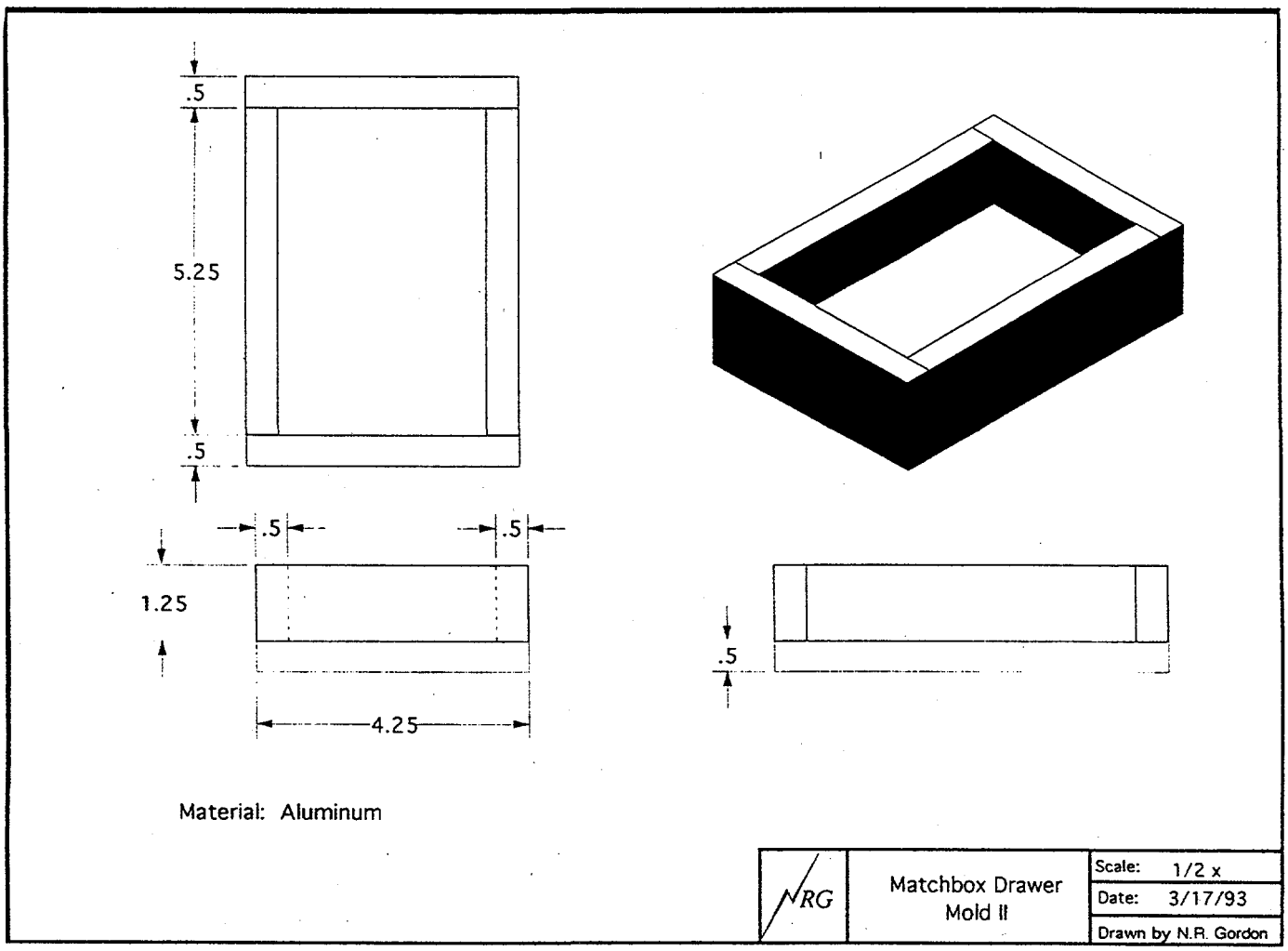

Figure A.2. Schematic and Perspective Drawings of Secure Container Drawer Outside Mold

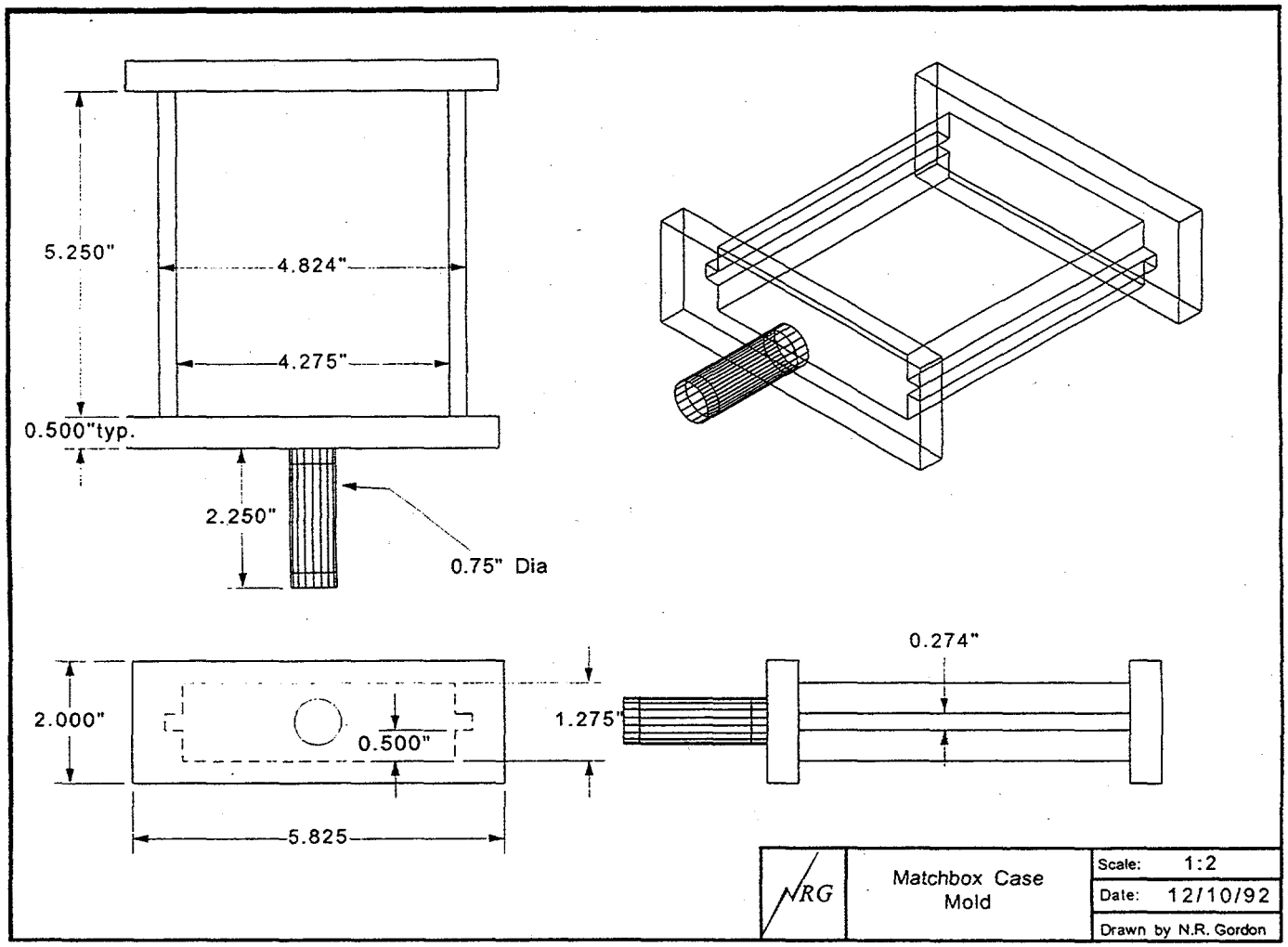

Figure A.3. Schematic of Secure Container Outer Shell Mandrel Showing Original Plans for Side Guide Channels

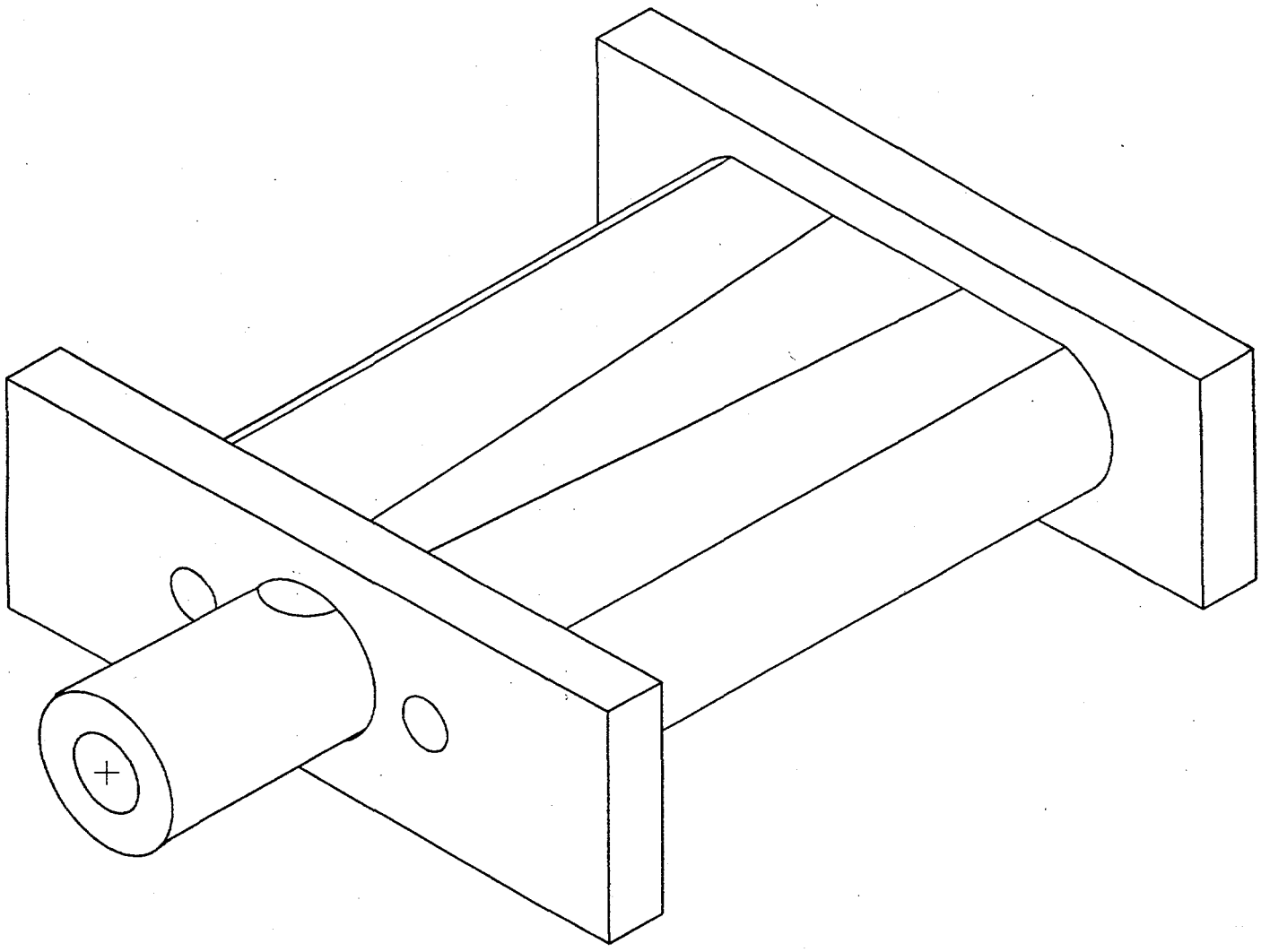

Figure A.4. Perspective Drawing of Second Generation Secure Container Outer Shell Mandrel Showing Wedge Insert

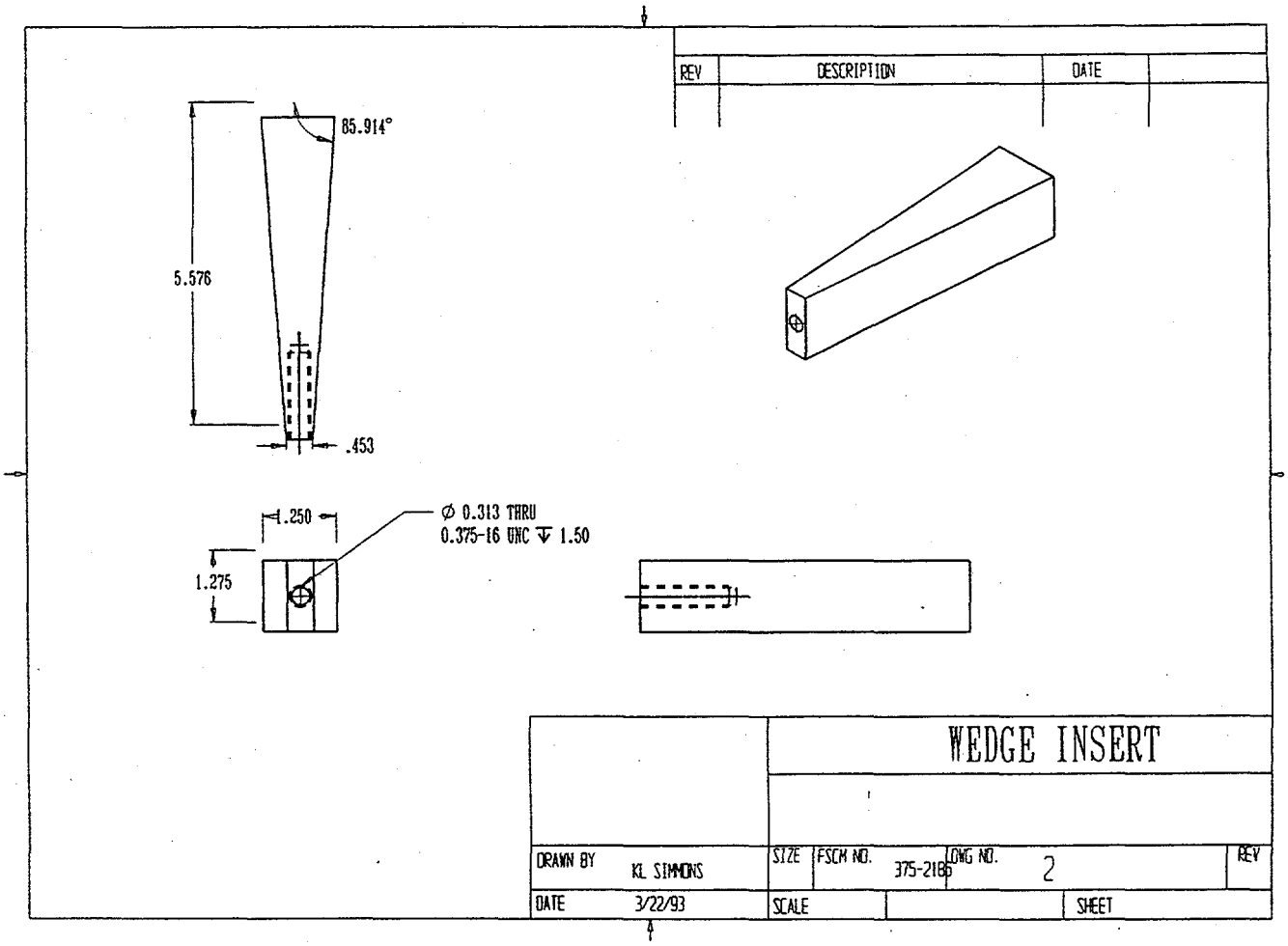

Figure A.5. Schematic Drawing of Wedge Insert for Second Generation Secure Container Outer Shell Mandrel

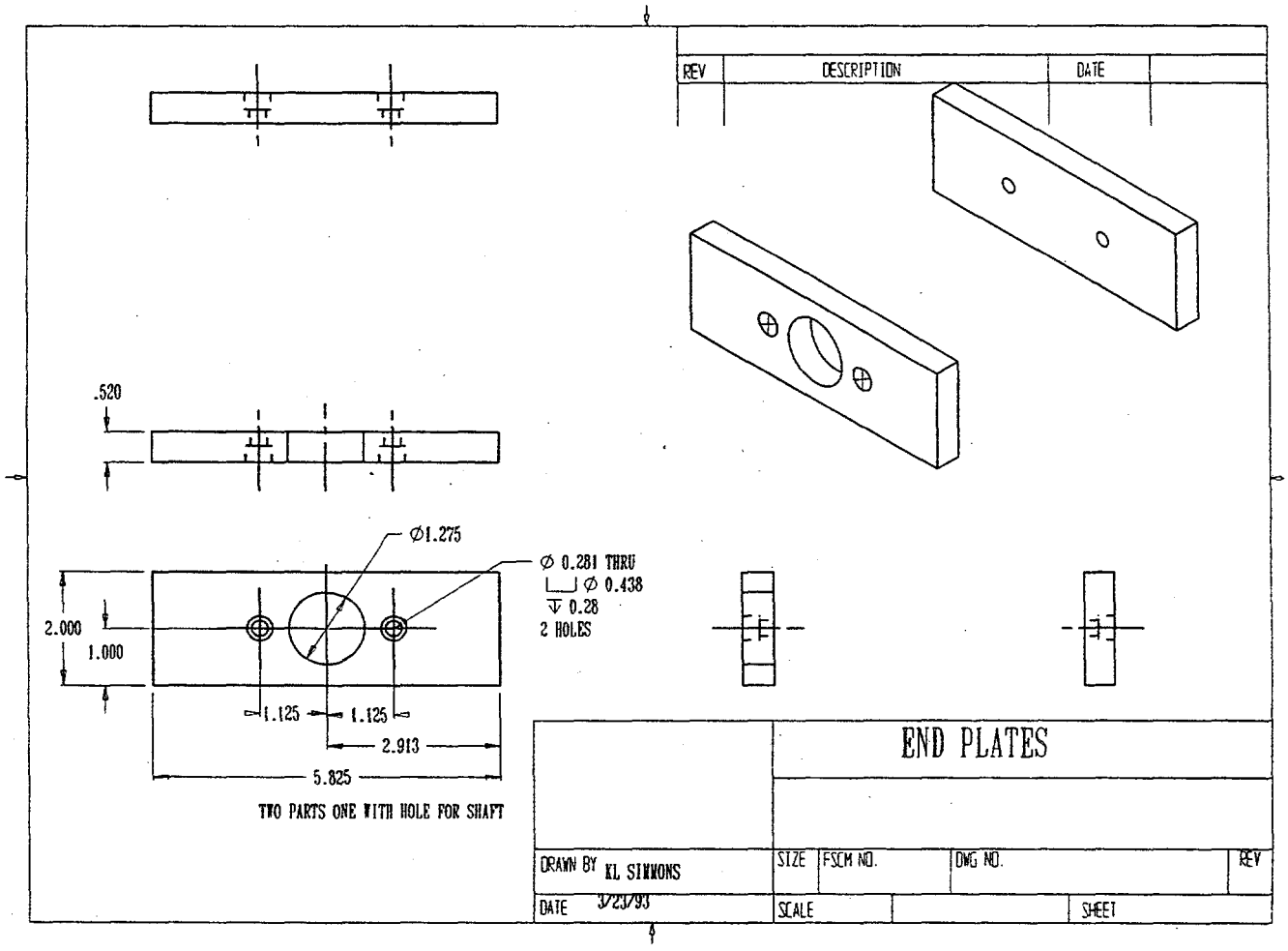

Figure A.6. Schematic Drawing of Mandrel End-Plates for Second Generation Secure Container Outer Shell Mandrel

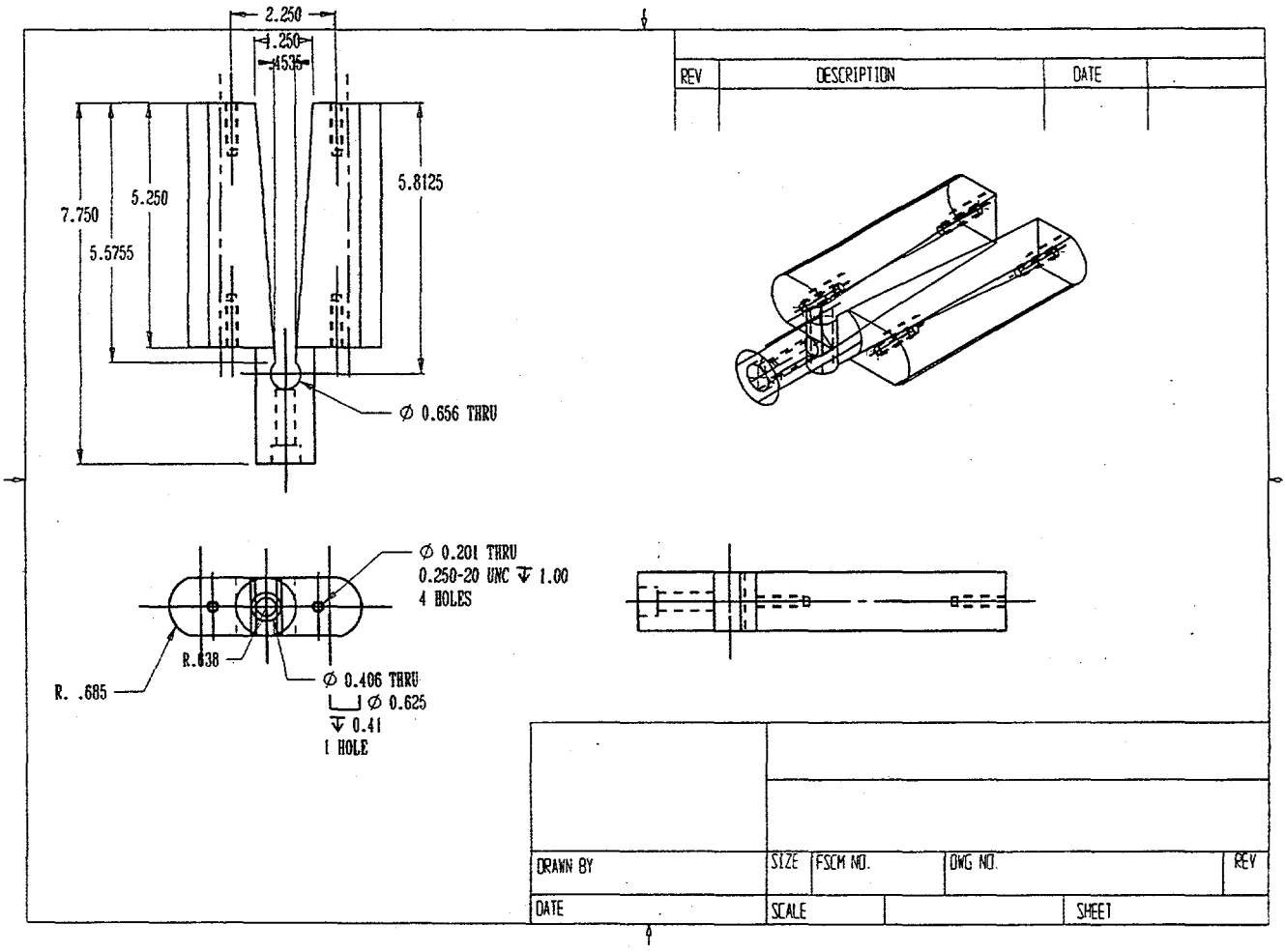

Figure A.7. Schematic of Second Generation Secure Container Outer Shell Main Body Mandrel

Appendix B

Appendix B

Block Diagram and Schematic Circuit for Optical Fiber-Based Smart Secure Container

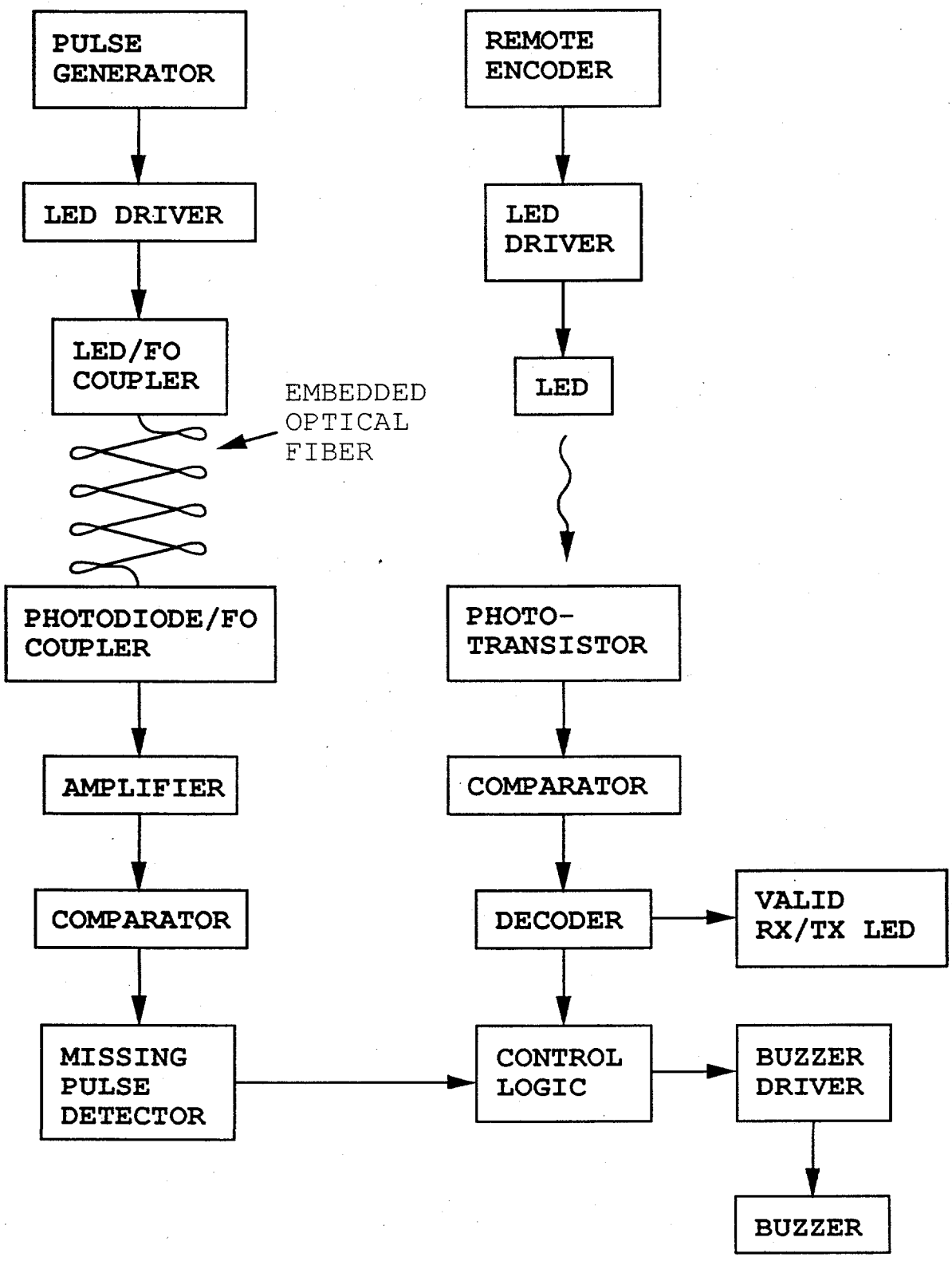

Figure B.1. Block Diagram for Optical Fiber-Based Smart Secure Container Electronic Circuitry Showing Light Pulse "Pitch-Catch" Operation and Security Logic

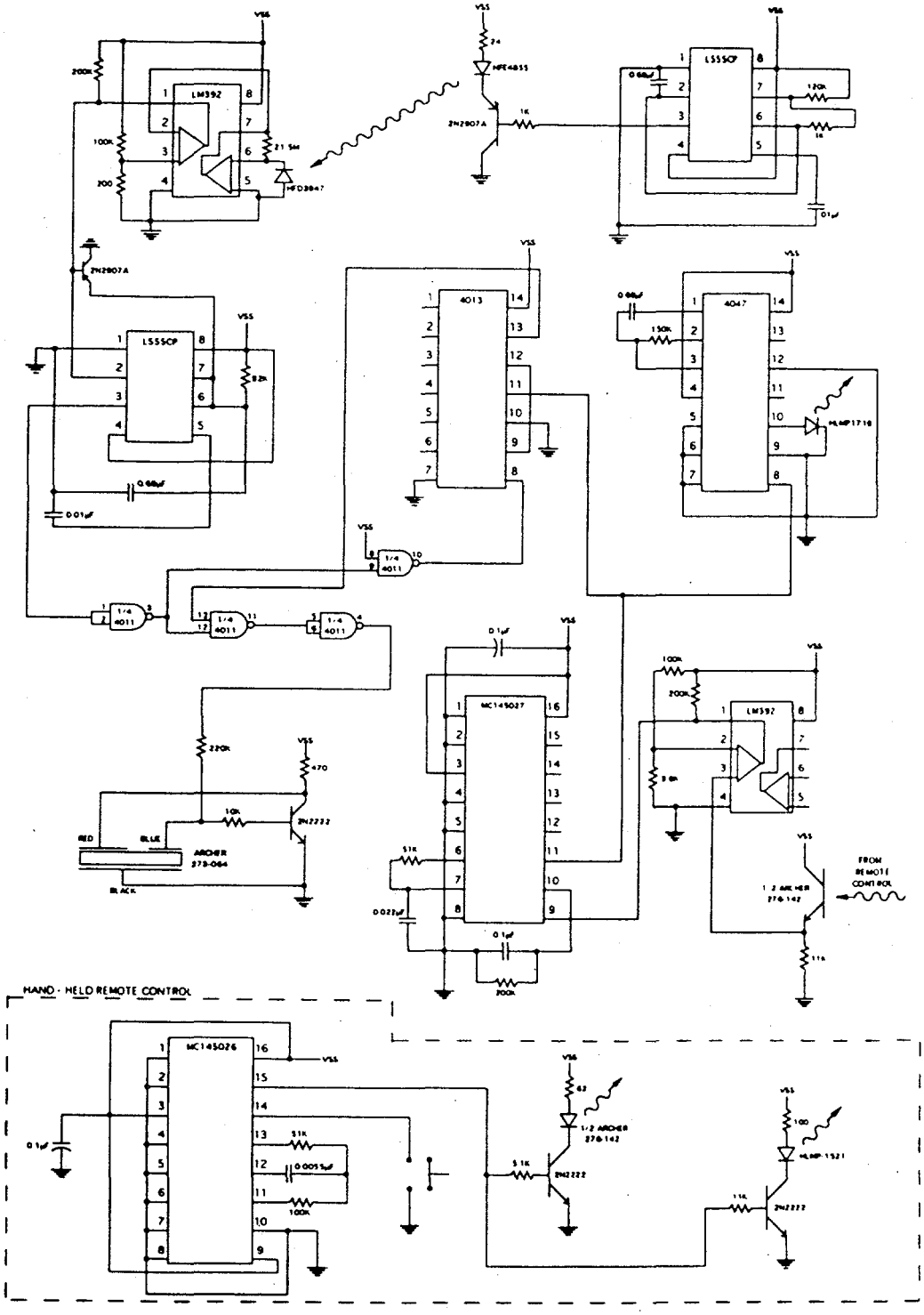

Figure B.2. Schematic of Optical Fiber-Based Smart Secure Container Electronic Circuitry

Appendix C

Appendix C

Schematics of Optical Fiber-Based Secure Video Container Electronic Circuitry

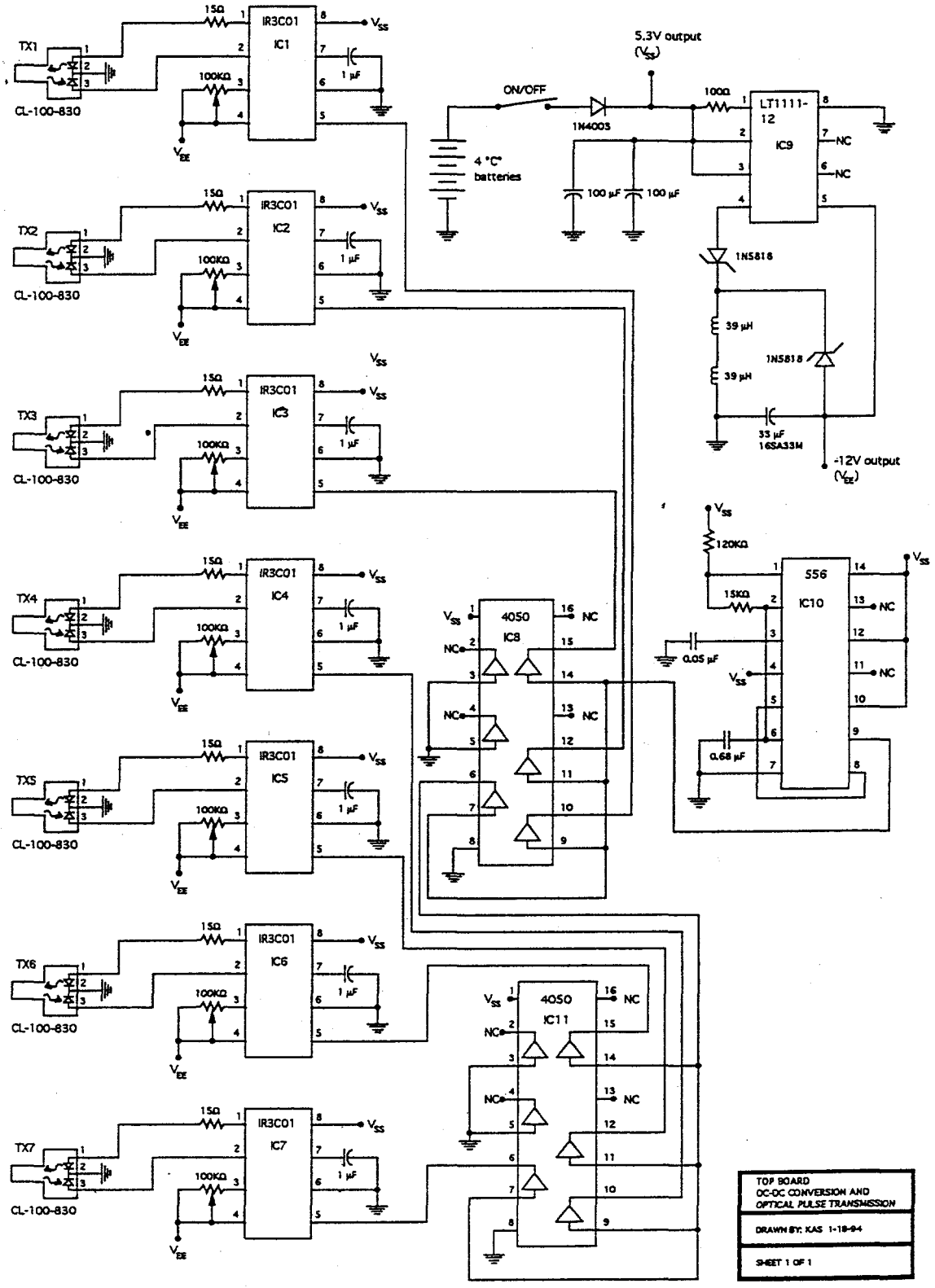

Figure C.1. Schematic of Power and Optical Pulse Transmission Circuitry for Optical Fiber-Based Tamper-Indicating Video Container

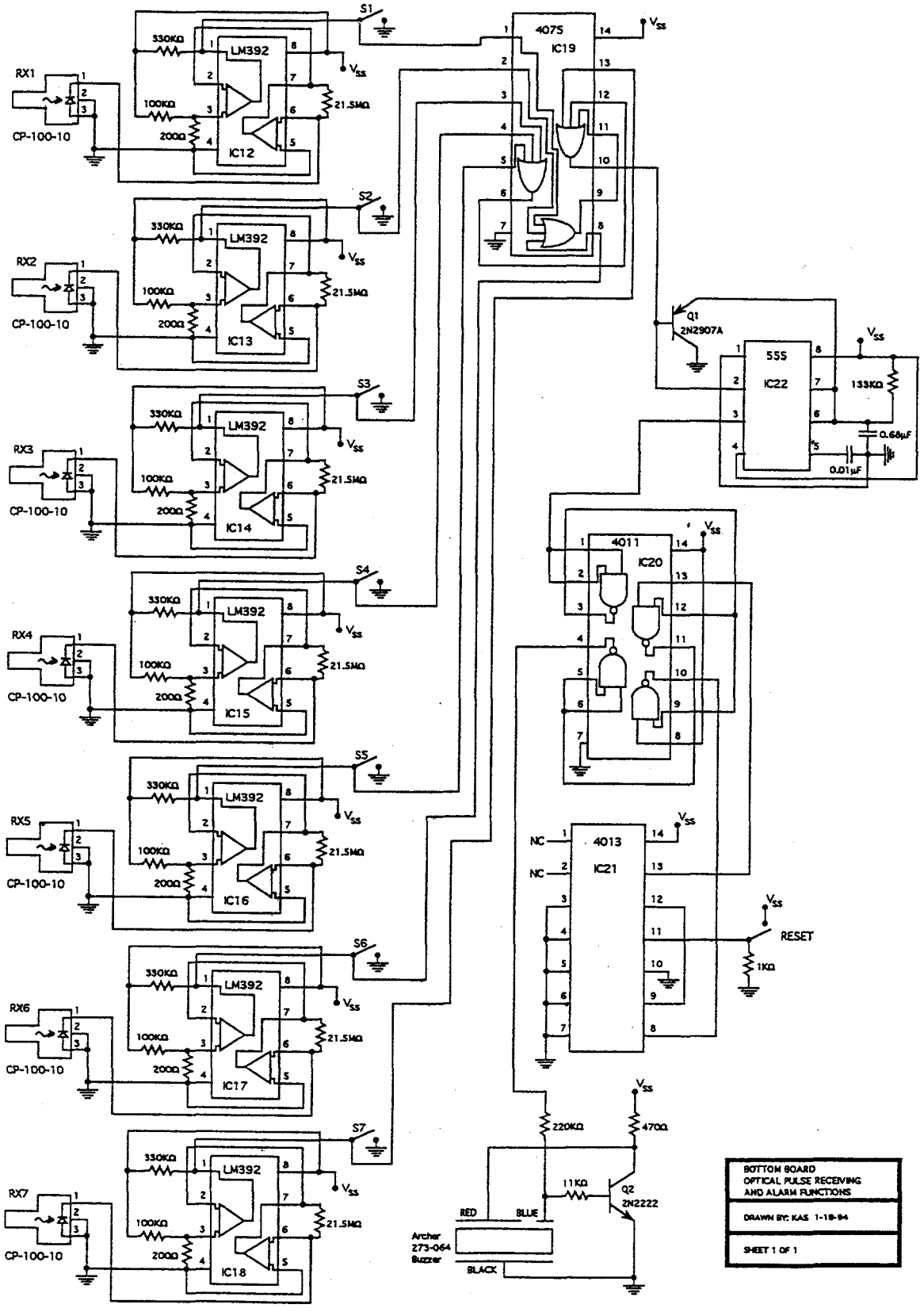

Figure C.2. Schematic of Optical Pulse Receiving and Alarm Function Circuitry for Optical Fiber-Based Tamper-Indicating Video Container

Distribution

No. of
Copies

OFFSITE

Information Release Office (7) K1-06

C. Terry Chase
Battelle Washington Office
370 L'Enfant Promenade, Suite 900
901 D Street SW
Washington, D.C. 20024-2115

S. Herrick
Chief, Advanced Systems Division
NN-20
Forrestal Building
U.S. Department of Energy
1000 Independence Ave. SW
Washington, D.C. 20585

Thomas J. Lennox
Battelle Washington Office
370 L'Enfant Promenade, Suite 900
901 D Street SW
Washington, D.C. 20024-2115

David E. Scharett
Battelle Washington Office
370 L'Enfant Promenade, Suite 900
901 D Street SW
Washington, D.C. 20024-2115

No. of
Copies

T. Witter
Defense Special Weapons Agency
6801 Telegraph Road
Alexandria, VA 22310-3398

ONSITE

DOE Richland Operations Office

R. B. Goranson K8-50

41 Pacific Northwest National Laboratory

J. R. Abraham	K8-58
N. A. Anheier	K5-25
J. L. Fuller	K6-48
S. W. Martin	K6-49
B. J. Merrill	K6-49
K. L. Simmons	K2-44
P. Sliva (30)	K6-48
H. A. Undem (5)	K6-48