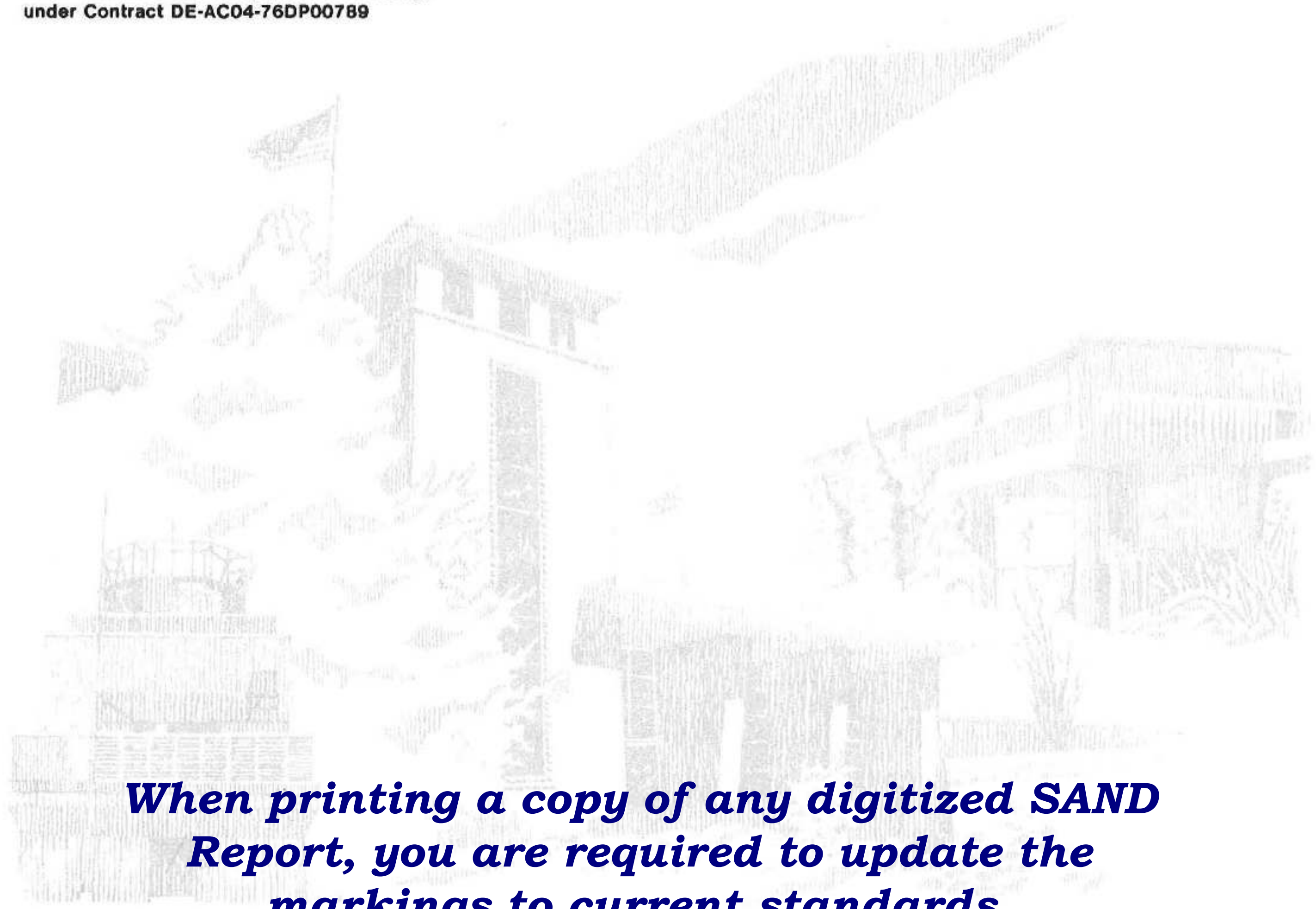
SANDIA REPORT
SAND87—0947 • UC—15
Unlimited Release
Printed July 1987

The Evolution of Interior Intrusion Detection Technology at Sandia National Laboratories

R. H. Graham, R. M. Workhoven

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-76DP00789



Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof or any of their contractors or subcontractors.

Printed in the United States of America
Available from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161

NTIS price codes
Printed copy: A02
Microfiche copy: A01

THE EVOLUTION OF INTERIOR INTRUSION DETECTION TECHNOLOGY *
AT SANDIA NATIONAL LABORATORIES

R. H. Graham and R. M. Workhoven
Sandia National Laboratories
Albuquerque, New Mexico USA 87185

ABSTRACT

Interior Intrusion Detection Technology began at Sandia National Laboratories (SNL) in 1975 as part of the Fixed Facilities Physical Protection Research and Development program sponsored by the U. S. Department of Energy in connection with their nuclear safeguards effort. This paper describes the evolution of Interior Intrusion Detection Technology at Sandia National Laboratories from the beginning of the Interior Sensor Laboratory to the present. This Laboratory was established in 1976 to evaluate commercial interior intrusion sensors and to assist in site-specific intrusion detection system designs. Examples of special test techniques and new test equipment that were developed at the Lab are presented, including the Sandia Intruder Motion Simulator (SIMS), the Sensor and Environment Monitor (SEM), and the Sandia Interior Robot (SIR). We also discuss new sensors and unique sensor combinations developed when commercial sensors were unavailable and the future application of expert systems.

INTRODUCTION

Interior Intrusion Detection Technology at Sandia National Laboratories began in 1975 as part of the Fixed Facilities Physical Protection Research and Development Program sponsored by the US Department of Energy Safeguards and Security Office in connection with their nuclear safeguards effort. The Interior Sensor Laboratory was established in 1976 to evaluate commercial interior intrusion sensors and to assist in site-specific intrusion detection system designs as part of our goal of providing high-quality interior detection systems.

Interior intrusion detection systems focus on three areas of concern: (1) the enclosure or shell of a building, (2) the volume inside the shell, and (3) the target. The shell of a building, including openings such as doors, windows, skylights, and utility ducts, may have balanced magnetic switches, shock and vibration sensors, or continuity circuits as the first level of detection. Infrared, microwave, sonic, or ultrasonic motion sensors are normally used as interior volume sensors and provide the second level of detection. The third and final level of protection includes contact/proximity sensors installed at or near the expected target. With detection devices in all three locations, in-depth protection is achieved because the intruder must circumvent or defeat three different sensor technologies in sequence before gaining access to a target.

Probability of detection, false-alarm rate, and vulnerability to defeat are three performance factors often associated with sensors. It is very difficult to assign meaningful numbers to these factors. Not only must one consider the characteristics of the sensor, but also the characteristics of the environment in which the sensor is installed, the method of installation, and the assumed behavior of the intruder. If a number is assigned to any of these factors for a sensor or sensor system, that number must be qualified by identifying all conditions under which the number is valid. SNL's Interior Sensor Lab concentrated instead on defining the detection capabilities and limitations of intrusion sensors. For example, what are the effects of intruder velocity, direction of motion, and ambient temperature on the detection pattern of different sensors?

In order to evaluate sensors properly, special test techniques and new test equipment had to be developed. New sensors with greater capabilities regularly appeared on the market and required continuous examination of the changing technology. The evaluation procedures and equipment also had to be updated to stay current. Other lab activities included investigating troublesome field installations to identify problems, developing solutions for the problems, and implementing the appropriate upgrades.

Motion sensor testing is a good example of how test techniques have progressed over the years. In early testing, to try to maintain constant velocity, a human test target held onto and moved with a string looped over pulleys driven by a variable-speed motor. Eliminating the human element can often improve test results since motion sensors react differently to individuals according to variances in size, shape, body motion, and metabolism. To overcome increased

*This work performed at Sandia National Laboratories supported by the US Department of Energy under contract number DE-AC04-76DP00789.

difficulties as velocities and temperatures approached the upper and lower extremes of their test ranges, we created a motor-driven mannequin to replace the human test target. This mannequin, affectionately dubbed Intrudee (Figure 1), improved reliability and test results because she did not tire so easily, and she never "got up on the wrong side of the bed." Next, electronic intruder simulation was developed for the active Doppler motion sensors, and geometric scaling of a heated target simulated an intruder for passive infrared motion sensors. These devices were improved and combined into the Sandia Intruder Motion Simulator (SIMS), which tested motion sensors under full computer control.

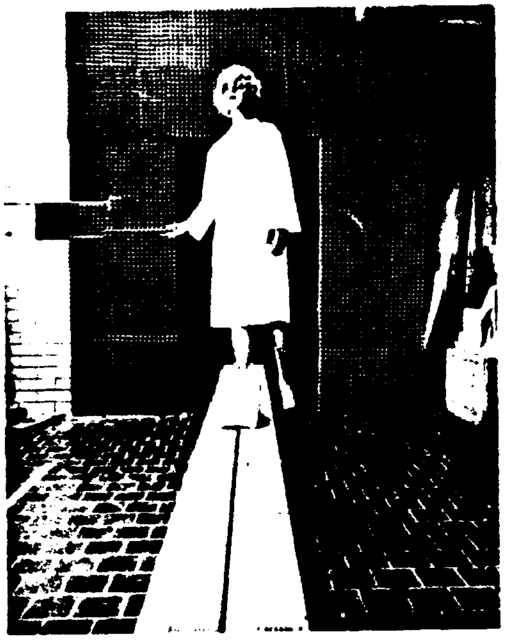


Figure 1. Intrudee

This paper discusses the SIMS and other unique equipment including the Sensor and Environment Monitor (SEM), a special-purpose data acquisition system, and the Sandia Interior Robot (SIR), which is a small, self-contained mobile sensor platform. At the Interior Sensor Laboratory, if commercial sensors were unavailable for certain tasks, then new sensors were developed, tested, and implemented in the field. Barrier sensors for the Weapons Storage Vault (WSV) are one example discussed here. For some unusual situations, sensors were combined in often unconventional ways to obtain the desired detection. We also describe a capacitance proximity blanket developed to couple with commercial sensors to provide detection in a special application.

Finally, we discuss future applications of artificial intelligence and expert systems in interior intrusion detection, including sensor selection, system design, and alarm diagnosis.

SANDIA INTRUDER MOTION SIMULATOR

The Sandia Intruder Motion Simulator (SIMS), was developed at SNL to provide systematic, repeatable testing of interior intrusion sensing devices. Consequently, better information is available from which decisions can be made with regard to the application of sensors. The SIMS can be run unattended during ambient and environmental tests and does not require excessive operator time while providing fully controlled evaluation not possible manually. Microwave, ultrasonic and sonic motion sensors have the same operating principles and can be given simulated tests of velocity, angular detection pattern, radiated power and sensitivity to oscillatory motion. Passive infrared sensors are tested to identify the sensitive zones, and to determine the detection perimeter for various velocities, radii and target-background temperature differences. Passive ultrasonic and sonic sensors, as well as vibration and glass-break sensors, may be tested by frequency sensitivity sweep, pulse length and pulse count tests. Capacitance proximity sensors are tested by several capacitance changes, and balanced magnetic switch (BMS) sensors can be tested by using either a changing magnetic field or systematic separation of the sensor components.

Although the SIMS system is capable of testing all of the sensors mentioned above, it is used primarily for motion sensor testing.

The SIMS consists of two separate computer controlled subsystems, one for testing sensors which employ the Doppler principle, and the other for testing passive infrared sensors. Two subsystems were chosen because the bulk of the sensor testing requirements were for the two types of motion sensors.

The SIMS subsystems were designed around HP 9825T computers. This machine can be programmed to provide control of the environmental conditions, as well as to test the sensors. The subsystems have built-in disk drives to store the operating parameters and the data acquired during the tests. Movement is automatic from one environmental condition to another and through the tests at each condition. This allows the test apparatus to be left unattended for significant periods of time. When new test profiles or environmental profiles are needed, it is simple to enter the desired test parameters. Figure 2 is a photograph of the SIMS' controls and environmental chamber.

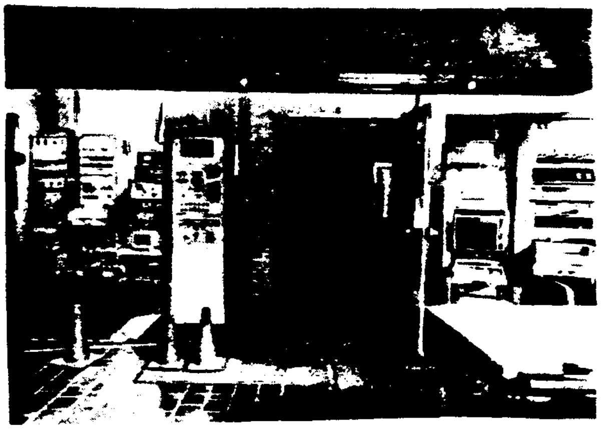


Figure 2. Sandia Intruder Motion Simulator

Environmental tests of interior sensors are important because many of the buildings to be protected are warehouses or bunkers without environmental control. In severe weather, temperatures and relative humidity inside such buildings may fluctuate almost as much as outside.

Three types of standard environmental test profiles are available in the current software. These are called (1) the Engineering Test, which is a simple profile with several temperatures above and below room temperature, (2) the Mil Std 810C Temperature Test, and (3) Mil Std 810C Humidity Test. Each has a set of default parameters that can be modified as needed for a specific test. In each case, the profile is presented to the operator in graphic form and can be modified or completely replaced.

A series of manual tests are conducted at ambient conditions to verify simulator test results. The manual tests must show acceptable agreement with velocity and pattern data. A manual oscillatory motion test may also be performed, and the results must agree within experimental error limits of the simulator.

To illustrate the typical output of SIMS, the results of detection pattern tests on a microwave sensor as a function of temperature are shown in Figure 3. This sensor was tested at several other temperatures too, but only three are plotted together for clarity.

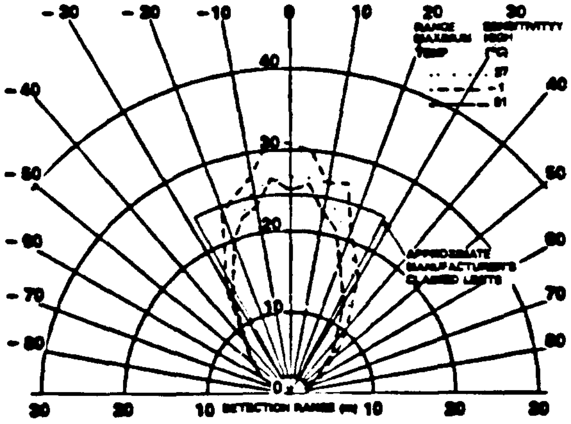


Figure 3. Typical Microwave Sensor Test Results

Figure 4 is a sample of passive infrared motion sensor test results. This plot defines the detection pattern for a specific velocity, Delta T, temperature and relative humidity. Several plots may be combined on one graph so that the relative effects of velocity or environment may be viewed. More information on this subject is available in the references listed in the Bibliography.

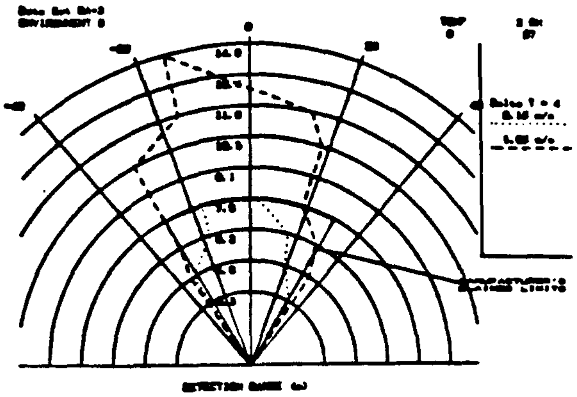


Figure 4. Typical Infrared Sensor Test Results

Data generated by the Interior Sensor Laboratory and other intrusion detection groups at SNL, as well as information from different government agencies, DOE labs, the DoD, and commercial security equipment suppliers, were combined by SNL to form the "Intrusion Detection Systems Handbook." This Handbook was first published in November 1976 and updated annually until it was discontinued in 1984.

INTERIOR SENSOR AND ENVIRONMENT MONITOR

Ideally, alarm systems should respond only to intruders and should disregard benign stimuli. This ideal, however, is difficult to achieve because intrusion sensors are unable to distinguish between harmless and harmful stimuli. Nevertheless, by being attentive to the selection and placement of the sensors and through a proper understanding of the environment, it is possible to achieve both an effective and a reliable alarm system. With this goal in mind, SNL developed a special purpose data acquisition instrument, the Sensor and Environment Monitor (SEM). At the same time that the SEM records a sensor's response to an environment, it can gather substantial data about that environment. This information can then be used to correct a system plagued by nuisance or false alarms. By characterizing the environment while sensor installation is still in the planning stage, SEM can provide invaluable assistance in the installation process.

The SEM was designed as a custom instrument and was fabricated as a prototype. Its main function is to measure and record the more common environment parameters known to stimulate interior intrusion sensors. In addition, its function is to record the sensor's response to any stimulus. The SEM is capable of measuring up to 16 analog signals and four digital inputs. Eleven of the analog inputs are dedicated to the following environmental parameters: temperature, relative humidity, barometric pressure, wind, A.C. line voltage, ambient light, electric field, three axes of acceleration, and sound. The remaining five analog and four digital inputs are for general use and can be connected to the intrusion sensors being tested. Normally, the analog output of an intrusion sensor is connected to the SEM's analog input, and the sensor's alarm contacts are connected to the SEM's digital input. Figure 5 shows the SEM and host software block diagram.

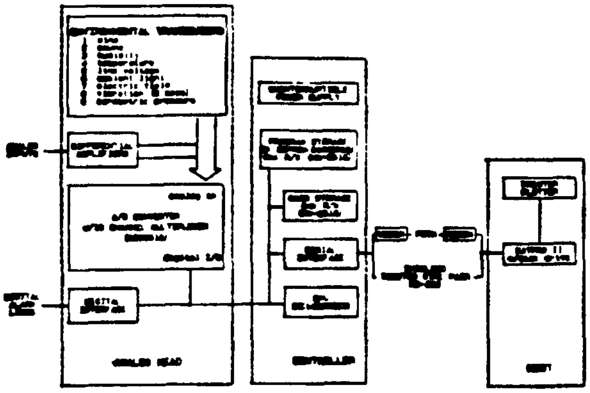


Figure 5. SEM and Host Software Block Diagram

When sufficient data is recorded, it is transferred from the SEM to a portable host computer. Either a dedicated wire or a Public Switched Telephone Network (PSTN) line can be used to transfer these data. The portable computer can then be used to reduce and display the data either in tabular or graphic form.

The SEM was custom designed and thus its volume and power requirements are less than what commercial instruments require. The SEM consists of two main subassemblies: the digital controller and the analog head (see Figure 6).

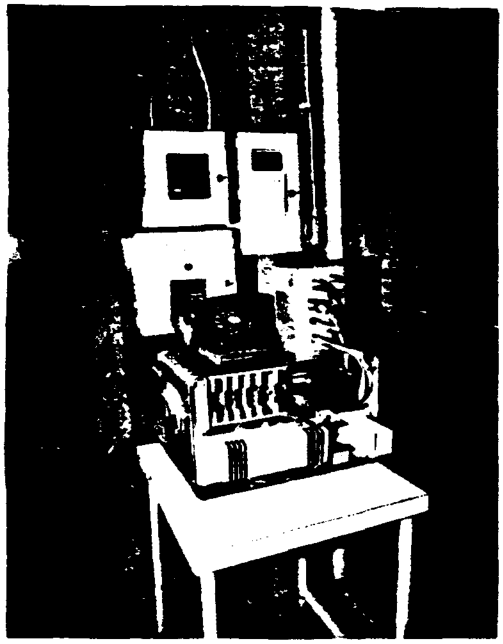


Figure 6. An Alarm System (on the wall) being Monitored by the SEM

The controller is lodged in a standard 17-in. wide, 5-in. high card cage which accommodates a Central Processing Unit (CPU), mass storage memory, interface circuits, and an uninterruptible power supply.

The analog head measures 5 x 6 x 9 in. and contains all the environmental sensors and analog circuits. It communicates with the controller via a multiconductor cable which carries only digital signals.

The entire SEM is powered by an uninterruptible power supply which is built into the controller. The total power requirement for the SEM is 3W. The unit is normally powered by 110 VAC, but a 24V battery is provided to serve as battery backup during power failures. The SEM draws 120 mA from the battery.

During shipping, the controller and analog head are contained within a portable equipment case which measures 13 x 16 x 21 in. The equipment case is large enough to house the modem, interconnecting cables, and three generic interior intrusion sensors as well.

Further use of the SEM should result in additional insight for interpreting the data gathered by this acquisition system. The knowledge gained regarding the performance of individual sensors complements Sandia's already extensive data base which has been compiled on interior intrusion sensors.

Due to the SEM's modular design, it could serve as a general purpose data acquisition system with differential input amplifiers connected to the 16 analog channels. By reprogramming the SEM and the host computer, a totally different functioning system could be realized.

At the time the SEM was designed, the Kapro II computer was among a handful of portable computers offered by manufacturers. Since then a Gridcase Computer became the host computer. For even more portability, the digital controller was eliminated by transferring its functions to the Gridcase. More information on this subject is available in the references listed in the Bibliography.

SANDIA INTERIOR ROBOT

The Sandia Interior Robot (SIR) is a prototype mobile robot system configured to function as part of an overall security system at a high security facility. The features of this robot system include specialized software and sensors for navigation without the need for external locator beacons or sign posts, sensors for remote imaging and intruder detection, and data link facilities to communicate information either directly to an electronic security system or to a manned central control center. Other features of the robot system include low weight, compact size, and low power consumption. The robot system can operate either by remote manual control, or it can operate autonomously where the need for direct human control is limited to the global command level. The robot can act as a mobile remote sensing platform for visual alarm assessment or roving patrol, or as an exploratory device in situations potentially hazardous to humans. This robot system may also be used to walk-test intrusion detection sensors as part of a routine test and maintenance program for an interior intrusion detection system (IDS), and to provide a programmable, temporary sensor capability to backup an IDS sensor that has failed. This capability may also be used to provide improved sensor coverage of an area that will be secured on a temporary or short-term basis, thereby eliminating the need for a permanent sensor installation.

The SIR system was originally designed as a test-bed system to develop navigation algorithms and to evaluate sensing devices and methods. The initial design philosophy was to use a remote host computer for algorithm development in a high-level language and to integrate that computer or its functional equivalent on board in later stages of system development. Therefore the system presently consists of two main elements: a mobile robot platform and a remote host computer (see Figure 7).

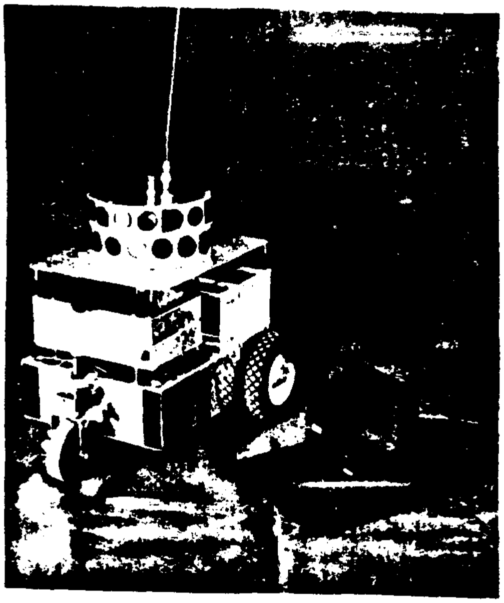


Figure 7. SIR Mobile Platform and Remote Host

The mobile platform (hereafter referred to as SIR) contains an on-board central processing unit (CPU) that handles data transmission via a radio link to and from the host computer and controls hardware operations such as motors and sensors on SIR. The host computer handles other functions which can be generically described as either high-level decisions or man/machine interfacing. The high-level functions include such navigation problems as path planning, path execution, obstacle avoidance, position estimation, and detection/elimination of position errors. The man/machine interfacing functions include translation and presentation of SIR-generated sensor data for human interpretation and translation of human-initiated global commands (such as "go to room X") into a series of machine instructions that SIR can execute.

The host computer is an "off-the-shelf" IBM PC compatible machine fitted with 512KB RAM, an asynchronous serial communications port, and typical keyboard, disk drive and monitor display hardware.

The mobile platform is a front-steered, rear-drive, wheeled tricycle arrangement with a minimum turning radius of approximately 22 in. that weighs approximately 22 lb. It is 24 in. long, 17 in. wide, and 20.5 in. high with a circular array of 30 Polaroid ultrasonic (sonar) transducers. Other sensors presently installed on SIR include an optically encoded magnetic compass to provide azimuth information, an optically encoded odometer to record travel distance, and an optically encoded steering gear head/motor for steering wheel position information used in navigation. A remotely controllable Charged-Coupled Device (CCD) television camera is mounted on a panning platform which turns concurrently with the front wheel.

The software, diagrammed in Figure 8, includes a dead-reckoning routine for position estimation in navigation, an I/O section for communication with SIR, and a remote control routine to allow manual control of SIR. These constitute the very basic functions. The system's usability has been expanded by the addition of graphics and digital data displays, "user-friendly" features such as prompts or a numeric grid overlay to aid an operator in position estimation, and an audible proximity warning tied to sonar data to warn of possible imminent collisions. Also included are a position-estimation routine which relies on a sonar data base located in RAM and can account for and remove accumulated errors derived from the dead-reckoning routine, and a collision avoidance routine which allows the robot to negotiate unforeseen obstacles. Digital maps are prepared by remote control of SIR and use of the ultrasonic sensor array for data collection.

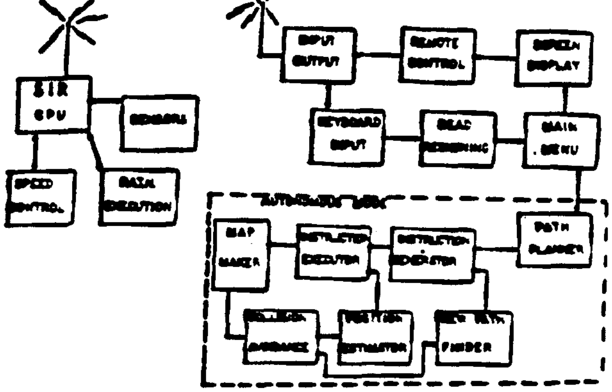


Figure 8. SIR Software Block Diagram

Alarm assessment is an excellent application for SIR. In the case of an alarm from a sensor not collocated with the robot, the robot must be notified that a sensor has gone into alarm, either directly by the IDS system via the data link, or by the operator. SIR will then use the location of the alarmed sensor as a destination for its path planner and will proceed to that location using the aforementioned navigation techniques, providing video information along the way. The task of backing up, or providing alternative sensor coverage for a failed IDS sensor, makes use of the 30 ultrasonic range finders as a programmable motion sensor. The proper configuration of range sensitivity in the software will produce a custom-configuration of the sensor coverage area, one that can be virtually any shape or combination of shapes including a "corridor of insensitivity" with detection on both sides. It also has the unique capability of "presence" detection. In addition to detecting motion, it can detect the addition or subtraction of an object within its 70 foot diameter field-of-view.

SIR has been used to perform walk-testing of microwave motion sensors while in a hazardous environment. Conducting this test using human walkers would have been extremely difficult, dangerous, and would have produced data of questionable value. The system can be configured to report directly to an electronic security system's central computer via radio link, thus virtually eliminating the need for direct human interaction (though this might not be desirable in some cases). Within the security field are many mundane or hazardous tasks that the system can perform with minimal human interaction.

More information on this subject is available in the references listed in the Bibliography.

WEAPONS STORAGE VAULT SENSORS

Increased concern for the security of aircraft carried weapons during storage brought about development of a hardened storage vault for installation within the aircraft shelter itself. This Weapons Storage Vault (WSV) was built below grade with a self-contained elevator to raise the weapons for aircraft loading through a secure control system (Fig. 9). The top of the vault was the floor of the shelter so it had to withstand large compressive loads and fuel spills, etc. It was designed to detect attack on the vault from the top or sides and provide approximately 30 minutes of delay. The sensors were required to have no more than one false alarm per year and a 20-year lifetime.

The Interior Sensor Lab developed a flexible printed circuit approximately 5 ft. wide by 14 ft. long that was glued to the underside of the vault steel top that would detect any penetration greater than 0.050 in. Special cable assemblies attached to the rebar in the sides of the vault before the concrete was poured provided penetration sensors in the side walls. Both had redundant circuits since they became integral parts of the final assembly and cannot be replaced. A series of tests, including collapsing the shelter onto the vault, was conducted. During these tests, the sensors continued to operate as designed without false alarm or failure.

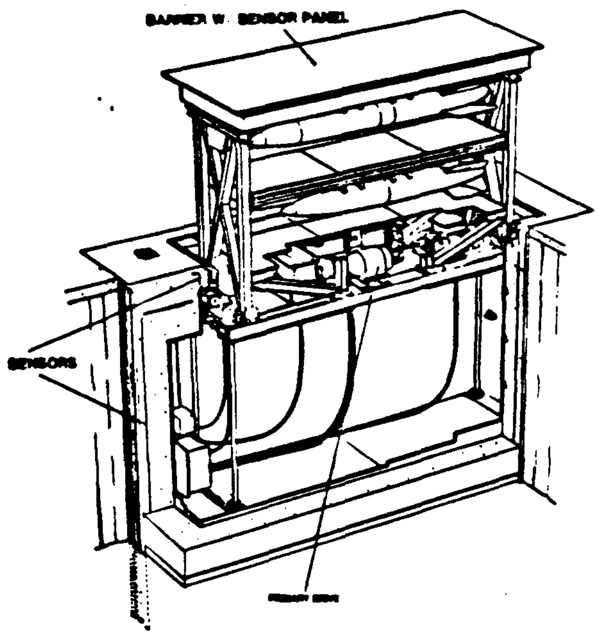


Figure 9. Weapons Storage Vault

CAPACITANCE PROXIMITY BLANKET

Interior capacitance proximity sensors are often used to detect unauthorized access to metal objects. They are sensitive to changes in capacitance between the protected object and ground which are caused by the approach of an intruder or another object. This change in capacitance is sensed by a tuned circuit located in the control unit. For normal installations, the item to be protected must be located away from walls and isolated from ground. The Interior Sensor Lab developed a capacitive blanket that can be used with commercial control units to protect objects that must remain grounded. In this case, the blanket is draped over the protected object, which can be considered the ground plane, and connected to the control unit as shown in Figure 10. If the blanket is made large enough to cover the object entirely, any access attempts will cause blanket movement and/or capacitance change and an alarm.

EXPERT SYSTEMS

The Interior Lab began a series of evaluations on expert systems to determine if they were suitable for use in intrusion detection sensor selection, system design, and alarm diagnosis. As people come and go, the knowledge of the "experts" is lost. It was hoped that the use of expert systems might help store this knowledge in a retrievable format for later use in intrusion detection system designs.

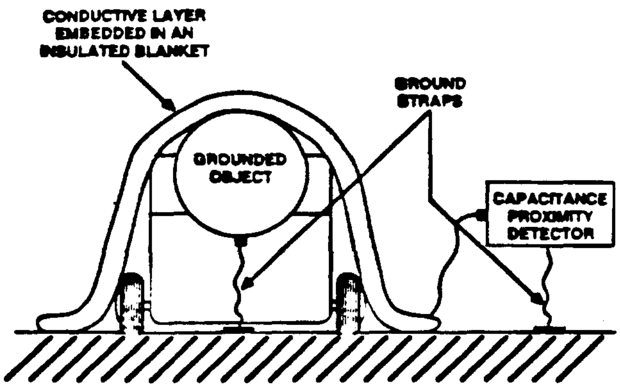


Figure 10. CAPACITANCE PROXIMITY BLANKET

The systems work by asking an operator for site-specific information to determine which sensors are most applicable to the facility.

Site-specific questions would cover subjects such as building construction, lighting types, noise sources, and coverage distance. After evaluating the information, the expert system would provide a list of sensors best suited to the facility.

The evaluations did show the potential for expert system use in system design, but the evaluations were not completed due to limited funding.

SUMMARY

Interior Intrusion Detection Technology began at Sandia National Laboratories (SNL) in 1975 as part of the Fixed Facilities Physical Protection Research and Development Program sponsored by the U. S. Department of Energy in connection with their nuclear safeguards effort. The Interior Sensor Laboratory was established in 1976 to evaluate commercial interior intrusion sensors and to assist in site-specific intrusion detection system designs, as part of our goal of providing high-quality interior detection systems. Many products were (and are) available; the good ones had to be identified and their capabilities and limitations determined. This required developing special test techniques and new test equipment. Accordingly, the Sandia Intruder Motion Simulator (SIMS) was designed and built to test motion sensors under computer control, which is far superior to earlier methods of manual walk testing, or the use of a motor-driven mannequin. New sensors with greater capabilities regularly appear on the market, which demands continuous examination of the changing technology. This, in turn, means that the evaluation procedures and equipment must be updated to stay current.

The Sensor and Environment Monitor (SEM), a special-purpose data acquisition system, was developed to aid in designing new interior systems and in diagnosing existing detection systems with unacceptable false-alarm rates.

The most recent example of specialized intrusion detection equipment is the Sandia Interior Robot (SIR). A small, self-contained mobile sensor platform, it can be used to assess alarms, detect intruders, and walk-test sensors without direct human involvement.

At the Interior Sensor Laboratory, if commercial sensors are unavailable for certain tasks, new sensors are developed, tested, and implemented in the field. The barrier sensors for the Weapons Storage Vault (WSV) are one example. For some unusual situations, sensors are combined, often in unconventional ways, to obtain the desired detection. For instance, a capacitance proximity blanket was developed to couple with a commercial control unit to provide protection for grounded objects.

Future applications of artificial intelligence and expert systems in interior intrusion detection include the areas of sensor selection, system design, and alarm diagnosis.

Interior intrusion technology at Sandia National Laboratories has reflected funding cuts recently, and its future is uncertain at this time.

ACKNOWLEDGEMENTS

The authors wish to express their appreciation to R. A. Darnell, J. J. Harrington, R. S. Howard, D. P. Jones, P. R. Klarer, D. L. Mangan, J. D. Williams, and R. J. Sons, of Sandia National Laboratories; J. D. Schmutz, of Holmes & Narver; and G. M. McNerney of US Wind Power Systems, Inc. for their contributions to this paper.

BIBLIOGRAPHY

Harrington, J. J., "Interior Sensor and Environment Monitor," Proceedings of Nuclear Materials Management, July 21-24, 1985.

Harrington, J. J. and P. R. Klarer, "Sandia Interior Robot (SIR-1): An Autonomous Mobile Sentry Robot," SAND87-0226, Sandia National Laboratories.

Mangan, D. L., "DOE-Sponsored Evaluations of Interior Intrusion Detection Systems," SAND77-1505C, Sandia National Laboratories, Feb. 78.

Schmutz, J. D., G. M. McNerney and R. M. Workhoven, "Motion Sensor Evaluation Using Simulation," SAND84-0539C, Sandia National Laboratories, July 84.

Sons, R. J. and R. H. Graham, Jr., "A Subtractive Approach to Interior Intrusion Detection System Design," SAND86-0654, Sandia National Laboratories, July 1986.

DISTRIBUTION:

DOE/TIC-4500 (Rev 74) UC-15 (190)

Department of Energy
Office of Safeguards and Security
Richard W. Brown, Director
DP-34
Washington, DC 20545

U.S. Department of Energy
Office of Safeguards and Security
Div. of Policy & Program Support
W. Barker, Director
DP-341
Washington, DC 20545

U.S. Department of Energy
Office of Safeguards and Security
Division of Safeguards
Glenn A. Hammond, Director
DP-342
Washington, DC 20545

U.S. Department of Energy
Office of Safeguards and Security
Division of Security
Director
DP-343
Washington, DC 20545

U.S. Department of Energy
Office of Safeguards and Security
Acting Chief
Technical Development Branch
DP-341.2
Washington, DC 20545

U.S. Department of Energy
Safeguards and Security Division
D. D. McIntyre, Director
Albuquerque Operations Office
P.O. Box 5400
Albuquerque, NM 87115

U.S. Department of Energy
Safeguards & Security Division
E. J. McCallum, Director
Chicago Operations Office
9800 South Cass Avenue
Argonne, IL 60439

U.S. Department of Energy
Central Training Academy
R. E. Sabre, Director
P.O. Box 18041
Albuquerque, NM 87185

U.S. Department of Energy
Safeguards and Security Division
G. T. Miserendino, Director
Savannah River Operations Office
P.O. Box A
Aiken, SC 29802

U.S. Department of Energy
Division of Safeguards and U.S.
Security
R. S. Bostian, Director
Idaho Operations Office
785 DOE Place
Idaho Falls, ID 83402

U.S. Department of Energy
Safeguards and Security
Division
E. W. Adams, Director
Nevada Operations Office
P.O. Box 14100
Las Vegas, NV 89114

U.S. Department of Energy
Safeguards and Security
Division
D. J. Cook, Director
Oak Ridge Operations Office
Oak Ridge, TN 37830

U.S. Department of Energy (2)
Safeguards and Security
Division
J. A. Bullian, Director
Pittsburgh Naval Reactors
Office
P.O. Box 109
West Mifflin, PA 15122

U.S. Department of Energy (2)
Safeguards and Security
Division
K. B. Jackson, Director
Richland Operations Office
825 Jadwin Avenue
P.O. Box 550
Richland, WA 99352

U.S. Department of Energy (2)
Safeguards and Security
Division
R. R. Fredlund, Director
San Francisco Operations Office
1333 Broadway, W. F. Building
Oakland, CA 94612

U. S. Department of Energy
Mr. Donald L. Alf
Office of Naval Reactors
Room 4513
Washington, Dc 20223

U.S. Department of Defense
LTC Richard Swanson, Chairman
DoD Physical Security Action
Group
OUSDRE/TWP/SP
The Pentagon
Washington, DC 20301

U.S. Department of Energy
Security Division
Director, Strategic Petroleum Reserve
Project Management Office
900 Commerce Road East
New Orleans, LA 70123

U.S. Department of Energy
G. M. Arriola
Los Angeles Security Office
P.O. Box 1949
Los Angeles, CA 90053

U.S. Department of Energy
Office of Military Application
Lew Newby, Director
Safety & Emergency Actions
DP-226
Washington, DC 20545

U.S. Department of Energy
Robert K. Peterson
Office of Military Application
DP-226.1
Washington, DC 20545

U.S. Department of Energy
Administrator
Western Area Power Administration
P.O. Box 3402
Golden, CO 80401

U.S. Department of Energy
Robert L. Windus, Security Manager
Bonneville Power Administration
P.O. Box 3621
Portland, OR 97208

U.S. Department of State
Wallace H. Gilliam
A/SY/OPS/T
3810A
Washington, DC 20520

U.S. Secret Service
Mr. Richard J. Solan, Chief
Technical Development & Planning Div.
1800 G Street N.W., Room 941
Washington, DC 20223

National Aeronautics and Space
Administration
John C. Hagan
Security Office (NIS)
Washington, DC 20546

Los Alamos National Laboratory
Darryl B. Smith
Q-DO/E550
Los Alamos, NM 87545

Central Intelligence Agency
Director, Office of Security
202 Jefferson
Washington, DC 20505

U.S. Arms Control & Disarmament
Agency
Chief
Nuclear Safeguards & Tech Div.
320 21st Street, N.W.
Washington, DC 20451

U.S. Nuclear Regulatory
Commission
Raymond Brady, Director
Division of Security (2)
Washington, DC 20555

U.S. Nuclear Regulatory
Commission
J. Partlow, Director
Division of Inspection Programs
Washington, DC 20555

U.S. Nuclear Regulatory
Commission
Director
Division of Safeguards (4)
Mail Stop 881-SSS
Washington, DC 20555

National Security Agency
Glenn M. Bell
M512
Ft. Meade, MD 20755

U.S. Department of Energy
David E. Bailey, Director
Division of Fuels and Reprocessing
NE-551
Washington, DC 20545

Hanford Engineering Development
Laboratory
Dan T. Johnson
Security Applications Center
P.O. Box 1970, W/B-1
Richland, WA 99352

Belvoir Research, Development
and Engineering Center
Attn: STRBE-JI (A. Zushin)
Fort Belvoir, VA 22060-5606

Belvoir Research, Development
and Engineering Center
Product Manager
Physical Security Equipment
Attn: AMCPM-PSE
Fort Belvoir, VA 22060-5606

U.S. Department of Justice
Harry Frankel
Immigration & Naturalization Service
425 I Street, N.W.
Washigntón, DC 20536

Holmes & Narver, J. D. Schmutz

US Wind Power Systems, Inc., G. M. McNerney

3141	S. A. Landenberger (5)
3151	W. L. Garner (3) for DOE/TIC Unlimited Room 3810A Release)
3161	N. S. Hey
5200	W. C. Myre
5210	J. J. Baremore
5217	D. L. Mangan
5219	R. Moya
5219	R. J. Sons
5219	R. H. Graham (10)
5220	A. A. Lieber
5230	M. L. Kramm
5233	R. S. Howard
5240	D. S. Miyoshi
5249	B. J. Steele
5249	R. Darnell
5250	T. A. Sellers
5260	J. Jacobs
5260A	J. D. Williams
5267	J. R. Kelsey
5267	J. J. Harrington
5267	D. P. Jones
5267	P. R. Klarer
5267	R. M. Workhoven (10)
8024	P. W. Dean