

CONF-970744--13

SAN097-1799C  
SAND--97-1799C

## Rapid Deployment Intrusion Detection System

Robert H. Graham  
Sandia National Laboratories  
Department 5838, MS 0780  
Albuquerque NM 87185-0780

RECEIVED  
JUL 30 1997  
OSTI

### Abstract

A rapidly deployable security system is one that provides intrusion detection, assessment, communications, and annunciation capabilities; is easy to install and configure; can be rapidly deployed, and is reusable. A rapidly deployable intrusion detection system (RADIDS) has many potential applications within the DOE Complex: back-up protection for failed zones in a perimeter intrusion detection and assessment system, intrusion detection and assessment capabilities in temporary locations, protection of assets during Complex reconfiguration, and protection in hazardous locations. Many DOE user-need documents have indicated an interest in a rapidly deployable intrusion detection system. The purpose of the RADIDS project is to design, develop, and implement such a system.

### Background

Several "rapidly deployable" intrusion detection systems have been developed in recent years. Some of these are little more than sensors mounted on tripods, while others are comprehensive systems offering sensor-to-annunciator capabilities. Market surveys revealed that the comprehensive systems tended to focus on military applications and had extensive hardware-related logistics costs. The less capable elements were stand-alone components and did not provide a system-level product. Although several good components are available, few addressed the specific needs of the Department of Energy. Consequently, Sandia began a project to provide a system-level, rapidly deployable intrusion detection system for DOE. The intent of this project was not to develop new hardware but to integrate existing commercial components into a viable system-level product.

### Design Guidelines

Several guidelines were followed in the development of the rapidly deployable intrusion detection system:

RAPIDLY DEPLOYABLE—provide a short-term, rapidly deployable system that could be installed in a few hours or a few days depending upon the application

LOW COST—reduce or eliminate the costs associated with fixed-installation cabling and guard personnel

LOW POWER—provide a system capable of using either site ac power or battery and/or solar power

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

MASTER

COMPATIBLE WITH EXISTING INFRASTRUCTURE—communicate RADIDS alarms to existing DOE central alarm stations

VIDEO ASSESSMENT CAPABILITY—provide a rapidly deployable assessment capability with jamming detection

WIRELESS ALARM TRANSMISSION—provide for reliable wireless communication of alarms

EASY TO CONFIGURE FOR SPECIFIC APPLICATIONS—provide a system able to be deployed and configured by trained site-security personnel without the need for outside experts.

Some of these guidelines may run counter to each other depending on the application. Obviously, there will have to be tradeoffs between these guidelines.

### System Level Operation

The system-level block diagram (Figure 1) shows how the communication device at the annunciation location arbitrates radio frequency (RF) communications between sensor pods and the annunciator. This coordination will prevent simultaneous and conflicting transmissions originating from the sensor pods. When an alarm, tamper, or other fault condition transmission is received from a sensor pod, the annunciator communication device passes that message to the annunciator for display to the operator. If the received transmission is an alarm, the annunciator communication device instructs the sensor pod communication device to send the previously captured alarm video image.

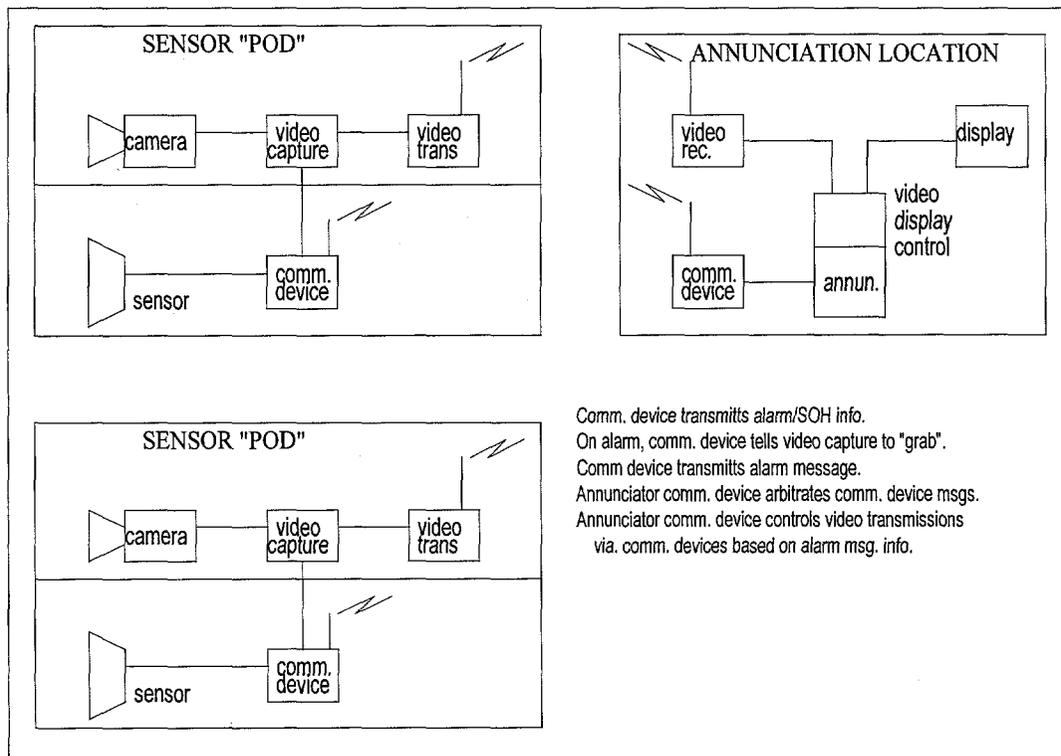


Figure 1. RADIDS system-level block diagram

The operator also has the option of requesting a current or live video image (depending upon the video transmission capabilities). The annunciator communication device will pass that request to the appropriate sensor pod communication device.

The sensor pod communication device periodically sends a state-of-health message to the annunciator communication device to ensure link integrity.

### **Sensor Pod Operation**

The sensor pods contain two modules: (1) the sensor and communication module, and (2) the assessment module (camera, video capture, and video transmission). Not all applications, however, require an assessment device with each sensor.

When an alarm, tamper, or other fault condition is detected at the sensor and relayed to the sensor pod communication device, the communication device transmits that information to the annunciator communication device. If the condition detected is an alarm, the sensor communication device will pass a message to the video capture element of the assessment module. This module will then snap a video image and process it for transmission to the annunciator display. After the annunciator communication device receives the alarm message it requests the video image from the sensor pod. When the video image request is received from the annunciator communication device, it passes the message to the assessment module which then begins to transmit the video image. The annunciator communication device must request assessment images to avoid video image transmission collisions if multiple alarms occur in a near simultaneous time period.

Sensor installations and sensor pod electronics are mounted on tripods similar to those used and tested in prototype installations for the Department of Defense. The tripods are typically stabilized with guy wires or sandbags.

A lighting element is an additional element that needs to be located with the assessment portion of the sensor pod. Unless thermal imagers are used, lighting is required for video assessment activities. For many applications existing light will be sufficient. For others it will be necessary to provide additional light. Tradeoffs between lighting and power requirements will obviously have to be made. There are also operational considerations: should lighting be provided continuously or only during alarm and video capture activities? One option may be to use nonvisible infrared flash lighting.

### **Power**

Having an adequate power supply system is important to the overall design of RADIDS. Although it is not possible to fully design the power supply portion of RADIDS until equipment is selected and actual power consumption requirements are determined, it is possible to develop the overall conceptual design for the power supply system. The power supply units for RADIDS will have a multiple-input capability and will be similar to the power supply units used for the US Air Force Tactical Automated Security System (TASS) program. These units will be capable of accepting 120-VAC grid power and regulating it for the sensor pods. It will also have a battery backup capability. Additionally, the power supply units will be capable of accepting solar panel inputs for battery charging and power

augmentation purposes. Figure 2 shows a prototype power supply unit with a solar panel attached.

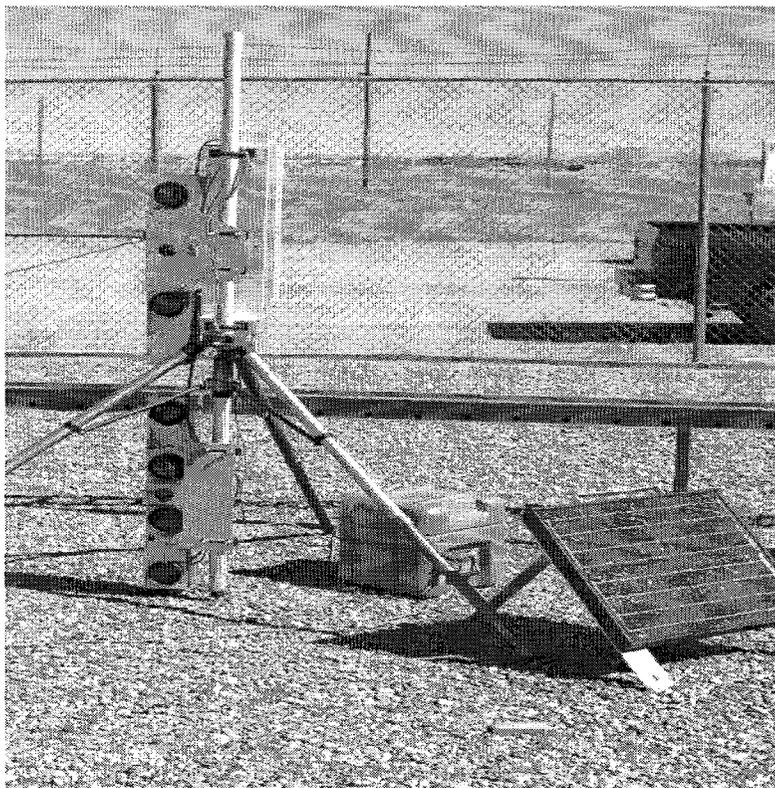


Figure 2. Prototype power supply unit with solar panel

## **Annunciator Operation**

The annunciator module consists of an annunciator display, a video display controller, an alarm assessment video display, a video RF receiver, and an RF communication device which will arbitrate communications between the various modules. The video display controller could be part of the annunciator computer, but in this case it is a separate monitor.

The annunciator display is a map-based, graphical interface with drag-and-drop icons and is designed to allow the operators to configure the annunciator to each site. This annunciator uses many of the features that have been previously prototyped in the USAF TASS program. One goal of the RADIDS project was to have the RADIDS annunciator interface to other annunciators, such as the ARGUS system.

The assessment display is a pair of standard monitors: one display presents alarm images and the other presents live or current images.

## Commercial vs. Custom Hardware

Another important goal of the RADIDS project was to keep the number of developmental items to a minimum. As a result, most components are in fact commercial:

- sensors
- RF communication modules
- video transmission modules
- frame grabbers
- annunciator hardware (PC)

Some of the few custom elements in the RADIDS are:

- annunciator software
- RF communication module software
- small interface card for the frame grabber.

It is hoped that all custom items will be transferred to commercial sources and become commercial items.

## Issues

Some issues exist concerning the actual use of an RF-based rapidly deployable intrusion detection system. Most of these issues address the lack of requirements regarding the use of RF communication devices in high-security environments. Some of these issues are:

- How often should state-of-health messages be received to be considered a tamper?
- What level of encryption is required in various applications?
- What constitutes redundancy in an RF system?
- Is video encryption required? If so, where and at what level?

RADIDS will continue to be defined as these issues are addressed. The result will be a final product that will better meet customer needs and expectations.

## DISCLAIMER

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, 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 or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

---

**DISCLAIMER**

**Portions of this document may be illegible  
in electronic image products. Images are  
produced from the best available original  
document.**