

SAND96-3029C
SAND-96-3029C
SPIE 2939-15

Technologies for security, military police and professional
policing organizations, the Department of Energy perspective

Basil J. Steele

Sandia National Laboratories
PO Box 5800, MS 0768
Albuquerque, NM 87185-0768

CONF-961113--20

RECEIVED

JAN 06 1997

OSTI

ABSTRACT

There are many technologies emerging from this decade that can be used to help the law enforcement community protect the public as well as public and private facilities against ever increasing threats to this country and its resources. These technologies include sensors, closed circuit television (CCTV), access control, contraband detection, communications, control and display, barriers, and various component and system modeling techniques. This paper will introduce some of the various technologies that have been examined for the Department of Energy that could be applied to various law enforcement applications. They include:

- Scannerless Laser Radar
- Next Generation Security Systems
- Response Force Video Information Helmet System
- Access Delay Technologies
- Rapidly Deployable Intrusion Detection Systems
- Cost Risk Benefit Analysis

2. SCANNERLESS LASER RADAR

The Scannerless Laser Radar is a laser radar system that uses image processing technology to perform perimeter intrusion detection and assessment. Radar range information is used to form a three-dimensional image of intrusion objects. The uses for the Scannerless Laser Radar include wide or narrow security zones, outer fences, secure buffer zones, and airborne rooftop intrusions. The system is useful where lighting conditions are low or nonexistent and where camouflage is present.



Figure 1. Exterior image from scannerless laser radar

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

This work was supported by the United States
Department of Energy under Contract
DE-AC04-94AL 85000.
Sandia is a multiprogram laboratory operated by
Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy.

DISCLAIMER

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

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, make 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.

3. NEXT GENERATION SECURITY SYSTEM

The next generation security system consists of a combination of two technical areas: volumetric video motion detection and distributed virtual reality. These types of systems can be deployed in dynamic environments where human activity and motion clutter are common. These systems allow the user to move throughout a defined environment and generate an alarm when certain defined three-dimensional spaces are violated. The virtual reality images of the environment are sent over existing communication links to a control center for monitoring. The data size of the images required for the virtual images is substantially smaller than those required for normal CCTV images. This type of system can also be used for simulations of tactical measures or to test security strategies.

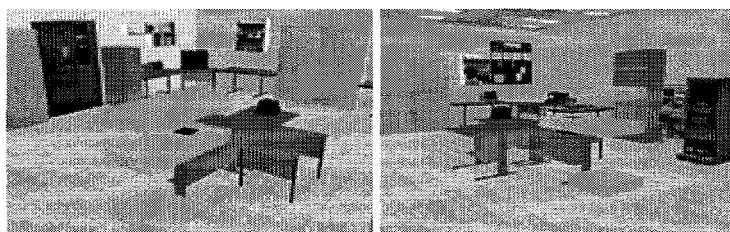


Figure 2. Virtual reality image with volumetric video motion detection

4. RESPONSE FORCE VIDEO INFORMATION HELMET SYSTEM

The Response Force Video Information Helmet System provides a means to share video information among the response force team members and the response force command center. The system will allow the command console operator to select, view, and transmit any response force member's video to the rest of the team. Law enforcement team personnel could use this type of system to provide more complete information sharing between the team members and control center. SWAT teams and special force assault teams could also find a version of this system useful.



Figure 3. Prototype response force helmet

5. ACCESS DELAY TECHNOLOGIES

Research and development of activated dispensable materials include physical characterization, security effectiveness testing, material longevity studies, and toxicology and environmental studies. The materials developed and used for safeguards applications include polyurethane foams, sticky thermoplastics foams, stabilized aqueous foams, chemical smoke, entanglements and deployable barriers, and chemical irritants. These technologies can be used for crowd control and access delay in high security areas where delay times are critical.

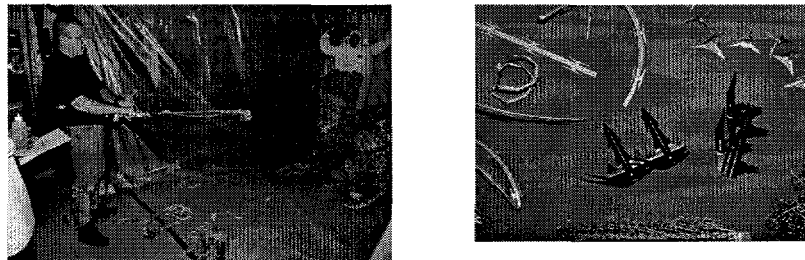


Figure 4. Deployable barriers

6. RAPIDLY DEPLOYABLE INTRUSION DETECTION SYSTEM

These systems are designed to provide intrusion detection, assessment, and delay capabilities that are easy to install, setup, deploy, and reuse. These systems emphasize several technologies: rapid deployment security systems with RF communications, and battery-operated, portable monitors for protection of forces, facilities, and materials worldwide in covert, tactical, and temporary applications. Advanced imaging and alarm assessment technology include long-range and hand-held thermal imaging cameras, still video transmission, and video motion detection/tracking systems. These systems can provide backup protection for an area where the primary detection and assessment system is down or under repair. They will provide security in a temporary location, protect assets/personnel during reconfiguration, and protect areas that are hazardous.

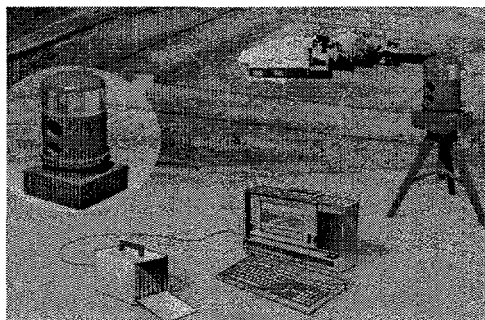
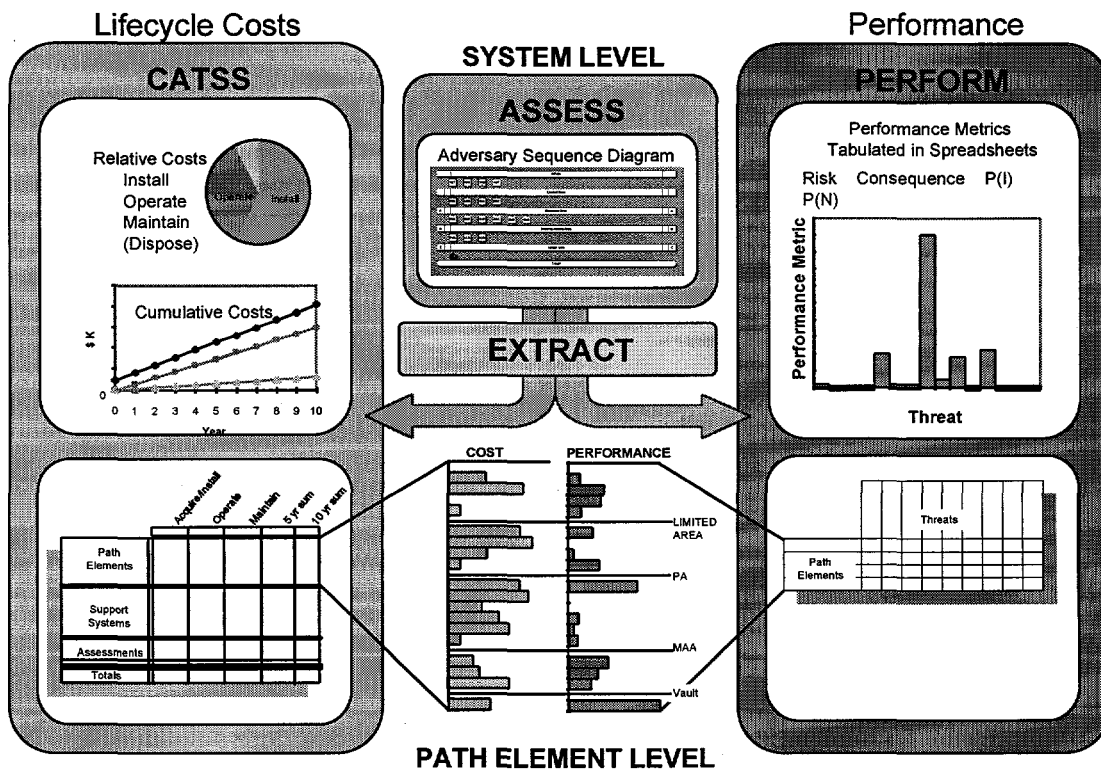


Figure 5. Advance exterior sensor systems

7. COST RISK BENEFIT ANALYSIS

The natural focus of security system design is to increase security at those features or areas that are most obvious and likely to be used by the defined threat. Each improvement moves the attention of the potential adversary to the next easier path of opportunity. The cost of each proposed improvement can be measured against the reduction in vulnerability to determine its worthiness for consideration. As the level of vulnerability decreases, eventually the system will reach the point of "acceptable risk" below which there is an acceptable vulnerability because additional security is not worth the cost. Sophisticated models are being developed to help the law enforcement community and the security system users better analyze their return on security investments as security improvements are applied at a particular facility.



SUMMARY

This paper has presented only a few of the many emerging technologies that are available or are currently being developed to help the security community better detect, delay, and respond to ever changing threats in the world. Applying these technologies in a cost-effective manner is a major concern of the decision makers in both government and industry.