# Intelligent Sensor Fusion for A Mobile Security Robot

The U.S. Navy is using a security assessment algorithm that collectively assesses data from a variety of sensors built into a robot to detect intruders in secure areas.

The U.S. Navy has developed a mobile robot that uses sensor fusion to determine the probability of the presence of an intruder in a secure area (see Photo 1). The robot uses an algorithm that collectively assesses data from 82 sensors and returns a single composite threat value to an operator [1].

The algorithm employs a polar representation of the sensors' data to establish a composite threat score for each of the 24 wedge-shaped zones that make up the area around the security robot (see Figure 1). An operator is alerted to situations in which the composite threat score for a zone rises above the alarm threshold. A threat assessment value in the range of 0–100 acts as a quantitative indicator of classification confidence, and a threat vector originating from the robot's position is graphically depicted on the map display.

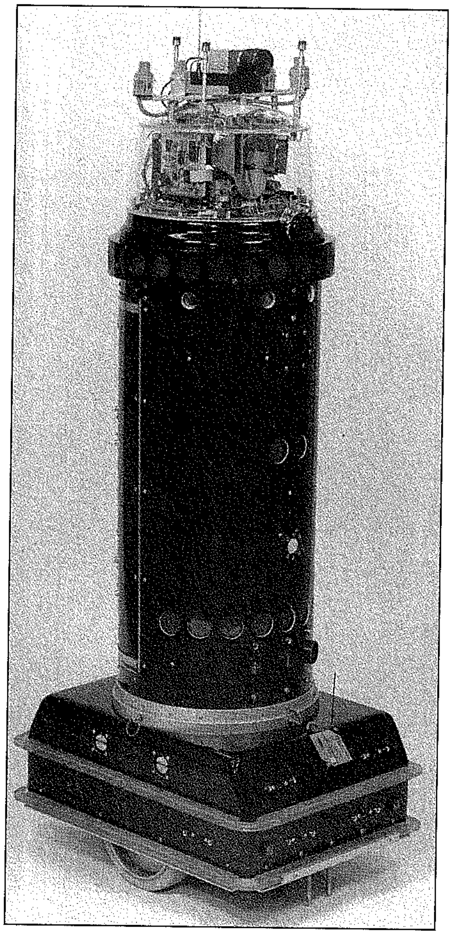

**Photo 1.** *Robart II was the U.S. Navy robotic testbed for the development and initial testing of a security assessment algorithm used to report the possibility of an intruder to a remotely located, manned guard station.*

## SENSOR SUBSYSTEMS

To assess the possibility of an intruder, the robot receives information from five types of sensors: a video motion detector (VMD), an acoustic sensor array (ASA), a passive infrared (PIR) array, a microwave array, and an ultrasonic (sonar) array.

**Video Motion Detector.** The subsystem used on the robot consists of a video camera mounted on a pan and tilt mechanism, which allows the camera to cover the 360° view around the robot. To conserve power, the VMD is activated only when the composite threat is at the warning level, and then it is automatically trained in the direction of the perceived disturbance to confirm or discount the threat. The VMD subsystem includes a video line digitizer, an 8-bit microprocessor, an address controller, and video RAM.

To reduce image processing needs, the VMD digitizes only three select lines from the composite video image. With three lines equally spaced throughout the scene, effective full-screen coverage is achieved without having to grab the entire frame [2].

The vision processor begins data transfer and analysis when the line grabber has completed an acquisition operation. The simplest motion-detection scheme subtracts the current intensity array from a previously acquired array and reacts to significant discrepancies between the two, which indicate a change in the scene under observation. Some software filtering is required to eliminate noise and to reduce the occurrence of nuisance alarms, but this is easily accomplished with a 512-element linear data array.

Assuming 512-pixel coverage, the VMD requires a minimum of 2 KB of RAM to support the PC's operating system and to save the three lines of video data. When motion is detected in any of the three lines, three new lines are selected for motion analysis. If the lines are chosen around the vicinity of the initial disturbance, it is possible, over successive frames, to converge on and effectively bound the area of the intrusion. Thus, the system is able to detect and output

**Richard P. Smurlo and H.R. Everett, Naval Command Control and Ocean Surveillance Center**

information describing the geometric area involved to provide servo-control inputs for camera positioning or robot motion algorithms.

**Acoustic Sensor Array.** A passive ASA provides information on the bearing of the source of the detected noise. The array consists of three omnidirectional microphones symmetrically oriented 120° apart and separated by a distance d. The prototype version of the ASA is shown in Photo 2, with the three transducers individually supported by coil springs. The springs provide a degree of acoustical isolation and raise the transducers to yield a clear path for wavefront propagation without any blockage by the video camera [2].

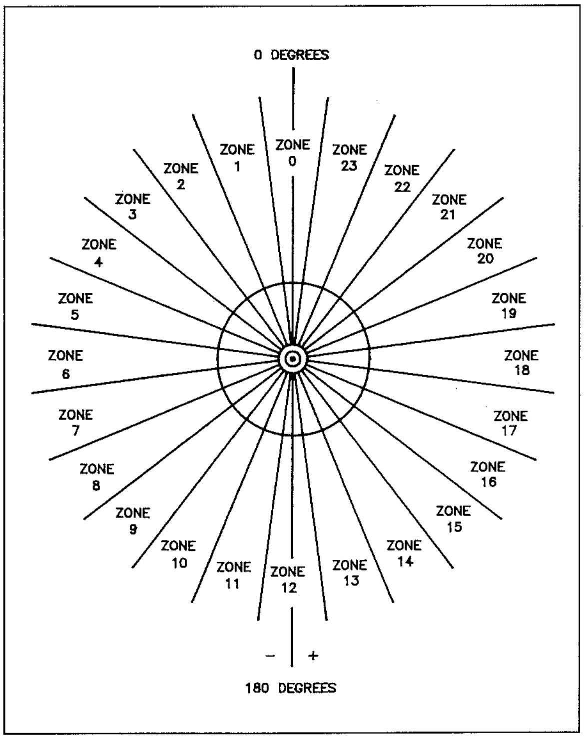


**Figure 1.** *Each of the sensor arrays in the system covers the full 360° surrounding the robot and divides the area into 24 equally sized zones. Values are assigned to the zones by each array based on the state of the sensors covering the zone.*

The ASA calculates the bearing to an acoustical disturbance when the sound travels across the array and triggers all three detection elements in a specific sequence—the order is dependent on the relative position of the source. Because of the symmetrical orientation of the detection elements, the direction of the disturbance can be classified as being in one of six sectors by examining the firing sequence of the comparators associated with each of the detectors. The relative bearing to the perceived source is calculated using conventional triangulation techniques and then converted to an absolute bearing depending on the sector involved.

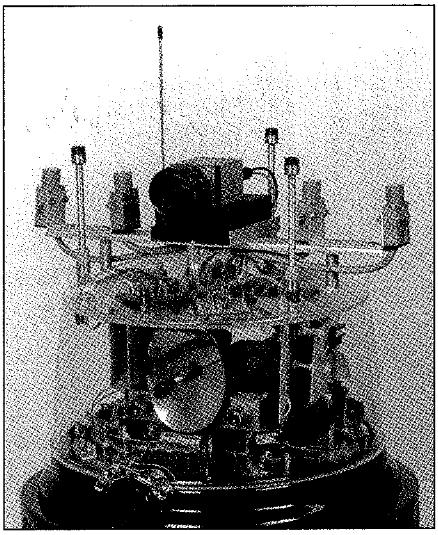

**Photo 2.** *An acoustic sensor array was mounted on Robart II to detect sound in the environment. Data collected from this array are fused with data from a passive infrared array, a microwave array, an ultrasonic (sonar) array, and a video motion detector to determine the possibility of and bearing to a potential intruder.*

**Passive Infrared Array.** PIR motion sensors detect changes in the energy spectrum at the 10 µm wavelength, which are generated by a potential intruder's body heat. This type of pyroelectric sensor is well suited to use on mobile robots because of its small size, low power consumption, excellent performance, and reliability [2].

The PIR array on the security robot consists of 48 sensors arranged in a symmetrical pattern. Each sensor covers a cone-shaped detection field that does not overlap the field of any of the other PIR sensors. After a brief settling period on power-up, the circuit adjusts itself to ambient conditions, and subsequent deviations from that setpoint result in an alarm output. This type of sensor exhibits a low nuisance alarm rate indoors and is weighted heavily when calculating the possibility of an intruder.

**Microwave Array.** Microwave motion detectors are active devices that operate

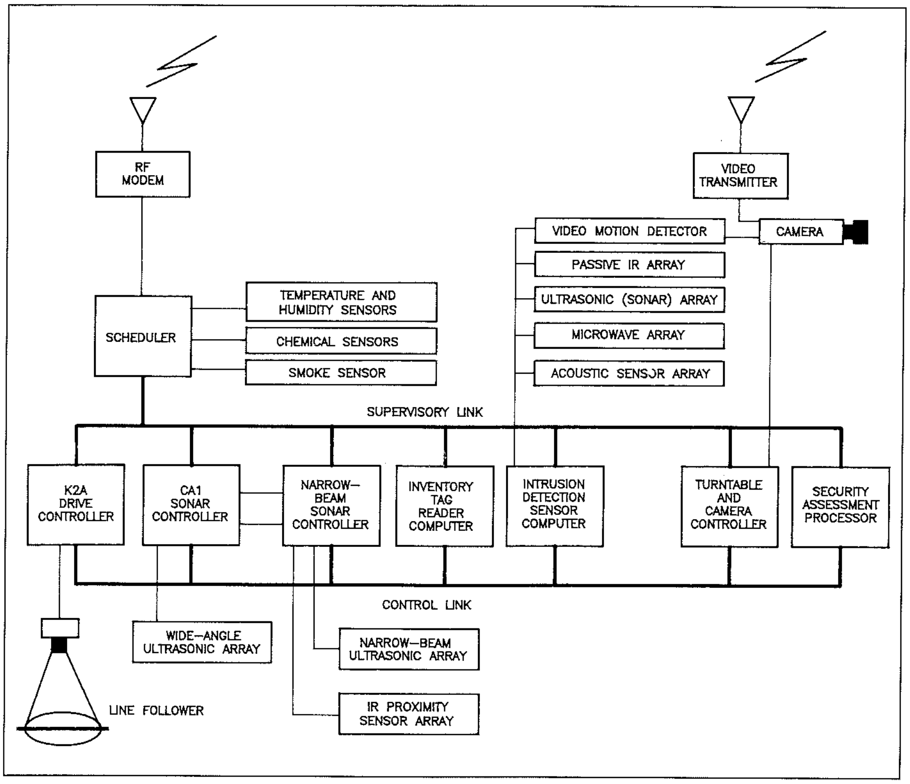


**Figure 2.** *This diagram of the remote platform shows the physical connections of the security assessment system. Sensor timing and data collection are performed by the intrusion detection sensor computer, which transmits the data to the security assessment processor for analysis by the security assessment algorithm.*

at radio frequencies and rely on the Doppler shift introduced by a moving target to sense the relative motion of an intruder. The six microwave sensors of the array are equally spaced to provide full coverage around the robot. Because microwave energy reflects off walls in confined spaces, each sensor tends to flood the room being monitored, so an intruder may activate several sensors simultaneously. To compensate for this omnidirectional effect, the directional information provided by these sensors was weighted less than other sensors in the initial prototype implementation.

**Ultrasonic (Sonar) Array.** This array consists of two Texas Instruments ultrasonic modules multiplexed to 24 Polaroid electrostatic transducers. The modules are active time-of-flight ranging systems developed for automatic camera focusing, and they determine the distance to a target by measuring the elapsed time between pulse transmission and detected echoes.

On initial activation in a security assessment scenario, the 24 sensors of the ultrasonic array are fired to get baseline, or template, range readings. The sonar sensors then fire at a periodic rate and compare the new range readings with the baseline readings. A deviation in the two readings is interpreted as indicating the possible presence of an intruder. Both the range and the bearing of the intruder can be determined using this technique.

**Sensor Arrays.** The arrays described above are independent of one another. Each one does its own local signal conditioning and is connected to input ports on the intrusion detection sensor computer (see Figure 2). The modular design of the sensor arrays, and of the computers themselves, allows subsystems to be easily modified or upgraded when new hardware or improved software algorithms become available [3].

Each sensor array continuously sends information to the intrusion detection sensor computer (see Figure 2), which prefilters the data before reporting it (on request) to the security assessment processor. Once the security assessment processor acquires the information, it determines the probability that an intruder is present and establishes the bearing to the potential intruder. This information is stored until it is requested by the scheduler. The scheduler transmits the information across the RF modem to a control station, where a security guard is stationed.

## DATA ACQUISITION AND ASSESSMENT

On each pass through the main program's security assessment loop (see Figure 3), the state of each sensor is monitored. If a sensor state has changed, its new state is time-stamped and stored in the current information field. The data that were previously in that field are placed at the front of the history list in the same data structure. A detailed history of the state of each sensor is kept for about 5 min.

Also in the data structure is a baseline weight for each sensor, which determines how much each sensor contributes to the overall composite threat assessment value. These values are taken from an array that bases the initial weight on the demonstrated reliability of the sensor.

After new data have been read, the threat assessment function is called, which adjusts the sensor weights when purposeful motion is detected or when different types of sensors correlate with each other. The threat assessment function (see Figure 4) then calculates the composite threat value based on the adjusted weights.

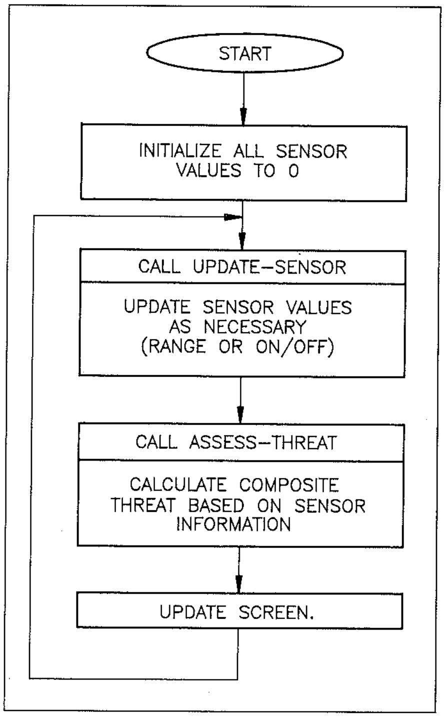


**Figure 3.** *The main program flow updates the sensor information received from the intrusion detection sensor computer and calculates the composite threat based on that information. The composite threat is transmitted to the control station, where the supervisor display screen is updated and an alarm is sounded if an intruder is present.*

**Detecting Purposeful Motion.** The algorithm identifies the first active sensor of a group. If the sensor to the right or the left of the active sensor is also active, the active sensor's weight is increased by a factor of $K_0$. Data stored in the history file are examined to determine if the sensors adjacent to the active sensor have been previously active within a specified period of time. If they were, the weight of the active sensor is increased by an increment equal to its initial weight times a scalar $S_1$.

If an adjacent sensor has been active, the history file is again examined to see if the next sensor in the array detected motion. If previous motion is indicated, the weight of the active sensor is further increased by a second increment equal to its initial weight times a scalar $S_2$.

This process is repeated for the other active sensors of the given type, after which the remaining groups of motion detection sensors are similarly examined. If there is a temporal history of lateral motion across the array's field of view and the adjacent sensors have been activated in a distinct sequence, the resulting signature is classified as purposeful (as opposed to random) motion, and the active sensor weight is significantly increased.

Most of the motion detector arrays on the robot (e.g., the microwave, PIR, acoustical, and video arrays) are capable of angular resolution only, and they pro-

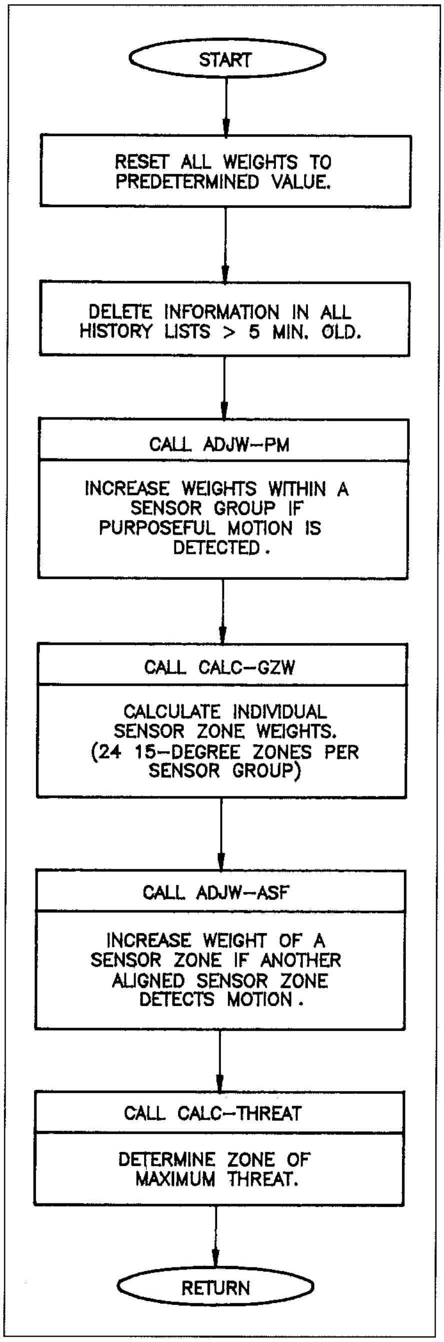


**Figure 4.** *The threat assessment algorithm increments the initial sensor weights for purposeful motion, converts them into 24 equally spaced zones, and increments the zone weights if angular sensor fusion is detected. The maximum zone weight is compared to the alarm threshold to determine if an alarm should be generated.*

vide no range information. An exception is the ultrasonic motion detection array, which identifies a potential intrusion through changes in measured target distances as seen by one or more sensors in the 24-element array. This feature allows an additional level of analysis to be performed on sonar data in the history file.

Purposeful motion of an intruder should result in a continuous target path profile, with no significant discontinuities or jumps in the target's position. When properly exploited, this analysis can be helpful in filtering out inaccurate sonar data (ultrasonic ranging systems operating in air are susceptible to errors caused by beam interaction at the target surface [4]).

To further minimize nuisance alarms resulting from the inherent poor repeatability in range measurements, information from the PIR sensors is fused with data from the ultrasonic motion detection array. Only those changes in sonar range that are validated by a corresponding PIR hit are considered significant by the system. This technique is referred to as cross correlation, or angular sensor fusion.

**Cross Correlation.** The next step in the assessment routine involves converting the individual sensor weights to zone weights for each sensor group. This is done by determining the probability that the potential intruder is in a zone by examining the state of each sensor in the zone.

For example, if an active sensor lies on the boundary of two zones, a 50% probability exists that the intruder is in either zone. The calculated probability is multiplied by the sensor's weight, and the values are summed for each sensor in the zone. The zone weights of each of the sensor groups are checked for correlation and increased or decreased accordingly.

**Composite Threat Calculation.** Once the weight contributions have been generated for the individual sensors of each type, the threat calculation function adds up the individual sensor group weights to produce a composite threat value for each of the 24 zones. The maximum composite threat of the individual zones is used as the current composite threat. To smooth out the composite threat that is displayed on the screen (see Figure 5), the current composite threat is compared with the values calculated in the last 4 s. The maximum of these values becomes the new composite threat.

**Persistence Factor.** The threat magnitude is further adjusted by a persistence factor (PF), which provides an additional predefined contribution to the composite threat score. The PF is indicative of and proportional to the magnitude and duration of prior activity in the area under surveillance. The PF increases system sensitivity for scenarios in which activity was previously detected, though at a level insufficient to generate an alarm condition.

$$PF = \int F(t)\, M(t)\, dt \qquad (1)$$

where F(t) represents a time-dependent weighting function, and M(t) represents the magnitude of the observed composite threat as a function of time.

These can be individually approximated over n arbitrary time increments as:

$$PF = \sum_{i=1}^{n} F_i M_i \qquad (2)$$
$$= F_1M_1 + F_2M_2 + \dots + F_nM_n$$

F(t) can be represented as a linear function that varies from 0 at $T_0$ to 1 at $T_f$, with the time between $T_0$ and $T_f$ divided into n sample periods. For example, if $n = 10$, then $T_1 = 0.1$, and so on up to $T_{10} = 1.0$.

M(t) can be individually implemented as the maximum observed composite threat over any time increment or sample period.

In keeping with the above example that assumed 10 sample periods, the equation would appear as follows:

$$PF = S\,[0.1\,M_1 + 0.2\,M_2 + \ldots + M_{10}] \quad (3)$$

where $M_1$ through $M_{10}$ are the maximum composite threat values observed during sample periods 1 through 10, respectively, and S is a scalar.

The PF should have a maximum upward bound, such as 10, and it would be added to the current composite threat as follows:

final composite threat = initial composite threat + PF

The final adjusted composite threat is compared with a predetermined alarm

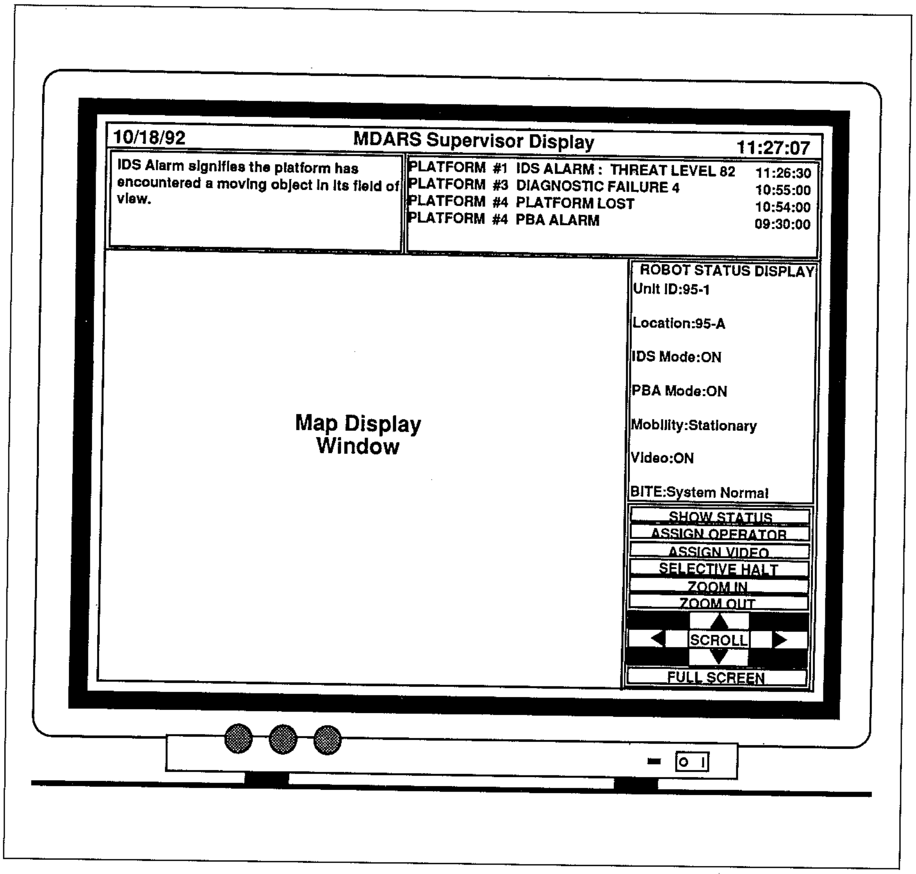


Figure 5. *The supervisor display screen prints the time and composite threat score received from the platform. If the threat score is above the alarm threshold, an alarm is sounded.*

threshold value. If the composite threat exceeds the threshold, it is assumed by the system to be in an alarmed condition. The axis of the active, or alarmed, zone is used to graphically plot a threat vector on the map display at the control station.

## CAUSES OF ALARMS

The initial weight values of each sensor and the multipliers (e.g., S and $K_0$) have been chosen so that the following minimum situations cause the robot to go into an alarm condition:

- A PIR sensor detecting purposeful motion and an active adjacent PIR array, an active microwave sensor, or any other sensor group cross correlating
- Cross correlation of a sonar sensor and a PIR array in addition to an active adjacent PIR array, an active microwave sensor, or a correlating video or acoustic sensor
- Cross correlation of a PIR sensor and a microwave sensor along with an active adjacent PIR array; three other active microwave sensors; or a correlating video, acoustic, sonar, or PIR sensor
- Activation of the VMD and cross correlation with an acoustic sensor, sonar sensor, or PIR sensor; motion detected by a microwave sensor at the same angle; or motion detected by two microwave sensors at different angles
- An active acoustic sensor array along with cross correlation with video or PIR sensors; cross correlation with a microwave sensor and a sonar sensor; or motion detected by three microwave sensors, one of which is at the same angle as the active acoustic sensor

Although these are not the only situations that cause an alarm, they are the most common.

## CONCLUSION

The real-time security assessment algorithm discussed in this article was tested by an independent evaluation team. The team performed a series of feasibility tests on the individual sensor suites and the security assessment algorithm.

After testing security assessment capabilities, the team found that the algorithm fused, interpreted, and assessed information from various types of sensors and successfully detected the intruder in all trials [1]. During the same time period, no nuisance alarms were recorded.

Furthermore, the results of the algorithm were compared with a system that neither correlated information obtained from different types of sensors nor correlated current information with past information. The comparison showed that the algorithm described in this article significantly improved the ability of the system to differentiate between real and nuisance alarms.

Since the completion of the feasibility tests, researchers have begun to convert the algorithm from the C programming language to Ada, which will make the program easier to maintain. In addition, the quantities and types of sensors in the system are also being modified.

The new system will consist of 32 PIR sensors and eight microwave sensors. The ultrasonic ranging modules are being upgraded to interpret multiple echos from a single chirp, which will greatly enhance the reliability of the range information in instances where an intruder walks behind a pillar or when multiple intruders are present in the same sensor zone. Finally, the acoustic sensor array is being eliminated. Although these sensors performed adequately during the tests, the testing team decided that there were too many sources of noise in a secured environment capable of causing the acoustic sensors to be in an alarm condition (e.g., heating/air conditioning units switching on and off or telephones ringing).

Because the omnidirectional effect experienced with microwave sensors falls off as the size of the room being monitored increases, the algorithm will be modified to incorporate a reflectivity factor representative of the size of the room based on the sonar template. For example, the average value of all sonar ranges within a zone will predict the influence of reflected energy on a microwave sensor. If the system is operating in an open area, the microwaves will be modeled as directional, but if the system is operating in a congested area, across-the-board influence will be expected.

Today, a number of these robots are used in the Mobile Detection Assessment Response System (MDARS). This program seeks to provide automated inventory management and security assessment in warehouses and storage sites of the Department of Defense.

## REFERENCES


1. R.C. Koerner. Nov 1991. "Formal Report—Technical Feasibility Test (TFT) of Mobile Detection Assessment Response System (MDARS)," *USACSTA-7160*, U.S. Army Combat Systems Test Activity.
2. H.R. Everett et al. Aug 1990. "Modeling the Environment of a Mobile Security Robot," *NOSC Technical Document 1835*, Naval Ocean Systems Center, San Diego, CA.
3. Richard P. Smurlo and Robin T. Laird. 1991. "A Modular Robotic Architecture," Mobile Robots V conf., *SPIE 1388*. Chun and Wolfe, eds: 566-577.
4. H.R. Everett. July 1985. "A Multi-Element Ultrasonic Ranging Array," *Robotics Age*.



**Richard P. Smurlo** is Project Engineer and **H.R. Everett** is MDARS Technical Director, Naval Command Control and Ocean Surveillance Center, San Diego, CA 92152-5000; 619-553-3668, fax 619-553-6188.


## Reader Feedback

To rate this article, circle the appropriate number on the Reader Service Card.

| 3 | 13 | 23 |
|---|---|---|
| Excellent | Good | Fair |