THE AUTHENTICATED TRACKING AND MONITORING SYSTEM (ATMS) CONCEPT

J. L. Schoeneman
On-site Monitoring Technology Department
Sandia National Laboratories
Albuquerque, New Mexico 87185-5800

Abstract

The Authenticated Tracking and Monitoring System (ATMS) has been designed to address the need for global monitoring of the status and location of proliferation-sensitive items. Conceived to utilize the proposed Global Verification and Location System (GVLS) satellite link, ATMS could use the existing International Maritime Satellite commercial communication system until GVLS is operational. The ATMS concept uses sensor packs to monitor items and environmental conditions, collects a variety of event data through a sensor processing unit, and transmits the data to a satellite, which then sends data to ground stations. Authentication and encryption algorithms will be used to secure the data. A typical ATMS application would be to track and monitor the safety and security of a number of items in transit along a scheduled shipping route. This paper also discusses a possible proof-of-concept system demonstration.

1. Introduction

Global monitoring of the movement and condition of Proliferation-Sensitive Items (PSIs) poses a significant challenge. A highly effective information system is needed for nonproliferation and nuclear weapon dismantlement monitoring activities. The Authenticated Tracking and Monitoring System[1] (ATMS) has been conceived to address the challenge, and would monitor, in a secure and authenticated fashion, the status and position of proliferation-sensitive items while in transit anywhere in the world. The resulting tracking, timing, and status information could then be processed and utilized to ensure compliance with, for example, various treaties. Selected items to be monitored could include Treaty Limited Items (TLIs) such as nuclear weapon systems, Re-entry Vehicles (RVs), weapon delivery and launch systems, chemical and biological agents, Special Nuclear Material (SNM), and related nuclear weapons manufacturing equipment. The ATMS has potential applications in the areas of arms control, disarmament and nonproliferation treaty verification, and military asset control, as well as International Atomic Energy Agency (IAEA) and Euratom safeguards monitoring activities. The concept focuses on a monitoring technology for PSIs. However, the system's potential applications are numerous and broad in scope, and could be applied to other types of monitoring activities as well. The global concept of the ATMS is shown in Figures 1 and 2.

For ATMS to function globally, a world-wide satellite communication system is a prerequisite. The satellite link chosen for ATMS is called the Global Verification and Location System (GVLS) which is currently under consideration for full scale development at Sandia National Laboratories, and would be available in the late 1990s. The time frame for the GVLS deployment is driven by the availability of the multi-mission GVLS, which in turn is dependent upon the launch schedules of the Global Positioning System (GPS) Block IIR satellites that are required to implement the GVLS system. In the meantime, however, there exist the necessary elements, components, communication links, and sensor systems, which, if properly integrated with the existing commercial International Maritime Satellite (INMARSAT) communication system, could provide a proof-of-concept demonstration of a near-term capability for monitoring PSIs either during shipment, at deployed sites, or in storage. The proof-of-concept demonstration could then be followed by an interim, fully operational ATMS based upon the INMARSAT satellite communication system. This interim system could be utilized during the long-term development of the GVLS ATMS system, which will provide expanded and enhanced ATMS capabilities.

The purpose of this paper is twofold: first, to describe the proposed near-term INMARSAT ATMS (which will function nearly identical to the proposed GVLS ATMS) to independently monitor the status and location of PSIs, and second, to discuss a possible proof-of-concept system demonstration in August 1993.

1 This project is sponsored by the Department of Energy Office of Intelligence and National Security under contract number DE-AC04-76DP00789.

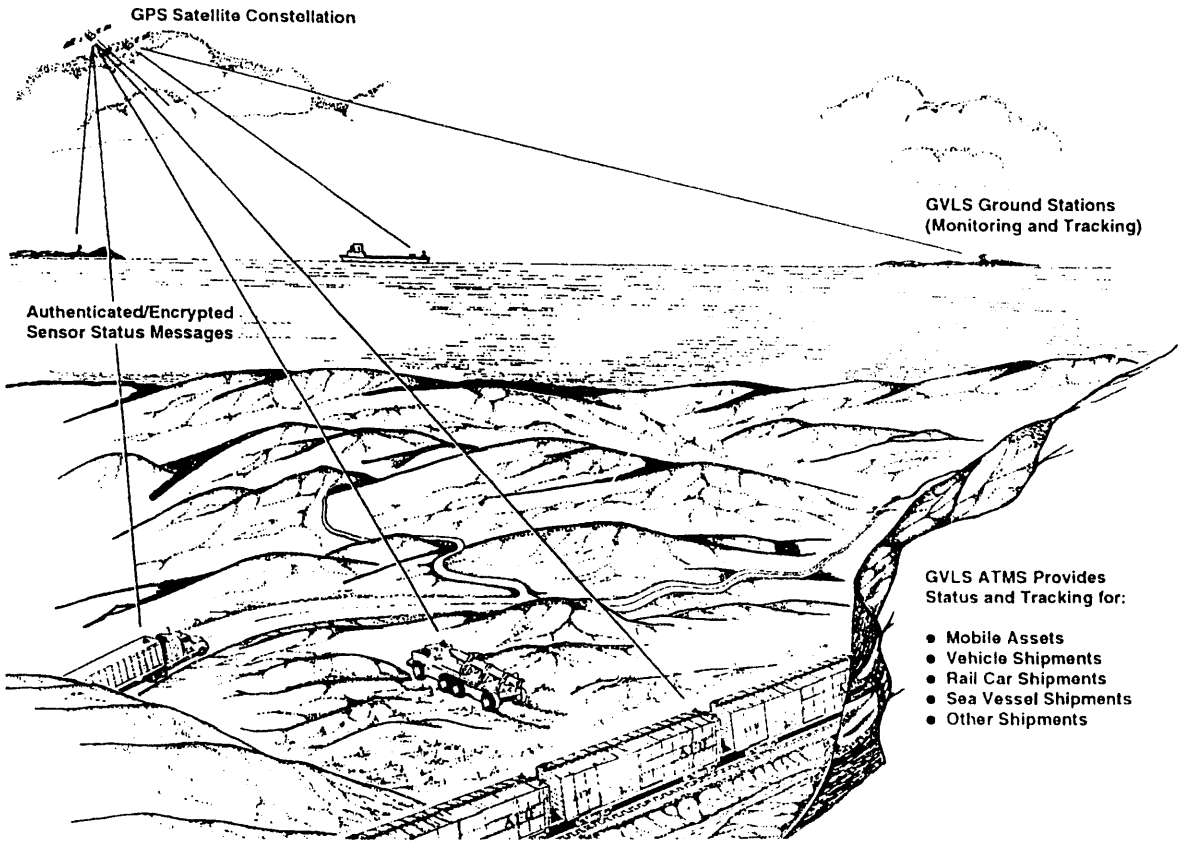

Figure 1. ATMS Global Concept

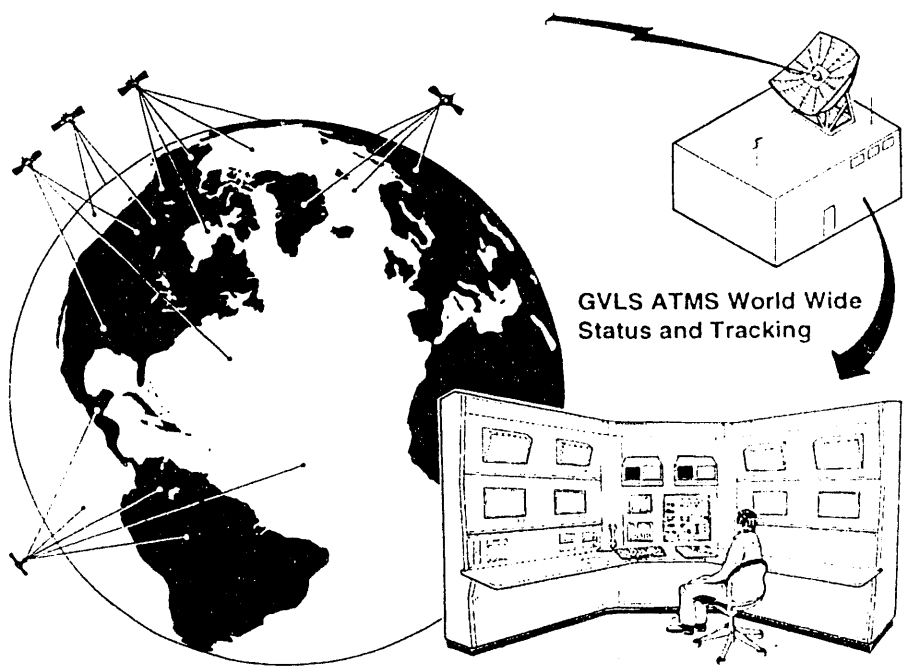

Figure 2. Satellite Linkup to Ground Station

2. ATMS Concept Overview

Figure 3 depicts a block diagram of the ATMS concept, and includes its major subsystem elements. These elements include the on-board sensor packs (which provide the capability to monitor the selected items), a sensor processing unit (SPU), a satellite transmitter/GPS receiver combination (transceiver) for communication with the INMARSAT satellites (and GPS satellites, as will be discussed later), and the ground station processing systems required to monitor the information provided by the sensors.

In the ATMS concept, the selected item's status and current global location are periodically transferred to an "on-board" INMARSAT transceiver and antenna combination for transmission to an appropriately located INMARSAT satellite in the field of view above. The status of the selected items will be monitored by a suite of sensors that could include: containment sensors (such as active fiber-optic seals); environmental and safety sensors (such as smoke and fire detectors); and intrusion detection sensors (such as microwave and infra-red detectors). The global position of the shipment, deployment site, or storage bunker is locally determined within the INMARSAT transceiver by utilizing signals from the currently existing GPS constellation. (The GPS receiver and the INMARSAT transmitter are common to the transceiver and share a common antenna.) The position and sensor status information is encrypted before transmission to the INMARSAT satellite. From the satellite, this secure data is then transferred to one of several available gateway ground station processing facilities located in the continental United States or several European cities, where the tracking and status information would be relayed in a secure form to another ground station for subsequent decryption and additional monitoring and display purposes.

A typical application of the ATMS could be to track and monitor the safety and security of a number of selected items in transit along a scheduled shipping route. ATMS potential applications could include tracking and status monitoring of selected items during sea vessel surface shipments, vehicular and rail ground shipments, and aircraft shipments. (See Figure 1.) The status and position of high-value military assets (e.g., mobile launch systems) could also be monitored and tracked in a real-time mode. Figures 4 and 5 show examples of secure rail car and sea vessel shipments, respectively.

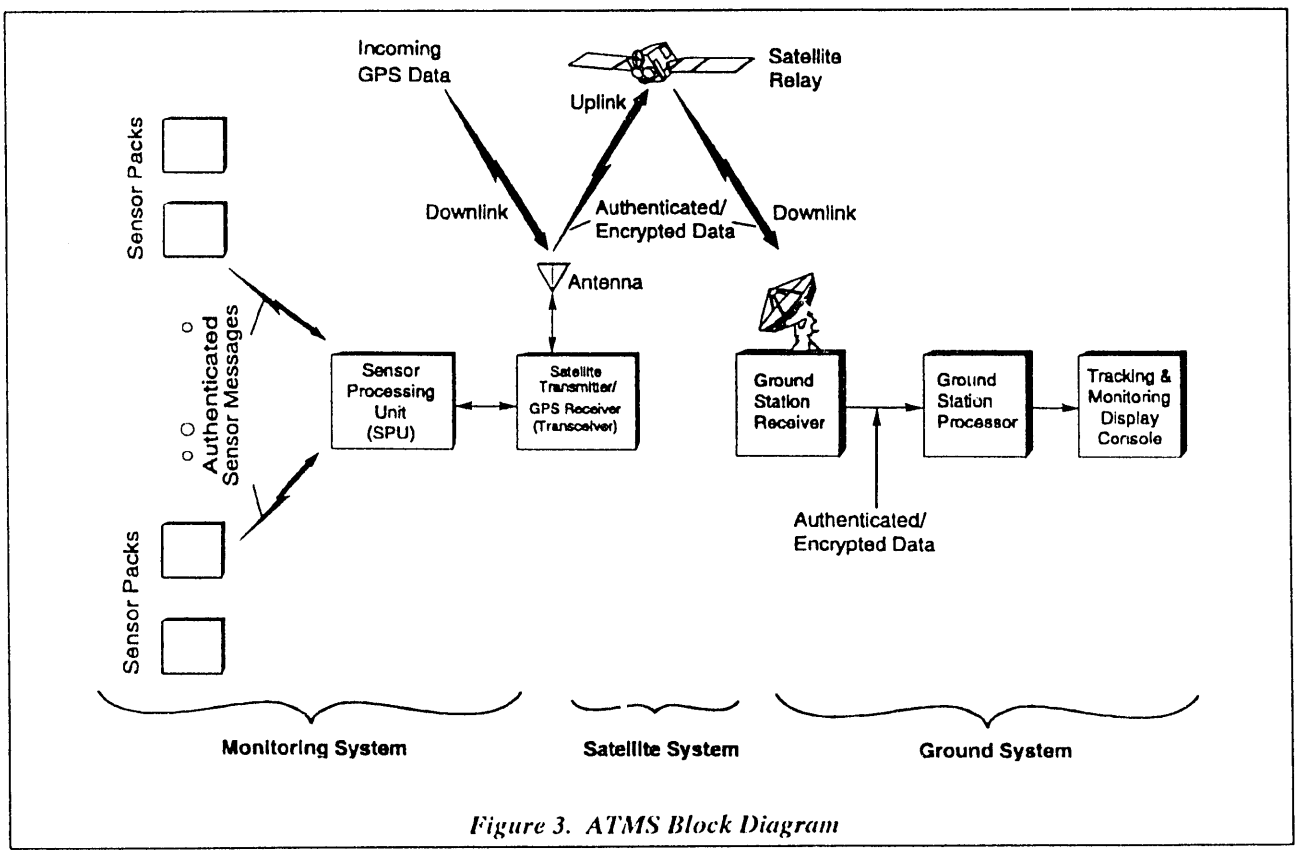

Figure 3. ATMS Block Diagram

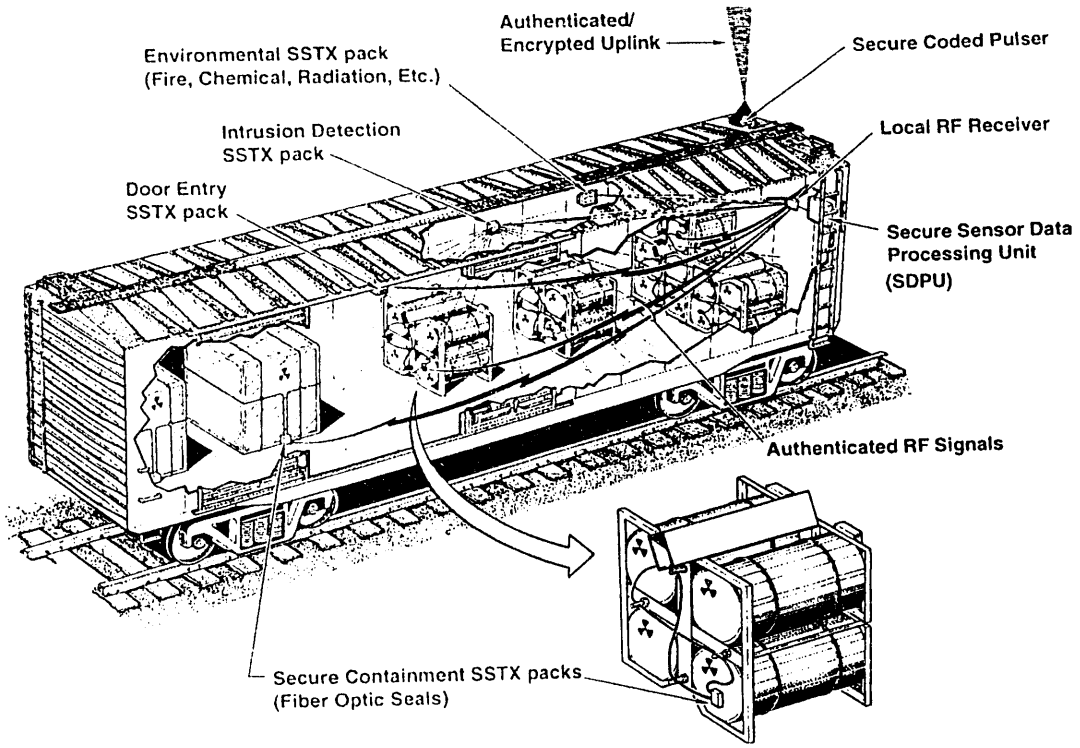

Figure 4. Rail Car Shipment Tracking and Monitoring Application

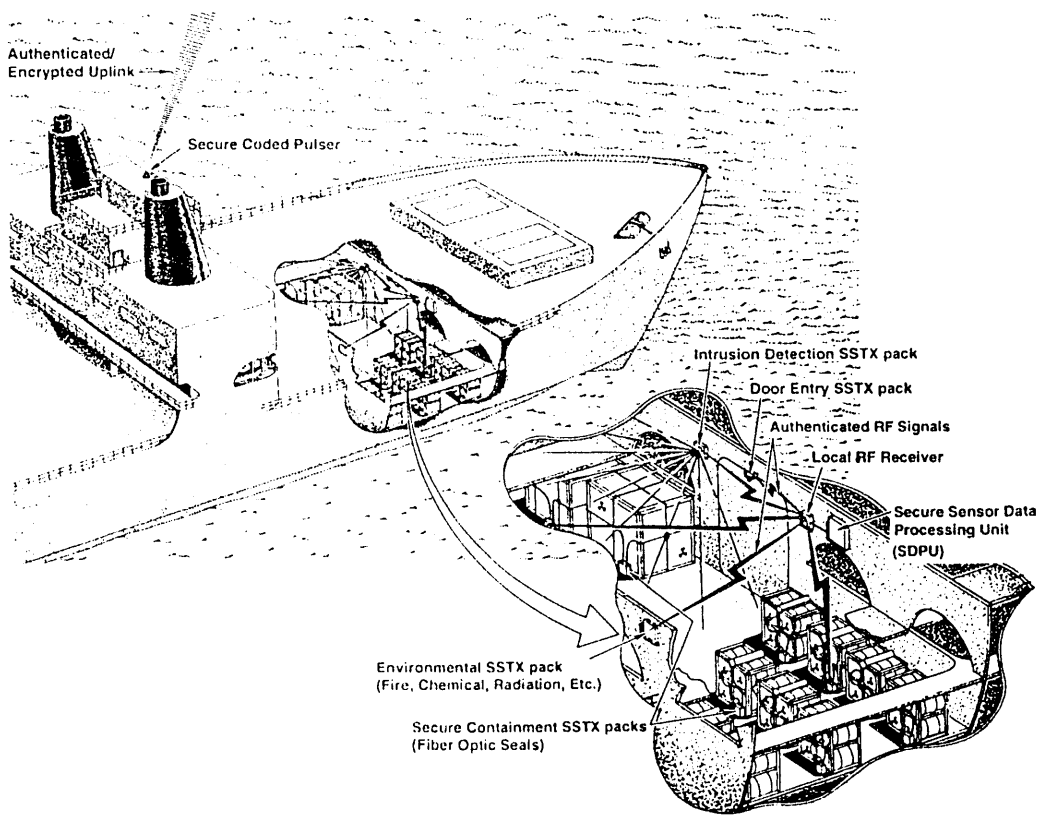

Figure 5. Sea Vessel Shipment Tracking and Monitoring Application

3. ATMS Subsystem Descriptions

Sensor Systems

The ATMS consists of a number of battery powered sensor packs that report (via a hardwired or wireless data link) significant sensor activations, known as "events", to the nearby sensor processing unit (SPU). In addition to event reporting, each sensor is required to send periodic messages that indicate the "state-of health" (SOH) of each sensor, and thus provides assurance that all sensors are on-line and have not been tampered with. The SPU processes and packetizes all incoming sensor pack messages and then sends this information to the INMARSAT transceiver for subsequent satellite transmission. When a significant sensor event occurs, the appropriate message will be transferred to the transceiver for immediate transmission to the above INMARSAT satellite. Normal status messages, used for tracking purposes, will be transmitted only at prescribed and periodic report-in intervals (e.g., every 10 minutes).

The sensors available for monitoring the status of weapons and components include environmental/safety sensors, containment sensors, and intrusion detection sensors. A number of sensor systems are currently under development as a joint effort by Sandia; Inovonics, Inc. of Boulder, Colorado; and Centrol, Inc. of Portland, Oregon. This development activity, called the Authenticated Item Monitoring System (AIMS),[1] is being pursued under the DOE program to support international safeguards, particularly technology to enhance the safeguards provided by the IAEA. Elements of AIMS will soon undergo field evaluation by the Euratom Safeguards Directorate. Current wireless sensor packs are: fiber-optic seal, motion sensor, duress pendant, glass-break detector, smoke detector, and passive infra-red detector.

Environmental and safety sensors will be used to detect and report conditions surrounding the selected items that vary outside acceptable limits (e.g., temperature trip points). Examples of environmental sensors include: smoke detectors, temperature detectors, humidity detectors, flame detectors, radiation detectors, and chemical detectors. Containment sensors are utilized to monitor the physical emplacement of selected items and thereby verify that they have not been moved or tampered with. As an example, active fiber-optic seals could be routed through weapon turnbuckle tie-downs in such a way that it is extremely difficult to move or remove the selected item without breaching the fiber optic loop, thereby causing an event. Examples of containment sensors include: motion sensors, active fiber-optic seals, and load cells/links. Intrusion detection sensors are utilized to monitor the physical presence and movement of an individual in the area of the selected items, or any attempt to obtain entry into the area containing the items. Examples of intrusion detection sensors include: microwave detectors, infrared detectors, balanced magnetic switches, and wire grid detectors. In addition, the sensor pack packs can monitor a variety of other sensor types by simply incorporating different sensor heads.

Sensor activations indicate that a significant anomaly or event has occurred. If a sensor is activated, the sensor pack immediately transmits a burst of authenticated messages to the SPU, where that event message is time-tagged and checked for authenticity. This is referred to as a **Sensor Event**. Once the SPU receives a message indicating that a sensor event has occurred from an authentic, on-line sensor pack, it packetizes this information, re-authenticates the newly created packet, and then passes it on to the transceiver for immediate satellite transmission.

In addition to monitoring a selectable sensor input, each sensor pack contains a detector that is designed to detect and report attempts to tamper with, or covertly breach, the sensor pack enclosure. This is referred to as a **Tamper Event**.

As an additional security feature, each sensor pack is required to periodically transmit local authenticated SOH messages to the SPU. This feature provides assurance that all sensor pack packs are operational, and have not been tampered with. (SOH message intervals are user-selectable.) If SOH messages are not received from an on-line sensor pack, the local time and date of the last transmission received, along with the number of missing SOH messages, is processed within the SPU, and then transferred to the transceiver. This type of incident is referred to as a **Missing SOH Event**. The last event type involves the authentication process. Any sensor pack message received by the SPU that fails the authentication process is also time-tagged and processed as a **Failed Authentication Event**.

In summary, the activation of sensor inputs, sensor pack tampering, missing SOH messages, or messages that are not properly authenticated, comprise events that will be time-tagged by the SPU and immediately transferred to the transceiver for satellite transmission and subsequent ground station reception and display.

Sensor Processing Unit (SPU)

The sensor processing unit (SPU) is responsible for processing all incoming sensor messages, packetizing and encrypting the messages, and then sending the information to the transceiver for satellite

transmission. The transceiver provides the information up-link to the satellite on a normal report-in (RI) basis (a prescribed interval, e.g., every 10 minutes), unless an event has occurred, which is transmitted immediately.

The SPU is also used in conjunction with a standard personal computer (PC) for initially programming each sensor pack and maintaining the receiver group data base. The group data base includes the pertinent parameters as to the current configuration of sensor packs within the group, and is automatically updated when and if changes are made. These parameters include: the number and type of sensor packs in its group; the individual sensor pack identification numbers along with their SOH message intervals; and each unique authentication keyword for all sensor packs within the group.

For unattended monitoring applications, the SPU and transceiver will be secured and provided with the necessary tamper-indicating measures, just as the sensor packs are. The cables and associated connections from the SPU to the transceiver do not require physical tamper protection since the message packets transferred over this link are in an encrypted form. Severing this cable would result in the total loss of all incoming ground station transmissions, including the periodically expected status RI messages used for tracking. Loss of these anticipated status messages is significant and would be noted during ground station processing as either a system compromise or total loss of the ATMS operational capability.

Authentication Overview

The definition of authentication from the IAEA reads as follows: "Authentication is the process of assuring that genuine information is obtained for safeguards purposes using equipment for which the Inspectorate (e.g., the IAEA) lacks sufficient control or knowledge." For the ATMS, authentication provides a method of determining, with a very high degree of confidence, that an SPU-received message was indeed sent from the proper sensor pack within the assigned group. For applications where tamper resistance is important, data authentication is required.

During sensor pack programming, the SPU generates a 48-byte unique random authentication key that is to be shared with that sensor pack, and only that sensor pack. Before a sensor pack transmits a message to the SPU (either an SOH or an event), the keyword, along with the sensor pack's identification number, current and past sensor status, and various message counters, are used in a special algorithm[2] to generate an authentication tag. This authentication tag is then appended to the overall "in-the-clear" message packet and transmitted to the SPU.

Once received and held in the SPU's memory, the processing software, using the same data and the same authentication key (unique for each sensor pack), performs the identical authentication algorithm to determine if the received authentication tag is correct. If so, the message will be deemed authentic, can be further processed and, if necessary, transferred to the transceiver for satellite transmission.

INMARSAT Transceiver and Antenna Combination

The INMARSAT transceiver provides two important functions in the ATMS. First, utilizing the overhead GPS satellite constellation, the transceiver contains an internal GPS receiver that periodically calculates its current latitude and longitude (lat-long) position information, accurate to within approximately 50 meters (300 feet) worldwide. Second, the transceiver and antenna combination provide the necessary communication link from the SPU to the selected INMARSAT satellite. The secure (e.g., encrypted) data transmitted from the transceiver include the packetized sensor status along with the lat-long position information. The INMARSAT system was chosen over other competing satellite communication systems due to its continuous world-wide coverage and availability.

System Power

The SPU, INMARSAT transceiver and antenna combination have the ability to be powered by universal AC power (with a wide range of voltages and frequencies for world-wide operation), by appropriate battery power systems, or by a combination of solar-generated electricity with a battery back-up provision. The sensor packs have internal battery power for up to two years of unattended operation.

INMARSAT Satellite Constellation and Coverage

The INMARSAT constellation consists of four satellites that are either operational or planned and provide the necessary worldwide communication coverage. Basically, the satellite constellation provides a conduit to relay the incoming messages from the ground-based transceiver to the appropriate end user ground stations for further processing and display.

Ground Stations and Communication Links

The end-user ground station collects and processes the incoming satellite messages and displays the current sensor status along with providing a graphical display of the past and present position of the shipment (in a

tracing manner) on an appropriate map-type display. Figure 6 illustrates the tracking and status monitoring capability of a currently available, off-the-shelf, PC-based display system. This real example shows the tracking of a vehicle from Albuquerque, NM to Raleigh, NC, USA. (The name Ellis represents the operator of the software.)

Shipment tracking resolution is dependent upon the periodic report-in interval and the computational accuracy of the GPS receiver. The selection of the report-in interval is dependent on the application and the tracking requirements, and is anticipated to be between 5 minutes and 1 hour. Assuming a 5-minute report-in interval and a trans-shipment velocity of 50 km/h, shipments could be tracked (between report-in intervals) to within a certainty of 4.2 kilometers, which should prove quite adequate for most tracking purposes. However, during report-in (RI) refresh periods, the absolute position is recalculated and updated via the GPS receiver, with an anticipated accuracy of approximately 50 meters.

When the GVLS ATMS is fully developed, it is envisioned that the inspector interface with the ground station monitoring equipment will be interactive, user friendly, and will have the capability to be fully automatic and unattended. In the unattended mode, an alert signal to the operator or inspector will be generated only if the ATMS detects that the system or sensor status has changed, or if the shipment transit path has deviated by a preset distance from the declared routing. Furthermore, an inspector could use the station to observe the actual tracking of selected item(s) during transit in a near-real-time mode (e.g. on the order of a few minutes delay). The display would depict the past and present positions of the shipment platform on an appropriate map-type display along with displaying the current ATMS sensor suite status. The display will also depict the desired route and timing information (e.g., where the shipment or movements should be at any particular point in time), overlayed with the actual route taken along with its current position. The inspector will also be provided the capability to query the system at any time to acquire the current system and sensor status.

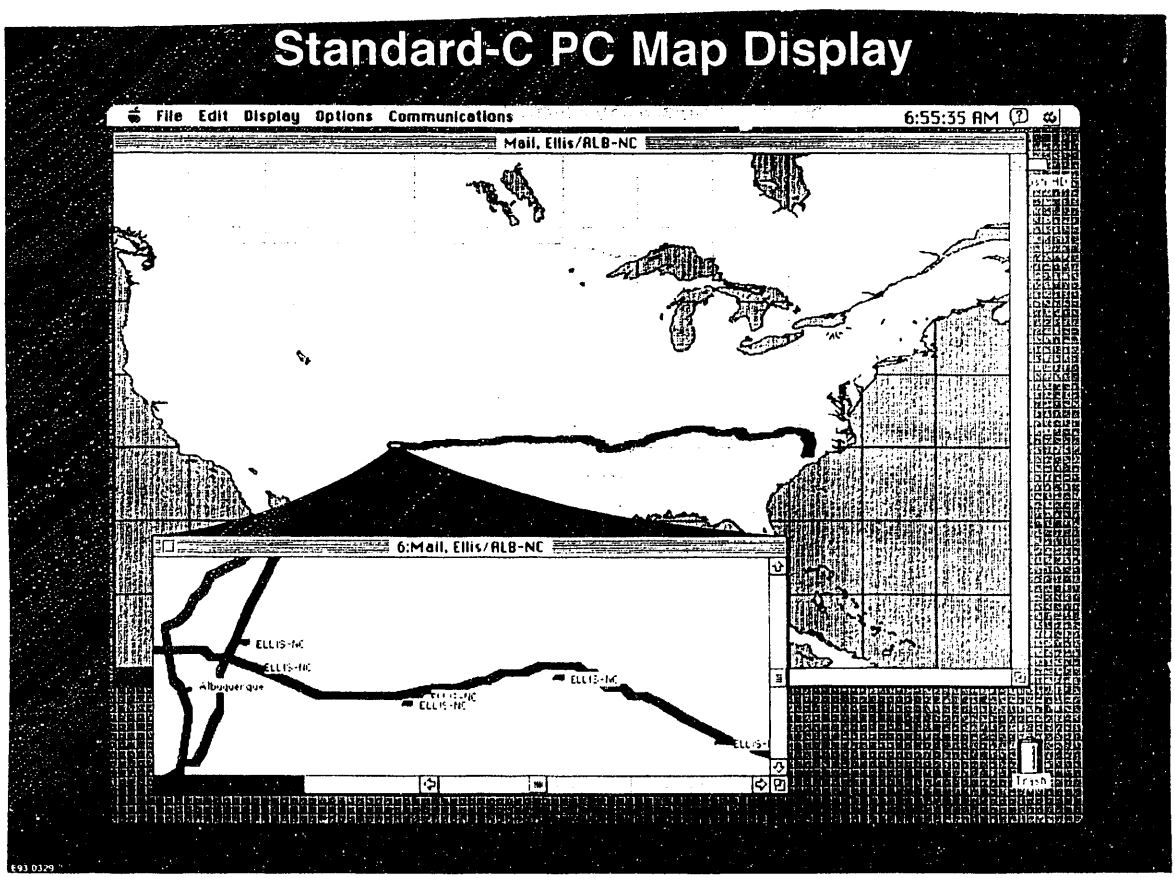

Figure 6. ATMS Tracking and Monitoring Facility

4. INMARSAT ATMS Demonstration System

The essential elements of the proposed INMARSAT ATMS system should be available for demonstration in August 1993. A demonstration will be conducted of a monitored storage bunker at a site in the Albuquerque area, a monitored transportainer suitable for tracking, and an "end-user" ground station display at Sandia, the State Department, or DOE Headquarters.

1) Monitor mock-up weapons and component containers in a secure weapons bunker at Sandia

For the storage bunker, a number of mock-up weapon components would be monitored in a static and unattended mode. Sensors that will be utilized in this demonstration include containment sensors in the form of movement or motion detectors along with active fiber optic seals used to seal mock weapon component containers. An appropriate suite of environmental/safety sensors and intrusion detecting sensors will also be demonstrated.

2) Monitor mock-up weapon containers in a transportainer

For this element of the demonstration, a shipment of mock weapon components will be monitored and tracked at a global level from Albuquerque to any desired location covered by the footprint of the INMARSAT satellite which communicates with the Southbury, CN ground station. The exact travel route will be identified at a later time.

5. Summary

When fully developed and deployed, the Authenticated Tracking and Monitoring System (ATMS) will provide a world-wide capability to track and monitor virtually any type of selected high-value item. The system described within this document incorporates sensors, electronics, and tamper-resistant technologies, including authenticated messages and robust tamper-indicating enclosures. The system is mobile, battery powered, and will survive environmental conditions commensurate with its anticipated usage throughout the world. The applications described here are somewhat limited in scope to tracking and monitoring proliferation-sensitive items. However, the ATMS has a very broad spectrum of potential future applications. A proof-of-concept demonstration of the ATMS's potential is tentatively scheduled to occur in August 1993.

References

1. J.L. Schoeneman, M.J. Baumann, L.J. Fox, C.D. Jenkins, A.W. Perlinski, "Universal Authenticated Item Monitoring System - Second Generation Equipment," *Proceedings of the 32nd INMM Annual Meeting*, Orlando Florida, 1992.
2. L.J. Fox, J. Davis, C.D. Jenkins, J.L. Schoeneman, "Authentication Algorithm for the Universal Authenticated Item Monitoring System (AIMS)," *Proceedings of the 32nd INMM Annual Meeting*, Orlando Florida, 1992.

END

DATE
FILMED
10/7/93