Advanced User Interface Design and Advanced Internetting for Tactical Security Systems

S.A. Murray, D.W. Gage, J.P. Bott, D.W. Murphy, W.D Bryan,
S.W. Martin, and H. G. Nguyen

Space and Naval Warfare Systems Center, San Diego
San Diego, California 92152

Abstract

In recent years, military security forces have operated in a climate of increasing mission complexity and diversity. As a response to such challenges, the US Army Training and Doctrine Command (TRADOC) approved a concept for a Family of Integrated Tactical Security Systems (FITSS) involving integrated security sensor systems to support future operations. In support of this concept the Defense Special Weapons Agency (DSWA), at the request of the US Army Product Manager – Physical Security Equipment, initiated two exploratory development projects at SPAWAR Systems Center, San Diego to develop an Advanced User Interface for Tactical Security (AITS) and a Tactical Sensor Internetting and Integration (TS^2I^2) capability. These projects are complementary in approach and application. AITS addresses the human factors and display technologies needed to effectively support tactical security personnel with sensor information in a clear, intuitive manner while TS^2I^2 is focused on a protocol architecture to support control of multiple tactical sensors using current communications resources. The concepts behind these projects, and their current progress, are described in this paper.

Background

Military security operations in recent years have shown a trend toward increased mission complexity and diversity, a trend that is exacerbated by budget and manpower constraints. Both operational and acquisition agencies are looking to technology solutions to aid security forces in accomplishing their missions, and distributed sensor systems are being designed that afford wide area surveillance coverage to small numbers of security personnel, augmenting their patrolling duties with enhanced situational awareness.

In December 1996 the US Army Training and Doctrine Command approved the US Army Military Police School Concept Statement for a Family of Integrated Tactical Security Systems (FITSS) [1]. This concept statement addressed requirements for a system of robust, man-portable sensors with detection and assessment capabilities to support future operations. The system was to be easy to employ and interoperable with joint forces. FITSS is an "open architecture" system and stresses maximum use of current commercial-off-the-shelf (COTS) and government-of-the-shelf (GOTS) components but provides for insertion of new technological capabilities as they become available, with minimal interface or communications redesign.

Many sensor systems, such as the Remotely Monitored Battlefield Sensor System (REMBASS), Improved Remotely Monitored Battlefield Sensor System (IREMBASS), Tactical Remote Surveillance System (TRSS), and the Platoon Early Warning System (PEWS) have been developed to help ground forces monitor perimeters or collect intelligence information. Each, however, has been designed for a specific application or user community. These systems share a common communications protocol (SEIWG-05) for transmitting data over point-to-point radio links, but are otherwise based on proprietary hardware and software and are not interoperable. Such architectures do not support easy expansion with new sensors, displays, or alternate communication links. The operator interfaces for these systems also require significant operator involvement for interpreting alarms. Alerts from REMBASS and TRSS sensors, for example, are displayed to the operator alphanumerically, i.e., with the identification number of the

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 1998	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Advanced User Interface Design and Advanced Internetting for Tactical Security Systems	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
S. A. /Murray; D. W. /Gage; J. P. /Bott; D. W. /Murphy; W. D. /Bryan; S. W. /Martin; H. G. /Nguyen	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Space and Naval Warfare Systems Center San Diego, CA 92152	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**6**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

transmitting sensor. The operator must then correlate these data to sensor locations plotted on a paper map. and mentally fuse them with any other related information prior to determining an appropriate situation response.

The FITSS concept is intended to correct current deficiencies and address future operational needs by focusing on interoperable sensors and information integration at the operator interface. To realize this concept, the US Army Product Manager – Physical Security Equipment has requested that the Defense Special Weapons Agency (DSWA) initiate two complementary, exploratory development projects: 1) Advanced User Interface for Tactical Security (AITS) and 2) Tactical Security Sensor Internetting and Integration (TS^2I^2). DSWA subsequently tasked SPAWAR Systems Center, San Diego (SSC-SD, a Navy laboratory) to execute these projects, based on extensive laboratory experience in communications architectures, distributed sensors, and human machine interfaces [2, 3, 4, 5, 6]. The AITS project is developing an operator interface to provide integrated and tactically relevant information from multiple types of sensors in a clear and intuitive manner. The interface controls and displays will allow the operator to receive and interpret alert signals and to control sensors without hampering mobility in the field. TS^2I^2 is developing a communication and interface architecture for distributed sensor systems to interface multiple sensors of varying types (e.g., seismic, acoustic, thermal, etc.) and to support their operation with available tactical communications systems.

The AITS Project

The objective of the AITS project is to increase the effectiveness of tactical security forces by improving the operator interface for situational awareness and ease of use in integrating new, and different sensor systems. A considerable range of sensor types must be supported in present field operations and technological improvements will expand this number in the future. Tactical security personnel must transport, deploy, and operate such equipment with minimal outside support. AITS can reduce these challenges with a portable interface designed to present an integrated tactical picture to the operator under mobile, hands-free conditions. A modular design approach provides a common set of information to the operator regardless of the number or type of sensors employed. This “plug and play” scheme is therefore user-focused rather than equipment-focused, and reduces operator task loading through improved human-computer interaction. The AITS project will develop a proof of concept interface system, and validate its design concepts with a progressive set of user evaluations and operational tests.

Approach

The AITS project is being conducted in two sequential phases: 1) information gathering, analysis, and baseline system definition, and 2) prototype construction, engineering validation, and systematic user testing. The entire development approach is structured around user involvement and input. User requirements were derived through visits to user facilities, on site interviews and observation of training exercises, and all concept development has been grounded on these identified user needs [7]. Appropriate technologies and human factors methods have been brought to bear as required to satisfy the requirements.

Information Requirements

Security personnel of the US Army (military police units), US Marine Corps, , Sensor Control and Management Platoons (SCAMP), and regular combat troops from both services were followed through a variety of field training exercises. The primary missions observed included route and area security, force protection, law and order, battlefield circulation control, amphibious assault support, and Military Operations in Urban Terrain (MOUT). Regardless of the unit or branch of service, the equipment suites for these missions were highly similar and included seismic/acoustic, optical break beam, passive infrared (IR), and magnetic sensors.

In general, the security task is continuous, active, and manual. Although auditory warnings are sometimes used to alert personnel about security breaches, the primary method for detecting intrusions is direct, continuous monitoring of displays by system operators. These operators expressed an overall consensus about essential interface support for the security job that included:

- Target location: Where are they? This information included the locations of the alerting sensors that activated in response to the targets. Some automated means for visually correlating target information to the location of the transmitting sensor is desired; current methods using paper maps are time-consuming and prone to errors.
- Assessment capability: What are they? This is a deficiency of current sensor systems. Knowing the type and number of targets greatly assists decisions about deploying scarce security personnel.
- Relative target locations: Where are they with respect to the operator? This leads to an operator-centered approach to the display design.
- Support information: This includes other friendly personnel command elements, terrain data, roads, waterways, etc. This type of information is useful for planning the best response to sensor alerts
- Geographic information: Specifically, perspective views of terrain topography that help the operator to better understand the location information
- Communication support: Good communications with other member of their units or with appropriate command echelons are pivotal to successful operations. While not technically a component of the AITS system, display support for the communication function can and should be integrated into the design
- Raw sensor information: Users requested a display of raw sensor information as a means of confirming processed information.

Interface Analysis

Examination of relevant human factors and display design principles centered on the key decisions required of security forces when responding to alerts. The technology review of system components focused on the practical implications of their working environment (i.e., in the field and typically on the move). Although the complete results of this analysis are beyond the scope of this report, the specifications of display features included:

- monoscopic data presentation (i.e., stereoscopic information was not required)
- color capability for grouping of certain data classes (e.g., headings, target classification, etc.)
- graphically-based icons for sensor and target classification
- both visual and auditory directional (azimuth) alerting signals, to orient the user to target location
- alphanumeric presentation of data needed in generating reports (e.g., range and bearing)
- a combination of automatic and operator-selectable data presentation formats.

Baseline System Design

SSC-SD efforts in display design and technology analyses were augmented by a support contract with the Human Interface Technology (HIT) Laboratory at the University of Washington. The HIT Laboratory is an international leader in the generation of innovative control and display concepts and maintains a current awareness of emerging technologies through its visiting scientist programs. In collaboration with the HIT Laboratory, SSC-SD defined a baseline AITS system concept design that includes:

- A see-through monocular HMD display; this approach will permit the soldier to see the entire working environment with minimal obstruction to vision. All information will be confined to the soldier's field-of-regard (i.e., in the region where he or she is looking). A small, hand-held display is included as a backup device.
- A control system based primarily on voice recognition. A wrist-worn keyboard and clothing-worn mouse are included as backup tools.

- An integrated architecture for voice and imagery communication and features for database access. This capability will benefit greatly from the products of the TS^2I^2 project.

In operation sensor alert generates a spatial auditory signal, via headphones, and a directional symbol on the display to orient the user to the azimuth of the intrusion. A small magnetic sensor integrated with the HMD provides sufficient directional information to register display symbology over the real world. When the user's field-of-regard is pointed correctly, visual icons are superimposed over both the target and the alerting sensor; each major class of target and each type of sensor is represented by a unique visual icon. Support information includes magnetic bearing and range to the target. Voice control is used to call up supporting displays such as map images, showing the user's position in relation to any or all alerts and sensors, or raw sensor information displays (e.g., video, sensor data). These additional displays can be located and stabilized anywhere in the user's total visual space, using voice or conventional input controls.

The approach described here supports all of the information needs identified during user interviews and field observations, and permits all security tasks to be performed while on-the-move. In addition, the basic technologies and display formats specified in this design are compatible with similar programs for information support to the dismounted soldier (e.g., the Army's Land Warrior program, SIPE).

The TS^2I^2 Project

The Tactical Security Sensor Internetting and Integration Project is focused on how to better exploit the surveillance potential of multiple remote sensors using internet communication protocols. This work has been based primarily on the Multipurpose Surveillance and Security Mission Platform (MSSMP), a distributed network of remote sensing packages and control stations, designed to provide a rapidly deployable, extended-range surveillance capability for a wide variety of military security operations and other tactical missions [8]. The baseline MSSMP sensor suite consists of a pan/tilt unit with video and FLIR cameras and laser rangefinder, and makes maximum use of commercial off-the-shelf (COTS) components. With an additional radio transceiver, however, MSSMP can also function as a gateway between existing security/surveillance sensor systems (such as TASS, TRSS, and IREMBASS, and IP-based networks), to support the timely distribution of threat detection and threat assessment information. The MSSMP architecture is, therefore, well positioned for integration with the IP-based tactical radio networks that will evolve in the next decade.

The DoD concept for joint services interoperability in the 21st Century, *C4I For The Warrior* [9], envisions a widely distributed user-driven infrastructure in which the warrior "plugs in" to obtain information from secure and seamlessly integrated Command Control Computer Communications and Intelligence (C4I) systems. Each branch of service has its own strategy for meeting this vision and IP protocol compliance has been designated as the glue between all of these strategies to obtain and maintain interoperability between the services. The *Army Digitization Master Plan (ADMP)*, the Army's roadmap for fulfilling its *Enterprise* strategy [10], further states that Army digital data communications will use Internet protocols such as Transmission Control Protocol/User Datagram Protocol (TCP/UDP) and Internet Protocol (IP) as their common thread.

TCP is the workhorse transport protocol of the Internet, so much so that the Internet protocol suite is usually referred to as "TCP/IP." Unfortunately, TCP is oriented to continuous data streams rather than discrete messages. Tactical military communications, however (i.e., low bandwidth, high error-rate links in an environment where RF links between mobile nodes dynamically come and go, and where adversaries may be trying to destroy our communications assets), are very different from the extremely high bandwidth, permanently-installed communications channels that support the Internet. TCP is thus poorly matched to the requirements of security sensors and other quasi-autonomous systems [5].

User Datagram Protocol (UDP) is a transport layer protocol that is much simpler than TCP, and allows user processes almost direct access to basic IP operations. UDP is also supported as part of all standard TCP/IP software packages. The TS^2I^2 project, therefore, is developing tools that build on top of UDP functionality. This project addresses some of the issues associated with using limited-performance IP networks to support

tactical security/surveillance sensor applications, i.e., to get the biggest "bang for the bit". Specific goals of the TS^2I^2 include:

- Transparent support for communications with both local and distant processors
- Tailoring to the design communications topology. If, for example, a processor sends a message to another processor, and the message is not acknowledged immediately, then we will want to retransmit the message as quickly as possible, and continue until it is received
- Adapting to the current communications topology. If another platform doesn't acknowledge *any* of the messages we send to it over a period of time, then our system should be able to make the inference that either the other node or the channel is down. That is, communications performance data must inform the behavior of the overall system and enable a more autonomous mode of operation, as necessary
- Prioritization of message transmission, including automatic handling of perishable data. A threat alarm/alert, for example, should have a higher priority than a routine status message, and a newer alarm may or may not be more important than an old one.

Transport Layer and Session Layer Tools

The TS^2I^2 Project is addressing functional tools for both the Transport and Session protocol layers of Internet communications. The first task is to develop a tightly written, efficient, and reliable *message-based* transport protocol layer for message buffering, numbering, timeouts and acknowledgements. We would, furthermore, like to include all the various performance improvement schemes being pursued as TCP options by the community of Internet protocol developers, such as selective acknowledgements.

A second task is to develop an enhanced Session Layer protocol. Operations within this layer are divided into the session connection establishment phase, data-transfer phase, and session connection release phase. The MSSMP system requires Session Layer mechanisms to cleanly support multiple sensor platforms and multiple control stations, to permit the orderly transfer of platform control from one station to another in a variety of circumstances, including:

- one operator requesting, and receiving, transfer of control of a platform from another operator currently controlling it
- an operator assuming control of a platform which has lost contact with its current operator
- an operator (e.g., higher echelon commander) invoking a higher priority in order to "steal" control of a platform from its current operator
- split control, in which one operator acquires control of one subsystem (e.g., for problem diagnosis and repair) while another operator controls the rest of the platform
- data sharing, in which multiple operators may have "read only" access to a platforms sensor data output, while just one operator has actual control.

These requirements are not unique to MSSMP, but apply to any system with dynamic client-server relationships and requirements for uniqueness of control.

Phase 2 Plans

The tasks reported here represent Phase 1 of both project efforts, which began in FY 98. Phase 2 will involve construction and user testing of the prototype AITS, using the MSSMP as a data source. In addition, some of the TS^2I^2 tools will be incorporated into the AITS prototype to evaluate the impact of these new capabilities on surveillance methods and command-level decision support. Phase 2 of the TS^2I^2 project will additionally focus on possible complications of Session Layer protocol design, such as:

- command interruption, which has implications for safety and system integrity; the concept of "emergency override" is one which must be further considered
- the concept of "delegation" of precedence, as tactical requirements shift
- assignment of operator precedence, as a systematic method for breaking “ties” between operators of equal precedence, each seeking control of a sensor resource.

Summary

The common goal of the AITS and TS^2I^2 projects is to provide enhanced access to information using concepts that are easily adaptable to any security sensor suite. This goal is achieved by involving the user community throughout the development cycle, and through developing general-purpose tools that function on top of existing protocols. The synergy of these two projects will be realized through more flexible control of tactical sensors and through improved situation awareness at all command levels of the security force.

Acknowledgements

This work has been performed under the Advanced Interface for Tactical Security (AITS) and the Tactical Security Sensor Internetting and Integration (TS^2I^2) Exploratory Development (6.2) projects, sponsored by the Defense Special Weapons Agency.

References

1. US Army Training and Doctrine Command (TRADOC) Pamphlet 525-74.
2. Bryan, W.D., Nguyen, H.G., and Gage, D.W. (1998). Man-Portable Networked Sensor System. SPIE Proceedings 3394: Sensor Technology for Soldier Systems, Orlando, FL, April 13.
3. Nguyen, H.G., Marsh, W.C., and Bryan, W.D. (1996).Virtual Systems: Aspects of the Air-Mobile Ground Security and Surveillance System Prototype. Unmanned Systems, (vol. 14, no. 1). Winter. **
4. Gage, D.W. (1997). Network Protocols for Mobile Robot Systems. SPIE Proceedings. 3210: Mobile Robots XII. Pittsburgh, PA, October 14- 17.
5. Gage, D.W., Bryan, W.D., and Nguyen, H.G. (1998). Internetting Tactical Security Sensor Systems. SPIE Vol. 3393: Digitization of the Battlespace, Orlando, FL, April 15-17. **
6. Martin, B.F. and Bryan, W.D. (1995). Low-Cost Miniature Interface and Control Systems for Smart Sensors, Tactical Radios, and Computer Networks. IEEE Military Communications Conference (MILCOM 95). San Diego, CA, Nov. 6-8. **
7. Murray, S.A. (in press). Advanced Interfaces for Tactical Security – Part 1 (SSC-SD Technical Report).
8. Multipurpose Security and Surveillance Mission Platform. http://www.spawar.navy.mil/robots/air/amgsss/mssmp.html
9. Command and Control Umbrella. http://www.ado.army.mil/smrtbook/sbpage8.htm
10. The Army Digitization Office. http://www.ado.army.mil

** Available on the Internet at URL http://marlin.spawar.navy.mil/D37, under “Publications.”