AFRL-HE-WP-TR-2004-0070

United States Air Force
Research Laboratory

FAST ACCESS SITUATION AWARENESS TOOLKIT (FASAT)

Jeffrey Fox
Jean Fox
Mitchell Song
Dave Gillen

MOBILEFOUNDATIONS, INC.
103 W. BROAD STREET, SUITE 600
FALLS CHURCH VA 22046

JANUARY 2004

FINAL REPORT FOR THE PERIOD NOVEMBER 2001 TO DECEMBER 2003

Human Effectiveness Directorate
Warfighter Interface Division
2255 H Street
Wright-Patterson AFB OH 45433-7022

NOTICES

When US Government drawings, specifications, or other data are used for any purpose other than a definitely related Government procurement operation, the Government thereby incurs no responsibility nor any obligation whatsoever, and the fact that the Government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data, is not to be regarded by implication or otherwise, as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

Please do not request copies of this report from the Air Force Research Laboratory. Additional copies may be purchased from:

National Technical Information Service
5285 Port Royal Road
Springfield, Virginia 22161

Federal Government agencies and their contractors registered with the Defense Technical Information Center should direct requests for copies of this report to:

Defense Technical Information Center
8725 John J. Kingman Road, Suite 0944
Ft. Belvoir, Virginia 22060-6218

DISCLAIMER

This Technical Report is published as received and has not been edited by the Air Force Research Laboratory, Human Effectiveness Directorate.

TECHNICAL REVIEW AND APPROVAL

AFRL-HE-WP-TR-2004-0070

This report has been reviewed by the Office of Public Affairs (PA) and is releasable to the National Technical Information Service (NTIS). At NTIS, it will be available to the general public.

This technical report has been reviewed and is approved for publication.

FOR THE COMMANDER

//Signed//

LEE D. SHIBLEY, Lt Col, USAF
Deputy Chief, Warfighter Interface Division
Air Force Research Laboratory

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MMM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From – To)
January 2004	Final Report	November 2001 – December 2003

4. TITLE AND SUBTITLE

Fast Access Situation Awareness Toolkit (FASAT)

5a. CONTRACT NUMBER
F33615-02-C-6003

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Jeffrey Fox
Jean Fox
Mitchell Song
Dave Gillen

5d. PROJECT NUMBER
3005

5e. TASK NUMBER
HC

5f. WORKUNIT NUMBER
21

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
mobileFOUNDATIONS, Inc.
103 W. Broad Street, Suite 600
Falls Church VA 22046

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory
Human Effectiveness Directorate
Crew System Interface Division
Air Force Materiel Command
Wright-Patterson AFB OH 45433-7022

10. SPONSOR / MONITOR'S ACRONYM
AFRL-HE-WP-TR-2004-0070

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The primary goal for Phase II was to develop a next-generation near-real-time satellite monitoring and alerting system. This system would enable the Air Force to move towards distributed space operations with enhanced anytime, anywhere situation awareness, with a particular focus on Space Situation Awareness (SSA). This goal was driven by the Air Force Space Command (AFSPC) Strategic Master Plan (SMP) FY04 and Beyond that lays out the Air Force's plan for achieving its Vision of "Global Vigilance, Reach, and Power." The SMP states that "we cannon fully 'exploit' that medium until we first 'control' it. The needed foundation, therefore, consists of the space access and infrastructure provided by the Space Support and Mission Support areas..." The SMP calls for robust and real-time (SSA) and "on-demand" operations, while at the same time calling for cost-effective and responsive solutions.

15. SUBJECT TERMS

Space Situation Awareness (SSA), Air Force Space Command (AFSPC), Strategic Master Plan (SMP), satellite monitoring, alerting system

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON:
a. REPORT	b. ABSTRACT	c. THIS PAGE			June J. Skelly
UNCLAS	UNCLAS	UNCLAS	UNLIMITED	91	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-8749

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

THIS PAGE INTENTIONALLY LEFT BLANK

Executive Summary

This report summarizes the work performed by mobileFOUNDATIONS, Inc. (mFI) under Contract No. F33615-02-C-6003, a Phase II SBIR funded by the US Air Force Research Laboratory's Human Effectiveness Directorate at Wright-Patterson AFB.

The primary goal for Phase II was to develop a next-generation near-real-time satellite monitoring and alerting system. This system would enable the Air Force to move towards distributed space operations with enhanced anytime, anywhere situation awareness, with a particular focus on Space Situation Awareness (SSA). This goal was driven by the *Air Force Space Command (AFSPC) Strategic Master Plan (SMP) FY04 and Beyond* that lays out the Air Force's plan for achieving its Vision of "Global Vigilance, Reach, and Power." The SMP states that "we cannot fully 'exploit' that medium until we first 'control' it. The needed foundation, therefore, consists of the space access and infrastructure provided by the Space Support and Mission Support areas..." The SMP calls for robust and real-time Space Situation Awareness (SSA) and "on-demand" operations, while at the same time calling for cost-effective and responsive solutions.

Under the Phase II SBIR, mFI developed FASAT (Fast Access Situation Awareness Toolkit). FASAT is a unique and powerful combination of tools that answers those challenges by enabling rapid, reliable, and cost effective on-demand, distributed operations. FASAT combines that general functionality with tools specifically targeted at dramatically improving spacecraft mission operations, such as:

- Automated report-generation for anomalous events
- Integrated incident management and workflow technologies to streamline operations
- An XML architecture that allows FASAT to accept data from ground systems via "plug-ins"
- Support for third-party collaboration tools
- Two-way wireless access to data via almost any device over any network

FASAT represents the state-of-the-art in monitoring and alert notification for aerospace systems. It delivers the *right data* to the *right people, anytime* and *anywhere*. The technologies developed by mFI under this Phase II SBIR enable FASAT to monitor data from ground systems for user-defined events of interest. It can then log those data and distribute (via alerts) that data to any commercial wireless data device. It then autonomously monitors responses to the alerts (from wireless devices) and performs any rollover or call-down functions necessary to build the appropriately staffed team of on-call personnel. FASAT's architecture allows for the seamless integration of COTS collaboration tools so that the on-demand team can collaborate electronically. All told, FASAT provides the foundation for enabling on-demand mission operations systems and distributed Space Situation Awareness. In addition, FASAT technologies can be adapted to more general command and control environments.

This report describes: the Air Force's needs for a FASAT-like tool, the functionality of FASAT, mFI's development process, how FASAT supports the Air Force's needs, and issues related to wireless security and their impact on FASAT.

TABLE OF CONTENTS

1.0 Introduction

1.1 Strategic Master Plan Goals

The *Air Force Space Command (AFSPC) Strategic Master Plan (SMP) for FY04 and Beyond* (Air Force Space Command, 2002) lays out the Air Force's plan for achieving its Vision of "Global Vigilance, Reach, and Power." The Vision calls for "Space warfighting forces providing continuous deterrence and prompt global engagement for America and its allies ... through the control and exploitation of space. Space warfighting forces are our people, weapon systems and other capabilities that operate and employ space power in, from and through space."

The SMP defines "Pillars of Space Capabilities," with Space Support and Mission Support as the foundations. The SMP states that "we cannot fully 'exploit' that medium until we first 'control' it. The needed foundation, therefore, consists of the space access and infrastructure provided by the Space Support and Mission Support areas..." The SMP calls for robust and real-time Space Situation Awareness (SSA) and "on-demand" operations, while at the same time calling for cost-effective and responsive solutions.

1.2 The Challenge

The US Air Force supports a wide variety of spacecraft that serve different functions (e.g., communications, early warning, weather, navigation). Each space operations squadron (SOPS) has some unique ground systems and procedures, but the majority of the operational activities are the same.

Today, the SOPS use dated hardware and software, placing an unnecessary burden on the operations personnel. The user interfaces on deployed systems are antiquated and provide few

job aids (Mejdal, McCauley, and Remington, 1999). Crewmembers often use paper and pencil for planning and anomaly resolution. A few examples help to illustrate the operator's environment:

- It is common to find operators monitoring large screens of dynamic telemetry looking for anomalous data. A typical satellite will have thousands of parameters that must be monitored. Even simple color-coding is not implemented at some SOPS.
- Crewmembers generally must type in commands via a command line. This activity is highly prone to error, so at least two crewmembers perform command entry: one to type, and one to watch for typos.
- To resolve anomalies, crewmembers must manually navigate through paper checklists to know what to do or whom to contact for assistance.
- All anomaly tracking is done manually, via hand entry into databases (that contain no workflow).
- When console crewmembers need assistance in resolving anomalies, they must physically find the appropriate personnel for support.

There are areas where the infusion of new and innovative technologies could greatly benefit the Air Force. These new technologies could also address the SMP calls for the SOPS to move towards "Total Space Situation Awareness," "Autonomy," and "On-Demand Operations." Most technologies now under evaluation focus on providing better tools for the on-console crewmembers, such as graphical user interfaces for command management and anomaly detection. These tools are the first step in reaching the Air Force's vision. The technologies described in this report can significantly further progress toward the Air Force's vision.

1.3 Objectives

Under Phase I and Phase II Small Business Innovative Research contracts with the Air Force Research Laboratory's Human Effectiveness Directorate, mobileFOUNDATIONS, Inc. (mFI) proposed to develop a system that could assist the Air Force in achieving the objectives of improved Space Situation Awareness (SSA), "on-demand" operations, and cost-effective and responsive approaches. mFI proposed that properly designed tools that provide advanced automation and remote collaboration can significantly reduce the operators' burden, while increasing distributed situation awareness. Such tools can enable a paradigm shift from traditional 24 by 7 on-console operations to highly automated operations, in which many of the traditional monitoring tasks are handled autonomously. When problems occur, the tools can rapidly assemble appropriately skilled response crews, regardless of location. This concept transforms a valuable crew from task monitors to on-demand supervisors, freeing them to perform vital and cognitively challenging tasks such as planning and anomaly resolution. Not only is this approach cost effective, but it also provides for a better allocation of limited resources.

mFI's Phase I SBIR results determined that a system to be deployed to enable on-demand Air Force space operations would need to:

1. Work in a real-time manner (i.e., process telemetry streams in near-real-time and send and receive alerts from those streams as new events occur)

2. Incorporate an appropriately designed human factored user interface

3. Incorporate advanced collaboration tools (e.g., screen sharing and whiteboarding) for distributed crew anytime, anywhere access to data

4. Support open standards (e.g., SQL databases, XML)

Thus, our primary goal for Phase II was to develop a next-generation near-real-time system that would enable the Air Force to move towards distributed space operations *with enhanced anytime, anywhere* situation awareness, with a particular focus on Space Situation Awareness (SSA). Our vision of on-demand operations and anytime, anywhere access to personnel and data is shown in Figure 1. This figure illustrates that with the proper tools, the traditional operations center becomes "virtual." On-site engineers, specialists, and supervisors are immediately notified of critical events. If needed, remote personnel can be automatically notified and can share data and applications with on-site personnel to resolve anomalies or rapidly act on events of interest.

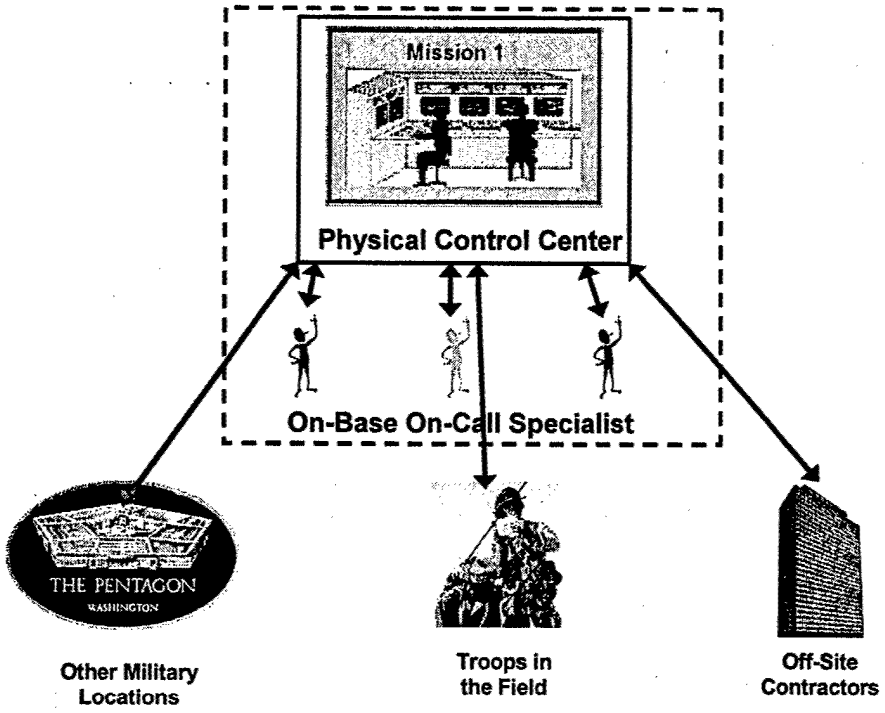


Figure 1. Vision of On-Demand Operations

Our Phase II SBIR focused on developing the core technologies to support the above requirements. Our primary focus was on near-real-time monitoring, incident management, and alerting functions. A secondary focus was on tying in real-time collaboration tools to support distributed communication and the sharing of data and applications.

1.4 Content of Report

This document serves as the final report for our Phase II effort. First, we describe the resulting software product from this Phase II, FASAT (Fast Access Situation Awareness Toolkit). FASAT is a unique and powerful combination of tools that enables reliable and cost effective on-demand, distributed operations. FASAT combines that general functionality with tools specifically targeted at dramatically improving spacecraft mission operations, such as:

- Automated report-generation for anomalous events
- Integrated incident management and workflow technologies to streamline operations
- An XML architecture that accepts data from ground systems via "plug-ins"
- Support for third-party collaboration tools
- Two-way wireless access to data via almost any device over any network

In addition, FASAT is highly usable (it incorporates mFI's IncidentPortal™ user interface) and standards-compliant. A high-level view of FASAT's core functionality is shown in Figure 2.

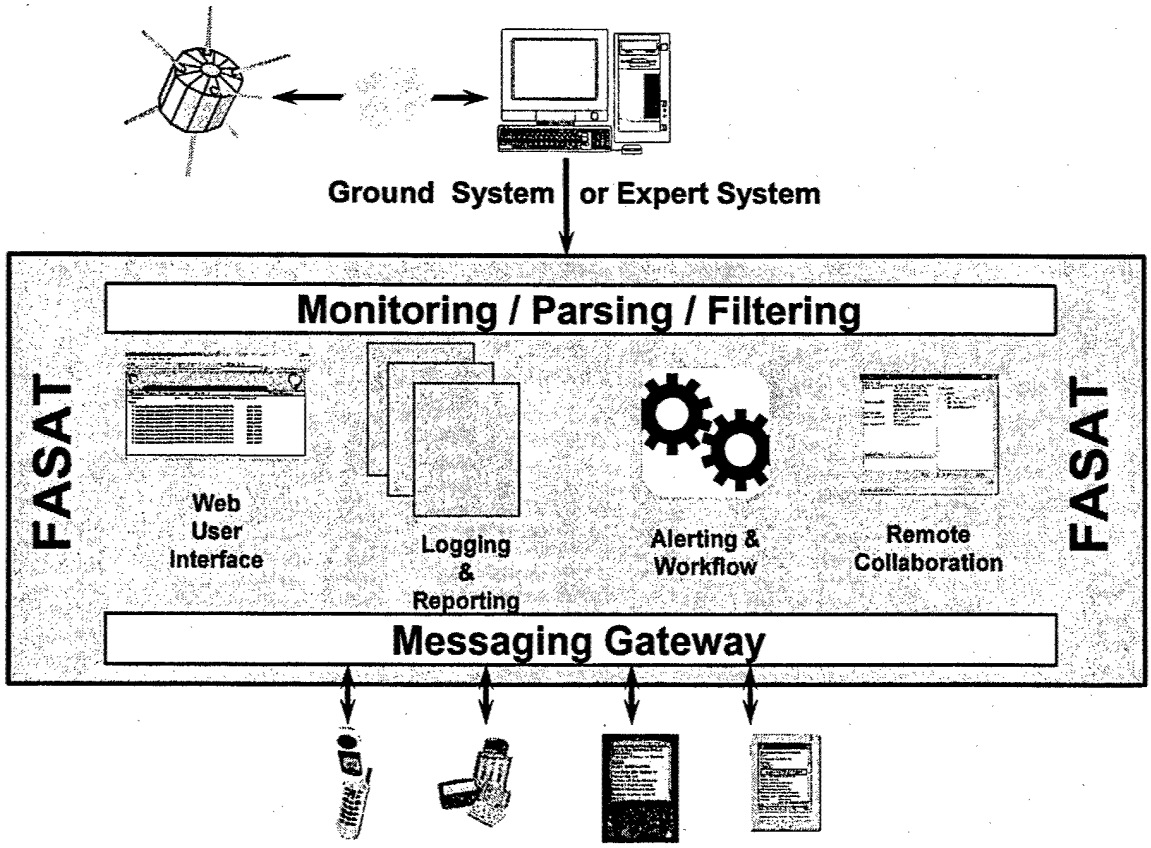


Figure 2. High-Level View of FASAT

Then, we describe the activities we conducted to analyze and understand the users and their needs and to investigate critical technical issues: near-real-time monitoring, incident management, and alerting.

2.0 Overview of FASAT Design

This section provides a high-level overview of the software design of FASAT.

2.1 Architecture of System

In order to build a FASAT system that could process streams of telemetry, we could not use the same architecture as the enhanced SERS system from the Phase I SBIR. The three most significant elements of FASAT developed under this Phase II SBIR are the:

a. *Near Real-Time Stream Processor.* The Stream Processor subscribes to and listens for data from the streaming data sources. The Stream Processor is also responsible for performing data parsing and filtering "on the fly."

b. *Incident Engine.* The Incident Engine manages the incidents, such as when incidents start, when they end, what event data belongs with which incident, when to notify responders about updates, etc.

c. *Alerting Engine.* The Alerting Engine decides whom to notify when a new incident occurs, how to notify them (which devices), and whom to notify when the currently alerted person doesn't respond in the allotted time period.

FASAT also leverages existing mFI technologies. The user interface and database structure are from mFI's commercial Homeland Security product, IncidentPortal™.

After evaluating different technologies, we decided to implement all of these systems using Java and to interconnect the systems using Web services and sockets. The architecture diagram of

FASAT (Figure 3) also shows the basic information and process flow, which will be described later in this section.

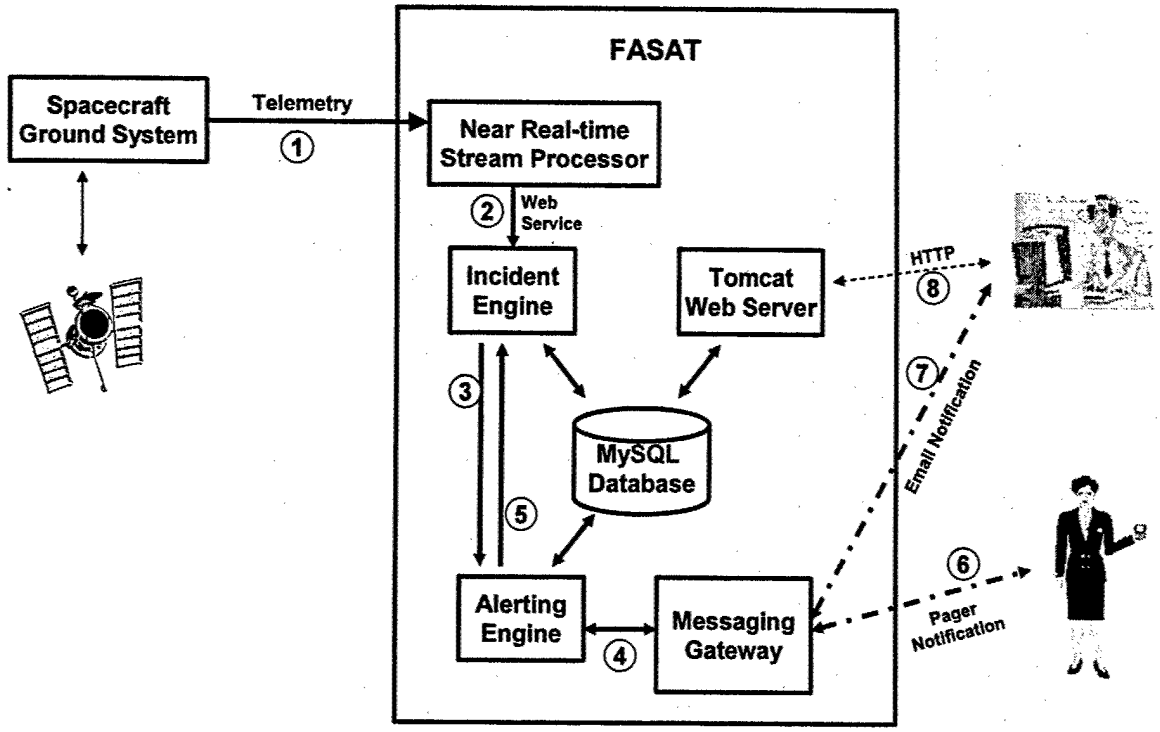


Figure 3. High-Level FASAT Architecture

2.2 FASAT Process Flow

In Figure 3 above, Sequence #1 shows a data stream feeding into the Near Real-Time Stream Processor. The Stream Processor parses and filters the data stream, looking for event data that match the criteria users defined in FASAT. Event data that match the criteria are sent to the Incident Engine via a Web service call (Sequence #2). We used Web services to allow the Stream Processor and the Incident Engine to be distributed across a computer network. We also wanted an open architecture to allow other processes similar to our Stream Processor to be able to send data to FASAT.

The Incident Engine collects the event data, and decides when to start a new incident, or notify users of an update to an existing incident. When the Incident Engine decides that users need to be notified of something, it communicates directly with the Alerting Engine (Sequence #3). The Alerting Engine is responsible for determining which specific users to notify, on what devices, and who gets notified next in case the primary user defers or fails to respond in a given period of time. The Alerting Engine sends its outgoing messages to users via the Messaging Gateway (Sequence #4). As replies come back from users, the Alerting Engine informs the Incident Engine (Sequence #5).

The Messaging Gateway is responsible for delivering individual messages to individual people. It knows nothing about the messages it delivers, only how to route the message content to specific carriers and what protocols to use. The Messaging Gateway uses either WCTP (Wireless Communications Transfer Protocol) or SNPP (Simple Network Pager Protocol) to communicate with a user who has a 2-way Pager (Sequence #6), and it uses SMTP (Simple Mail Transfer Protocol) to communicate with a user who wants to be notified via email (Sequence #7). The 2-way Pager user can read the alert notification and all of the details right on the pager, then respond via the Pager. This response flows back through the Messaging Gateway to the Alerting Engine, which processes the response and notifies the Incident Engine if appropriate.

PC users who received their alert notification via email would probably use the URL contained within the email message to access the Incident Report via their Web browsers on their PC's. The Web browser connects to the FASAT User Interface, running on a Tomcat Web Server (Sequence #8). The user interface allows the user to view the complete Incident Report and to respond to the alert notification.

At the heart of the system is a MySQL Database. Besides being the central repository for all of the data related to FASAT, we also utilized the master/slave functionality of MySQL, which allows the data to be replicated to another database server. Since FASAT is to be used in mission critical applications, all of the FASAT components have failover capability built-in. If a single process fails on a machine (like an Alerting Engine process, for instance) or stops running, a backup Alert Engine process will automatically wake up and begin processing where the former Alerting Engine process left off. Similarly, if an entire machine becomes unavailable, a backup machine with a complete replica of the database and all applications will become available for users until the primary machine is restored.

3.0 Analysis

3.1 Leverage Past Experience

3.1.1 NASA Work

Going to distributed on-demand operations can save money and better utilize personnel, but it must not significantly degrade the quality of operations. That is, it must not lower the system's overall effectiveness. Improper implementation of automation can lead to catastrophic consequences, including the loss of the space vehicle, opening the operating agency to harsh criticism (Trimble, 2000).

When NASA's Goddard Space Flight Center (NASA-GSFC) decided it needed to move to on-demand operations to reduce the cost of operations, it determined that in order to meet these sometimes-conflicting demands, the system must: (1) be easy to use, (2) reduce workload, (3) have flexible communications, (4) be reliable, and (5) be cost effective.

To accomplish these objectives, NASA-GSFC sponsored the development of a Web-based system called The Spacecraft Emergency Response System (SERS) (Fox *et al.*, 2000; Fox *et al.*, 1999a; Breed *et al.*, 1999; Fox *et al.*, 1999b; Fox, *et al.*, 1998; and Baker. *et al.*, 1997). SERS automates many of the monitoring, reporting, notification, and team management activities required for on-demand operations. When SERS detects a problem, it:

- Contacts appropriate on-call personnel
- Automatically generates all necessary reports and documentation
- Enables cooperative work by on-call personnel at distributed locations via wireless two-way communications.

SERS accomplishes these activities via its core functions:

- Intelligent Workflow – SERS dynamically creates teams, alerts team members, and facilitates their communication and collaboration based on its sophisticated knowledge base.
- 2-Way Wireless Communications – SERS not only alerts team members by their wireless devices, but also allows the team members to respond via their device to trigger additional actions and workflow processes. A key to SERS' usability is that communications are tailored to the characteristics of each wireless device (Fox *et al.*, 2000).
- Flexible Communications – SERS communicates with and responds to triggers from almost any front-end device or process (e.g., a signal indicating an irregular heartbeat from a heart monitoring device or the notice of a plane crash). This flexibility to interact with currently deployed systems protects clients' previous investments.
- Automated Reporting and Routing – SERS automatically generates appropriate paperwork (e.g., a problem report or an update to a patient record) based on the specific event. SERS also manages the workflow processes of the routing of reports.
- Web User Interface – All SERS operational and configuration functions are accessed via an integrated, a highly usable Web (HTML and Java) user interface.

A typical NASA mission using SERS generally needs only one operator working a single shift 8 hours/day, 5 days/week. Prior to SERS, a typical satellite operations center employed 2 - 3 operators per 8-hour shift, 3 shifts/day, and 7 days/week.

Despite SERS' capabilities, the direct application of the SERS system to Air Force operations is limited because:

- SERS only supports post-pass operations.
- There is a significant delay in sending out alerts.
- There is no way to keep remote personnel up to date on status changes.
- SERS has no ability for remote personnel to collaborate.
- SERS is based on proprietary legacy software (Lotus Domino).

However, mFI used the lessons learned from the deployment and operations of SERS in the design of FASAT. Many of the issues regarding space operations for NASA are common to all space operations.

3.1.2 Phase I Work

In Phase I, our goals were to conduct a project to: (1) understand Air Force users (human effectiveness) and architectural requirements; (2) study the impacts of current high-risk technology issues, such as wireless security; (3) demonstrate a proof-of-concept functional prototype based upon the Spacecraft Emergency Response System (SERS), which mFI's staff built for NASA; and (4) identify essential capabilities needed for Phase II operational prototyping.

Our studies primarily focused on evaluating current operations at the Center for Research Support (CERES) at the Schriever AFB. The Air Force and mFI both felt that this was the most appropriate environment for our research efforts since: (1) the majority of the CERES' staff are

ex-Air Force mission operations personnel and (2) it is the CERES' mission to support such technology demonstration and evaluation activities.

We collected requirements from several sources. The on-site contextual inquiries that we conducted with both the CERES operators and the technical staff (software and architectural) proved to be extremely valuable sources of data. Another important source of data was Air Force documentation. In particular the *RSC and CERES SYSTEM DESCRIPTION: A GUIDE FOR CUSTOMERS AND USERS* was very useful. That document provides details on the current "CERES Architecture," called the COTS Based Real-time Architecture (COBRA).

In our Phase I human effectiveness studies, we were able to:

- Gain a firm (though high-level) understanding of how the Air Force currently performs space operations at CERES and at the SOPS.
- Collect feedback on what types of technologies would be of assistance to the Air Force.
- Understand many of the user (skills and capabilities) and organizational (political and procedural) challenges and obstacles to introducing advanced automation into an Air Force operational environment.
- Document the human effectiveness research that would need to be conducted in our proposed Phase II effort.
- Develop a list of capabilities that would be required for the Phase I and Phase II prototypes.
- Specify the necessary features for our Phase I proof-of-concept to show the feasibility of our approach.

In our architectural (software design) studies, we were able to:

- Assess how advanced automation can be applied within the CERES COBRA architecture (the one upon which the proof-of-concept prototype was based).
- Develop a list of technical capabilities that will be required to implement the functions identified in the human effectiveness studies.
- Determine how to implement the capabilities in enough fidelity to demonstrate their utility in the Phase I proof-of-concept prototype.
- Determine what enhancements would be needed to make the SERS software operational within a CERES environment.

More specifically, we found that:

- Air Force operators can function in a distributed and wireless environment.
- We can seamlessly integrate COTS collaboration software with mission operations software.
- We can develop software to respond to triggers in near-real-time. Although we did not develop such software in Phase I, we defined some approaches towards satisfying this need.
- End-to-end security is possible using either COTS or custom tools.
- Our software can interface with a modern Air Force ground system (CERES' COBRA).
- The Air Force needed additional functionality. For some functionality, we demonstrated the feasibility of the new functions in our prototype. For others, we defined the functionality and the approach we would take to develop it.

3.2 Evaluate Situation Awareness

3.2.1 Introduction

As mentioned above, one of the major goals in the Strategic Master Plan is to achieve "Space Situation Awareness (SSA)." Before designing a system to maximize situation awareness, we reviewed the situation awareness literature to determine the issues that would impact the design. In this section, we define situation awareness, address why it is important for this effort, and discuss several issues that impact our design.

3.2.2 Definition of Situation Awareness

The term "Situation Awareness" (SA) comes from aviation, and generally refers to the pilot's understanding of the situation around them. A basic definition of SA is "knowing what is going on around you" (Endsley, 2000, p. 5). However, SA is more complicated than that. For example, Endsley (1995) further defines SA as:

> ...the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future. (p. 36)

As one of the early investigators of situation awareness in aviation, Endsley further explained her definition of SA by deconstructing the concept into three levels. At each level, there are psychological phenomena that influence an individual's SA. Theories that explain the individual phenomena, therefore, can then help explain the state of SA. The three levels of SA identified by Endsley are:

Level 1 – Perception

Level 2 – Comprehension

Level 3 – Projection

Level 1 SA is concerned with "Does the user perceive the relevant cues?" The research on perception covers a variety of issues such as saliency of the cue and attentional demands of the user.

Level 2 SA evaluates "Does the user understand the relevant cues?" At this level, the concerns are whether the user can correctly interpret the meaning and significance of the cues. A variety of factors can affect this process, including skill, training, workload, and stress.

Level 3 SA addresses "Can the user predict how the system will respond based on the current situation?" This ability is usually developed through training and experience. Users consider not only the current state of the system to predict future performance, but also past states and rates and trends of change.

Many researchers defer to Endsley's definition or use it as a basis for their own (Fracker, 1988, Salas *et al.*, 1995, Nofi, 2000). Others, though, have somewhat different ideas of SA and how it fits into the attention and memory system.

For example, McNeese and Vidulich (2002) discuss the broader role of Cognitive Systems Engineering (CSE) in the development of usable human computer interfaces for decision support systems. They suggest that the goal of CSE is to avoid "cogminutia fragmentosa," wherein "the worker's cognitive world breaks down into small, isolated strands of thought as unanticipated events transpire. There can be a loss of meaning or control as the worker becomes separated

from the demands of his or her work, and many remain lost in terms of comprehending the emerging elements of a situation" (p. xi).

Basically, when cogminutia fragmentosa occurs, the individual focuses on specific details and begins to lose SA. As this continues, he or she moves farther away from a connection to the overall picture and becomes less and less capable of relating the immediate cues and information to a broader context or situation. The authors state that systems design must take into account the operators' need for a coherent picture and a flexible structure that will keep them informed when unexpected situations occur. This, they claim, is where Cognitive Systems Engineering becomes important.

3.2.3 The Importance of Situation Awareness in Space Operations

With today's complex satellite systems, human operators often cannot process all the data themselves. For example, operators could not manage the thousands of parameters used for each mission without assistance. As systems have become more complex, the operators' roles have evolved from "active management," where they monitor every aspect of the system and respond to problems themselves, to "supervisory control," where they only respond to problems identified by the monitoring system. In some cases of supervisory control, the monitoring system can even recommend a course of action, but the final decision is left to the operators. The goal of supervisory control is to get both humans and computers to do what they do best (Adams, Tenny, and Pew, 1995).

As a "supervisor," when alerted of a problem, the operator must first review the relevant data to learn what has happened, then formulate a response. Unless the information is easily accessible, operators may have trouble transitioning from "passive observer" to "active participant" quickly

(Sheridan, 1980). In this paradigm of "supervisory control," it is critical for operators to have all the information they need when they respond to a problem. This understanding of the situation, or "situation awareness," is critical for the operators to respond appropriately to problems (Adams, Tenny, and Pew, 1995). In cases of reduced crew operations, the operator is brought in only to respond to problems or potential problems. While cost effective, this approach requires a system that presents the operators with the information they need, in a format they can interpret quickly, to insure they perceive all the relevant information without being overloaded (Adams, Tenny, and Pew, 1995). From the information they perceive, operators must rapidly assess the state of the system, prioritize response(s), and then take appropriate actions.

The challenge for designers is magnified when the operators use hand-held computers. These mobile devices often have very small screens, poor input mechanisms, limited graphics capabilities, and slow transmission rates (Fox *et al.*, 2000; Sheridan, 1980), making it especially challenging to display sufficient information.

The specific design implications of SA on FASAT are described below in the Design Process section of this report.

4.0 mFI's Design Process for FASAT

This section describes how FASAT supports SA. This section will address the design challenges and FASAT design decision for these SA issues. More specifically, it maps FASAT's capabilities to Albers' (1999) three specific design goals for complex decision making. Albers' (1999) suggests three specific design goals for complex decision making:

(1) Rather than simply providing the information, the design must assist in problem recognition and provide the information to define the situation and support decision making.

(2) The design must present the new and old information and assist in integrating the information into the user's mental model to support decision making.

(3) The design must support follow-on analysis of the problem to verify that a correct decision was made and that the overall situation is proceeding in the expected manner.

4.1 Rather than simply providing the information, the design must assist in problem recognition and provide the information to define the situation and support decision making.

FASAT is designed to facilitate understanding of situations by aggregating information based on user-defined characteristics and providing additional information as requested. As described above, the users themselves define the filters FASAT uses to identify relevant data and the workflow FASAT follows in sending out alerts. Since the information in the alerts is designed to reflect the way that users classify events, the users are able to understand the nature and significance of the problems FASAT identifies. Albers (1999) states that "once users *believe* they understand the problem, they tend to reach a decision quickly," which means that "the information to prove or disprove the classification must be quick and easy to obtain." (p. 156).

FASAT further supports the decision making process by providing the users quick access to additional information through its Web portal. Users may access the history of any incident through incident reports on the Web, and they may also view information added by other responders. This allows users to see how the incident has developed over time.

4.1.1 FASAT Data Sources and Types

FASAT allows users to indicate (1) what data to monitor, (2) what patterns constitute an incident, (3) whom to notify about an incident, and (4) what to tell them. When an incident occurs, FASAT automatically determines what specific content goes to which people at what time and via what methods. To accomplish these tasks, we designed FASAT to have ***Filters*** and ***Notifications***, tied together in ***Scenarios***.

The first step in building Scenarios is giving the Scenario a name, entering description, selecting the data source (e.g., ITOS), and either enabling or disabling the Scenario. See Figure 4, below.

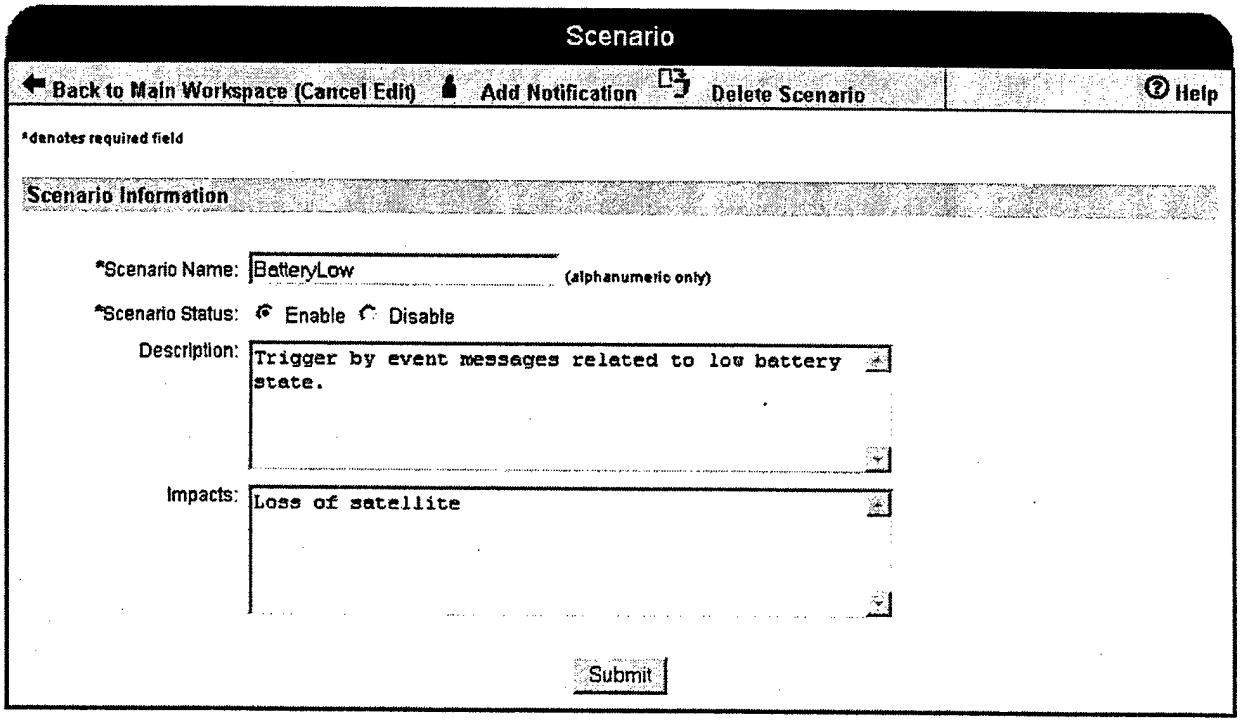


Figure 4. Form for Defining Basic Information for the "BatteryLow" Scenario

4.1.2 Filters

Next, the user defines the "events of interest," such as out-of-bounds parameters or particular messages. Users do this by adding filters. There are two types of filters in FASAT:

- "Include" Filters that define what patterns should trigger an incident
- "Exclude" Filters that define what patterns should not trigger an incident.

4.1.2.1 Filters used in FASAT

In the space domain, FASAT will typically monitor the event messages or log files outputted from a ground system. To validate our system, we needed a data source that could stream data to our system. Since we were unable to get actual Air Force spacecraft telemetry system to feed us data, for the majority of our testing we decided to use streaming telemetry data from the ITOS (Hammers, 2003) ground system used at NASA GSFC.

ITOS has many different data streams to which to subscribe. We chose to use the event data stream provided through "evtforward," a process associated with an ITOS system that is responsible for forwarding event data to external applications. The event data can be parsed into separate tokens, which can then be filtered on a variety of criteria. The Event Codes in ITOS are described in Table 1. Some sample ITOS event data appears below:

> 02 02-345-06:06:55 YEL_VIOL: Yellow low violation AGY1X cnv = 0.6787741 at 02-344-03:25:18.50901
>
> 29 02-345-06:01:40 CFG_ALERT: configuration rgnengtrend: "Command rejection occurred (CIREJREASON)" at 02-344-04:06:21.01991

This can be parsed into the following fields: 2 digit Event Numeric Code, Date Time stamp in Julian format, Event Code, Event Message.

For event messages, like Yellow and Red Limit Violations, the data in the Event Message is parsed further, into color value, status (high or low), mnemonic name, mnemonic value, and date and time when the mnemonic value was recorded.

We configured the Stream Processor to parse the ITOS data stream, and to apply filters on the data. Some filters that we designed were very general, such as "match on any data with an event code of "CFG_ERROR". Some were very specific, such as "match on YEL_VIOL events with mnemonic AGYIX in a high state". We designed others as exceptions: "match on any TM_MSG events except for ones where the Message contains A1X23".

The filters we used for testing were primarily looking for Limit Violation data (RED_VIOL and YEL_VIOL Event Types). We also setup filters to look for certain keywords as part of other Event Types, like CFG_ALERT messages.

4.1.2.2 Setting Up Filters

Once users have established scenarios, they add filters. They first enter the filter name and description, then they select the data source (e.g., ITOS) and whether the filter is enabled (see Figure 5). Next, users add "Filter Elements" which define individual parameters (elements) of the Filter. FASAT uses drop-down menus for this, eliminating the need for the user to have either a detailed understanding of the data source or complex Boolean logic (see Figure 6).

After the form has been submitted, FASAT automatically creates all of the Boolean constructs and populates that information back in the Filter form for the Scenario (see Figure 5).

enum	code	Meaning
NULL_EVENT	0	Unknown event type; can't be filtered.
RED_VIOL	1	A red limits violation occurred.
YEL_VIOL	2	A Yellow limits violation occurred.
DEL_VIOL	3	A Delta limits violation occurred.
IN_LIMITS	4	A value went back in limits.
TM_MSG	5	Telemetry informational message.
TM_WARN	6	Telemetry warning message.
TM_ERROR	7	General telemetry error message.
CMD_EVENT	8	Command event.
CMD_VERIFY	9	Command verify/no-verify message.
CFG_ERROR	10	Configuration error message.
CMD_MSG	11	Command informational message.
CMD_WARN	12	Command warning message.
CMD_ERROR	13	General command error message.
CMD_TF	14	Command transfer frame echoed in hex.
OPER_ERROR	15	STOL Operator error.
STOL_ECHO	16	STOL echo of directives.
STOL_MSG	17	STOL MSG directive message.
STOL_WARN	18	STOL warning message.
STOL_ERROR	19	STOL error message.
DSP_MSG	20	Display informational message.
DSP_WARN	21	Display warning message.
DSP_ERROR	22	Display error message.
FTCP_MSG	23	FTCP xmit proc informational message.
FTCP_WARN	24	FTCP xmit proc warning message.
FTCP_ERROR	25	FTCP xmit proc error message.
SYS_ERROR	26	System call failure message - call a programmer!.
TCW_FAULT	27	Serious error message - call a programmer!.
SC_EVENT	28	Spacecraft event message.
CFG_ALERT	29	Configuration monitor alert message.
DEBUG_EVT	30	A debugging message.
SDP_MSG	31	Science Data Processing message.
SDP_WARN	32	Science Data Processing warning.
SDP_ERROR	33	Science Data Processing error.
CTLR_MSG	31	Controller message.
CTLR_WARN	32	Controller warning.
CTLR_ERROR	33	Controller error.

Table 1. ITOS Event Codes

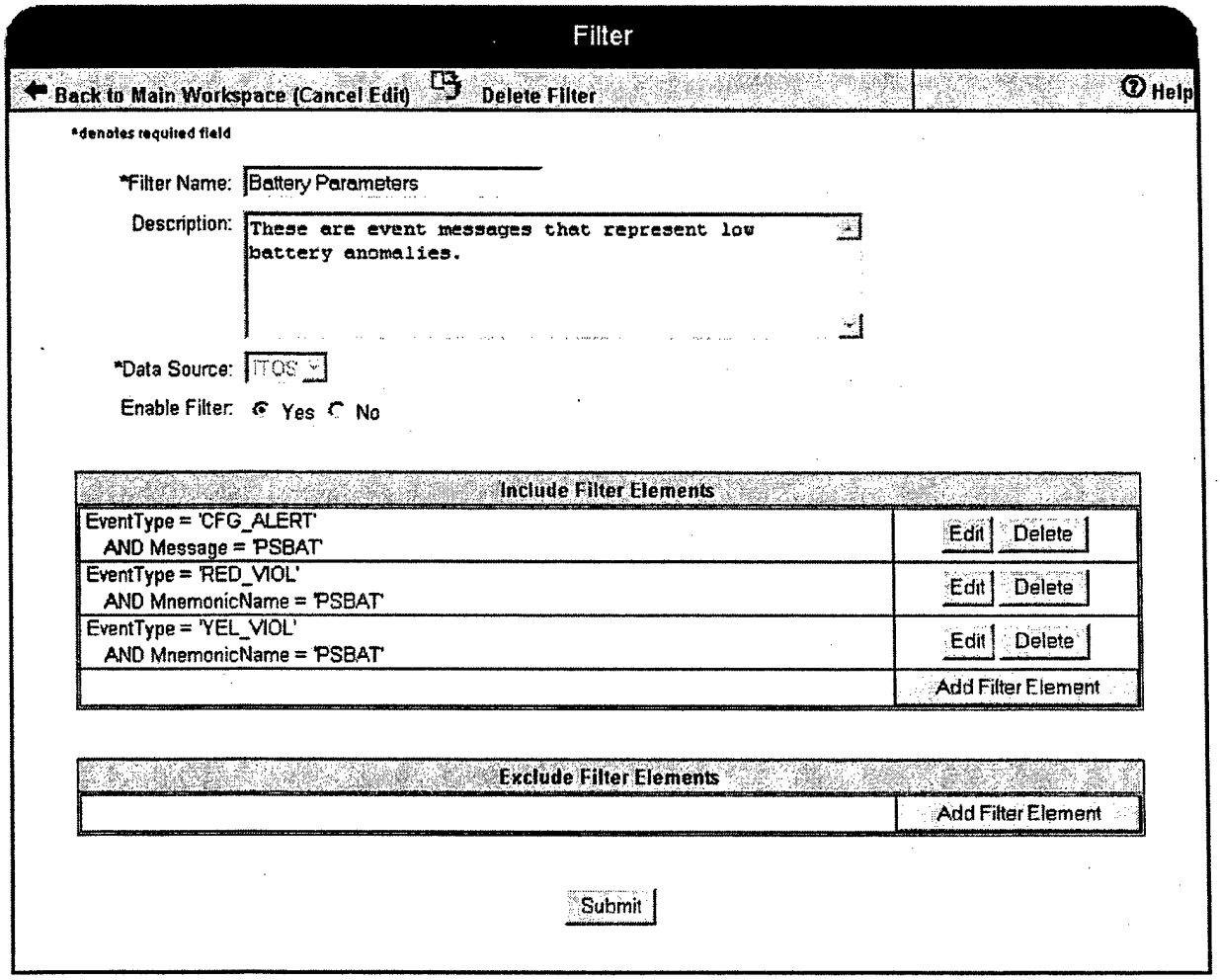


Figure 5. Form for Building a Filter for the "BatteryLow" Scenario

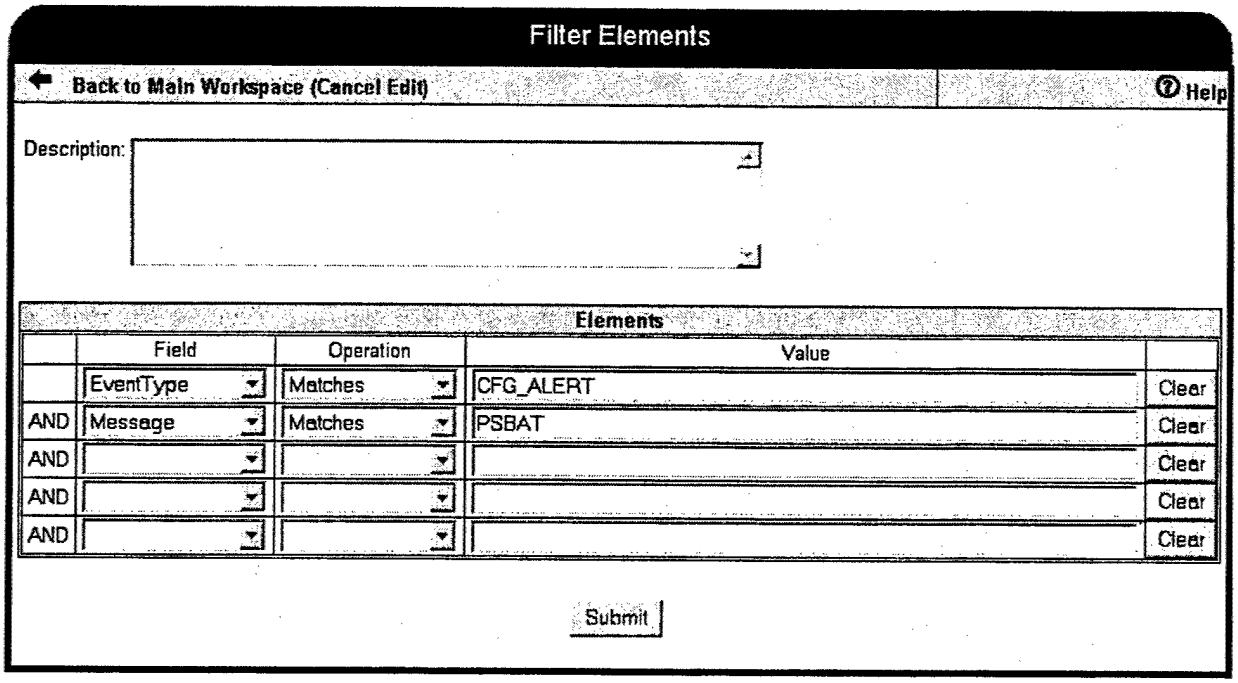


Figure 6. Form for selecting Filter Elements for the Filter in Figure 5 (Above)

4.1.3 Notifications

Users define whom to notify and how to notify them for each scenario with Notifications (see Figure 7). The Notification page allows the user to define:

- Whom to notify (by position or name)
- Method of notification (rollover, round robin, group, or informational)
- An alert message to send with the Notification
- Specific fields from the data file to go to this notification group.

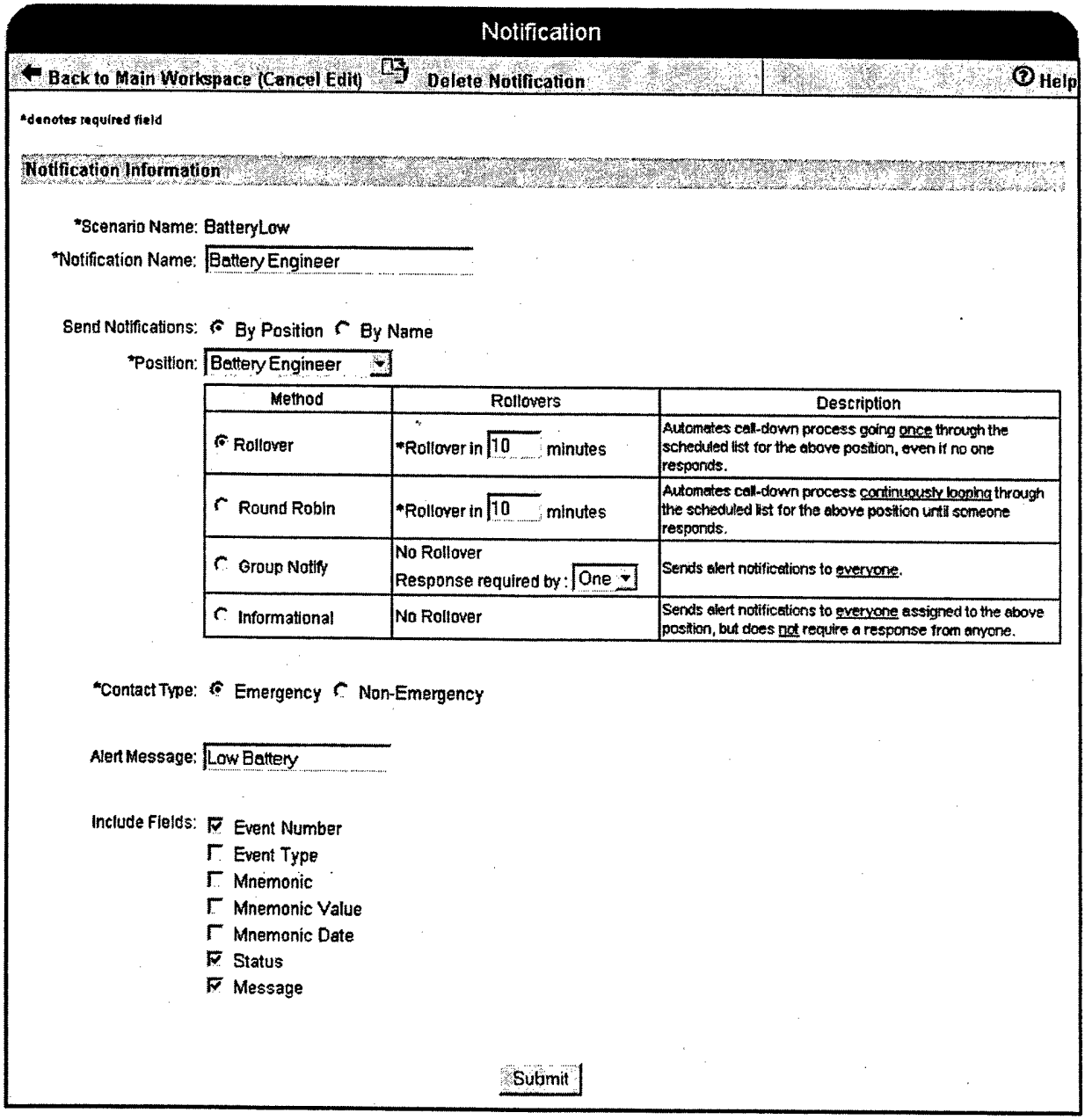


Figure 7. Form Defining a Notification for the "BatteryLow" Scenario

All of the filter and notification input is summarized in the Scenario view screen, as shown below in Figure 8.

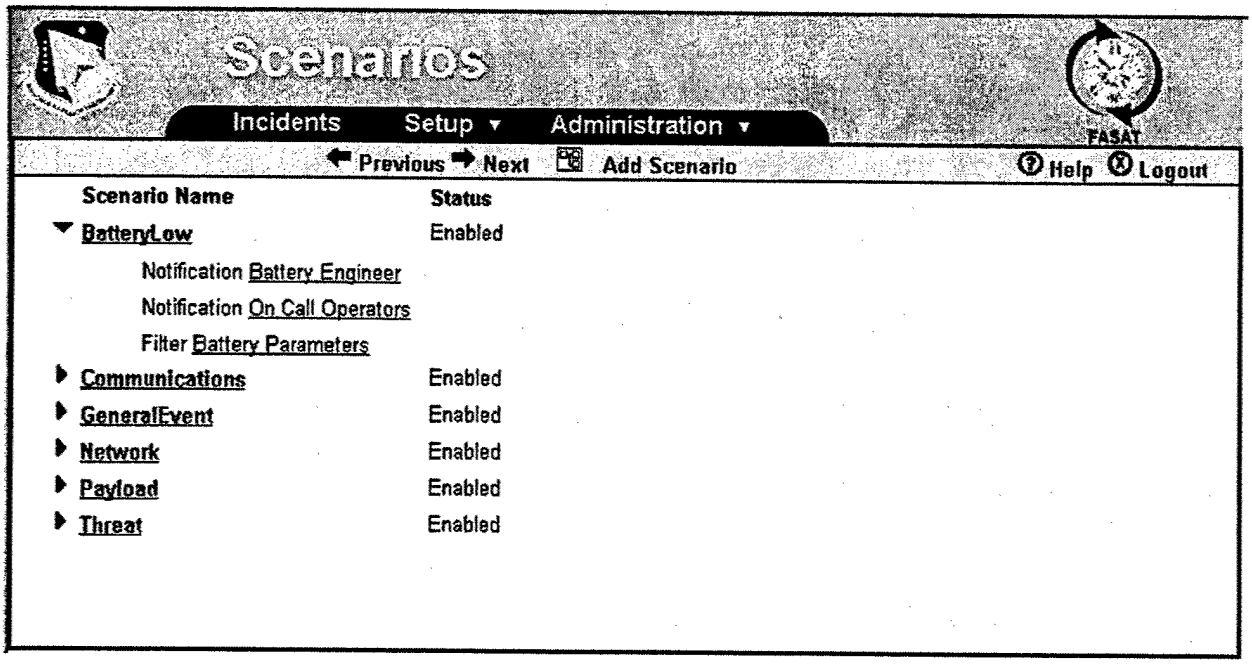


Figure 8. The Summary View for the "BatteryLow" Scenario

4.2 The design must present the new and old information and assist in integrating the information into the user's mental model to support decision making.

In order to ensure that users are able to understand a situation in its appropriate context, the first alert regarding an incident (the ***Initial Notification***) includes all the information requested in the scenario's Notification. This ensures that users receive all of the appropriate information. This initial information remains accessible on users' devices as long as they do not delete it.

In order to ensure that users remain aware of the situation as it changes, FASAT can provide current information both a) until the users respond to the notification and b) after the users have accepted or deferred responsibility for an alert.

a) Users who have not yet responded to the notification may be either busy or unable to receive notifications. Either way, users should have access to the most current information about an event as soon as they are ready or able to receive that information. To facilitate this, reminder messages (***Auto Reminders***) that include the new information about an alert can be sent to users who have not responded to the notification.

b) Users who have responded to the alert may also request ***Updates*** to keep them apprised of the situation as it changes over time. Updates include all of the information that has changed since the last notification was sent.

4.2.1 Managing Users

One of FASAT's greatest strengths is its ability to send notifications to users, regardless of their wireless devices and service providers. To accomplish this, we designed a form that allows users to enter all their contact information, such as work and home phone and email, cell phones, pagers, and wireless PDAs. Users then select a single device, or series of devices, that they wish to use for their "Emergency" and "Non-Emergency" contacts. FASAT uses this information to custom format the content of its alerts to maximize the information transfer to the user. Figure 9 and Figure 10 show all of the data collected on people profiled for FASAT. These capabilities are required to ensure that the right user gets the right data in the best format to gain initial SA and maintain SA.

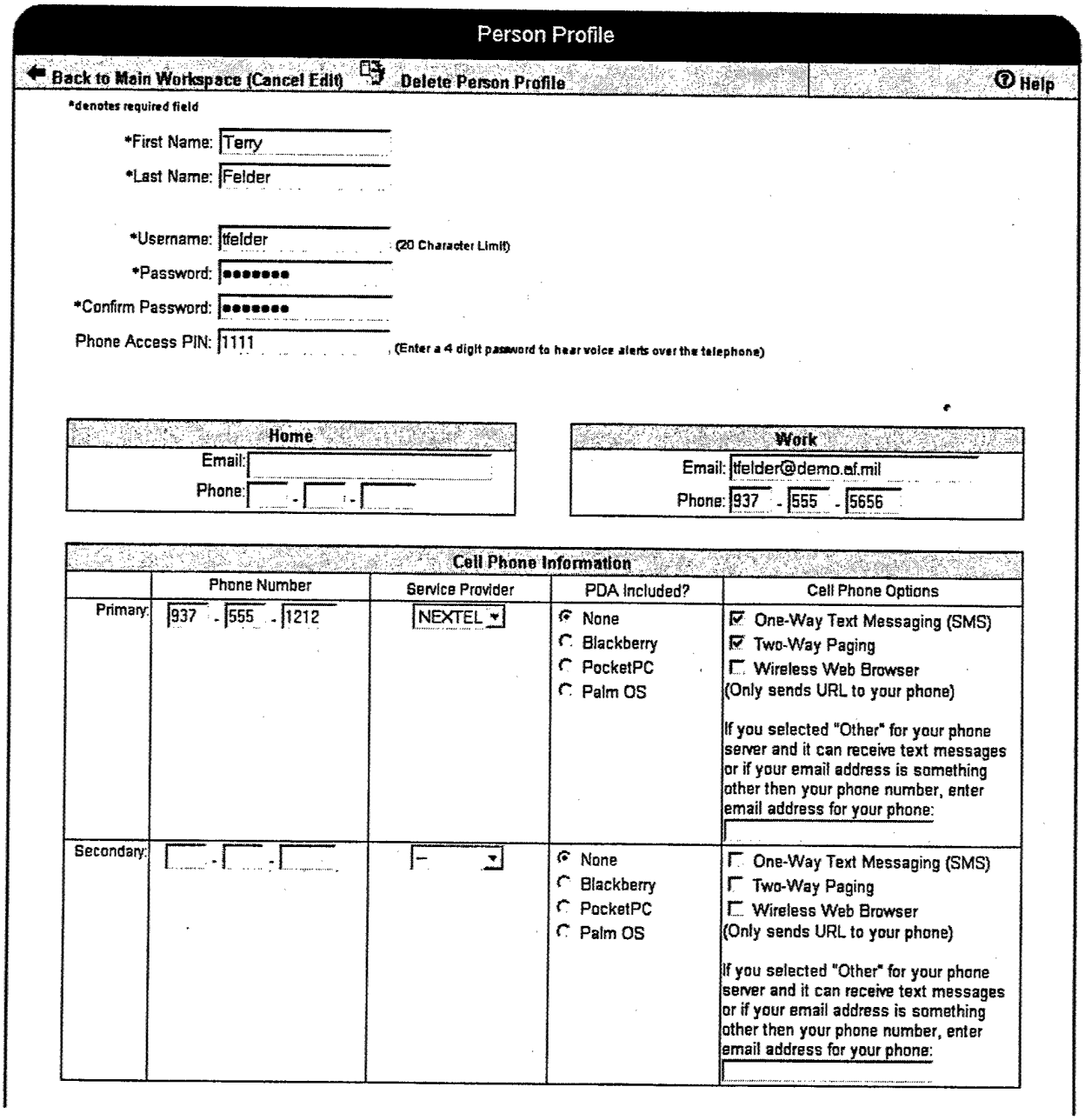


Figure 9. Top-Half of a Person's Profile

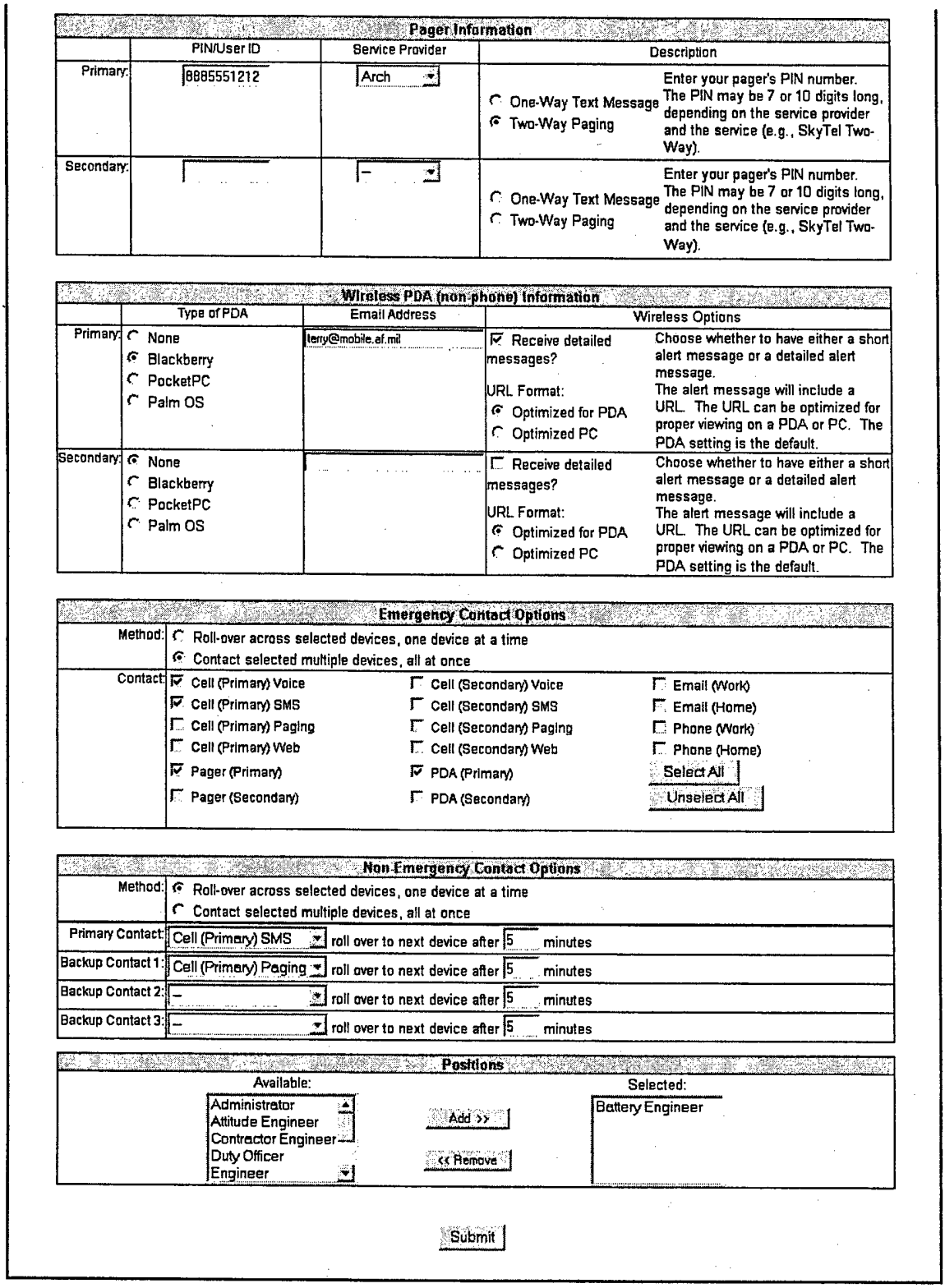


Figure 10. Bottom-Half of a Person's Profile

Figure 11 shows the list of all of the users and their email and work phone contact information.

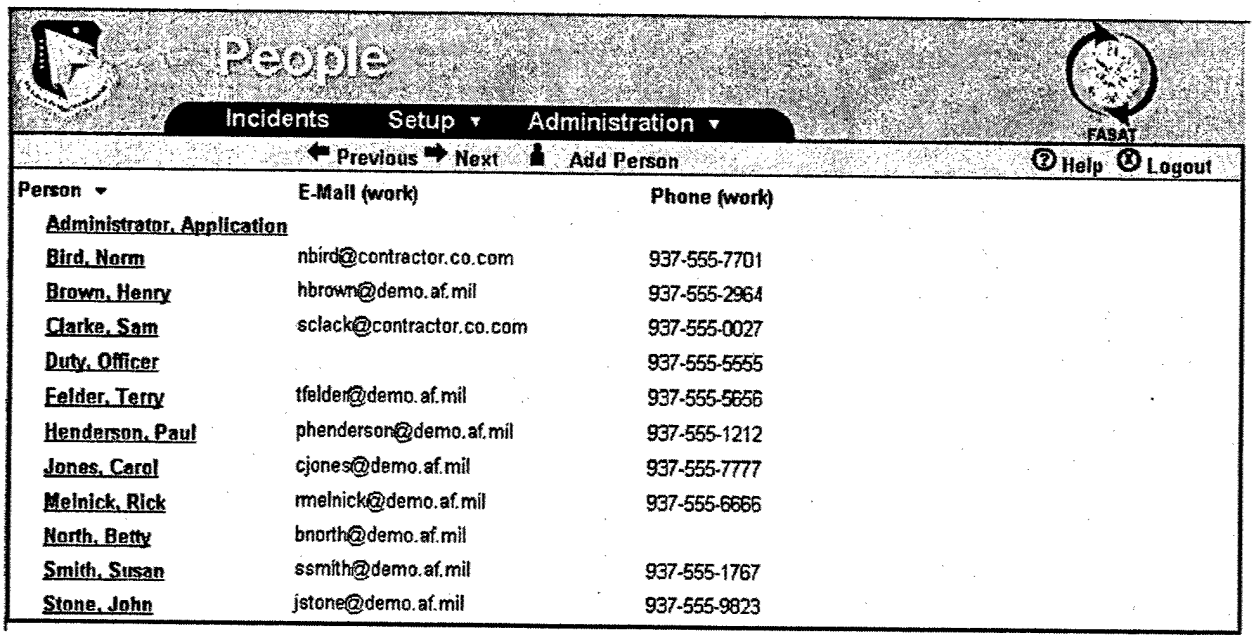


Figure 11. Summary View of People in the FASAT System

4.2.2 Managing User Access

A critical aspect of FASAT is the regulation of who can access the various features. FASAT accomplishes this through the use of "Positions". A position is the role assigned to one or more individuals in the organization using FASAT. In the "space" domain, the positions might include operators, battery engineers, or flight directors. The FASAT Position page is shown in Figure 12. Each position is assigned its own level of access to different features. For example, FASAT could be configured so that only engineers can add and edit alerts, while only flight directors can set up schedules. In addition to the user-defined positions, each organization will have a "system administrator." A person in this position would always have access to every

feature in FASAT. This person should be fairly knowledgeable of FASAT and also responsible enough to merit total access to the system. The Position view is shown in Figure 13.

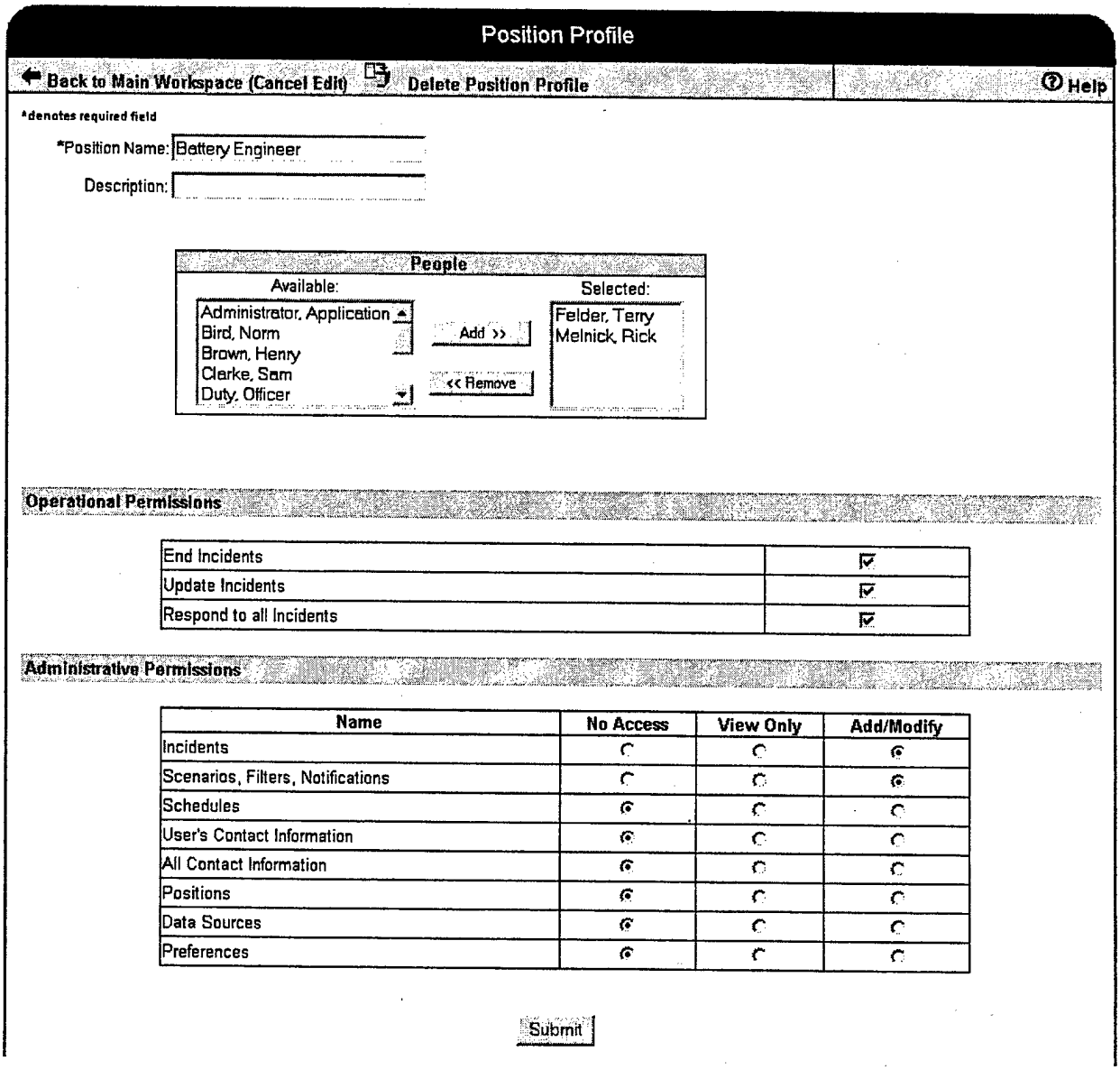


Figure 12. Form for the Battery Engineer Position

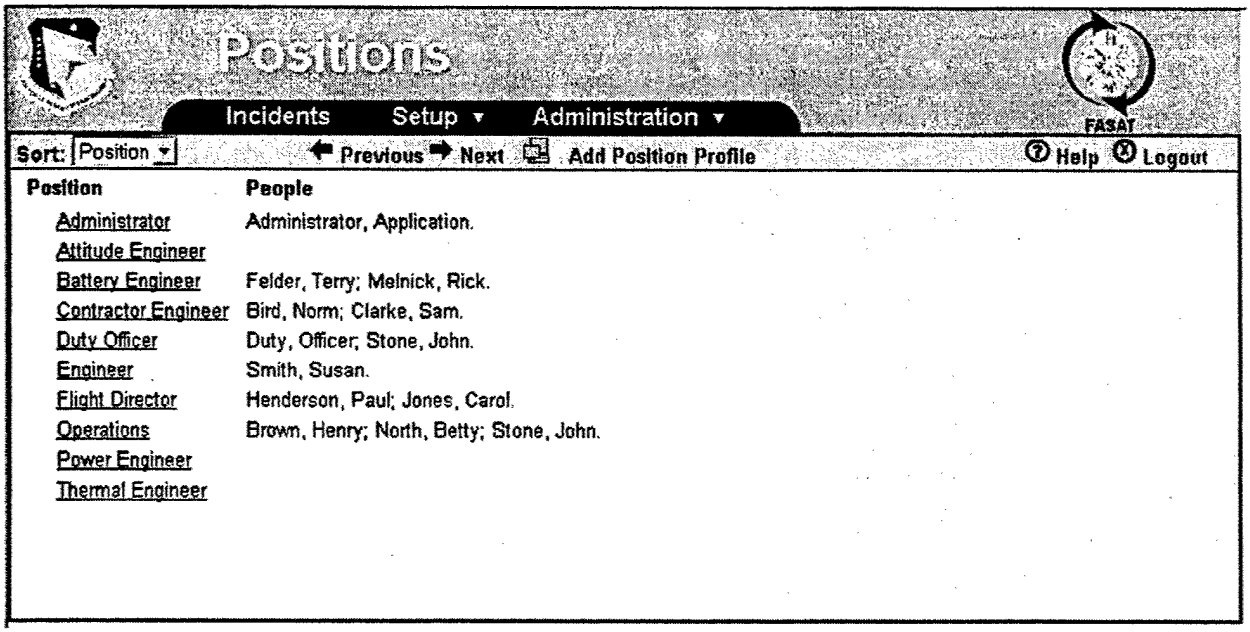


Figure 13. Summary View of Positions

4.2.3 Scheduling

FASAT also includes a basic shift scheduler. As shown in Figure 14, users are assigned to shifts by position.

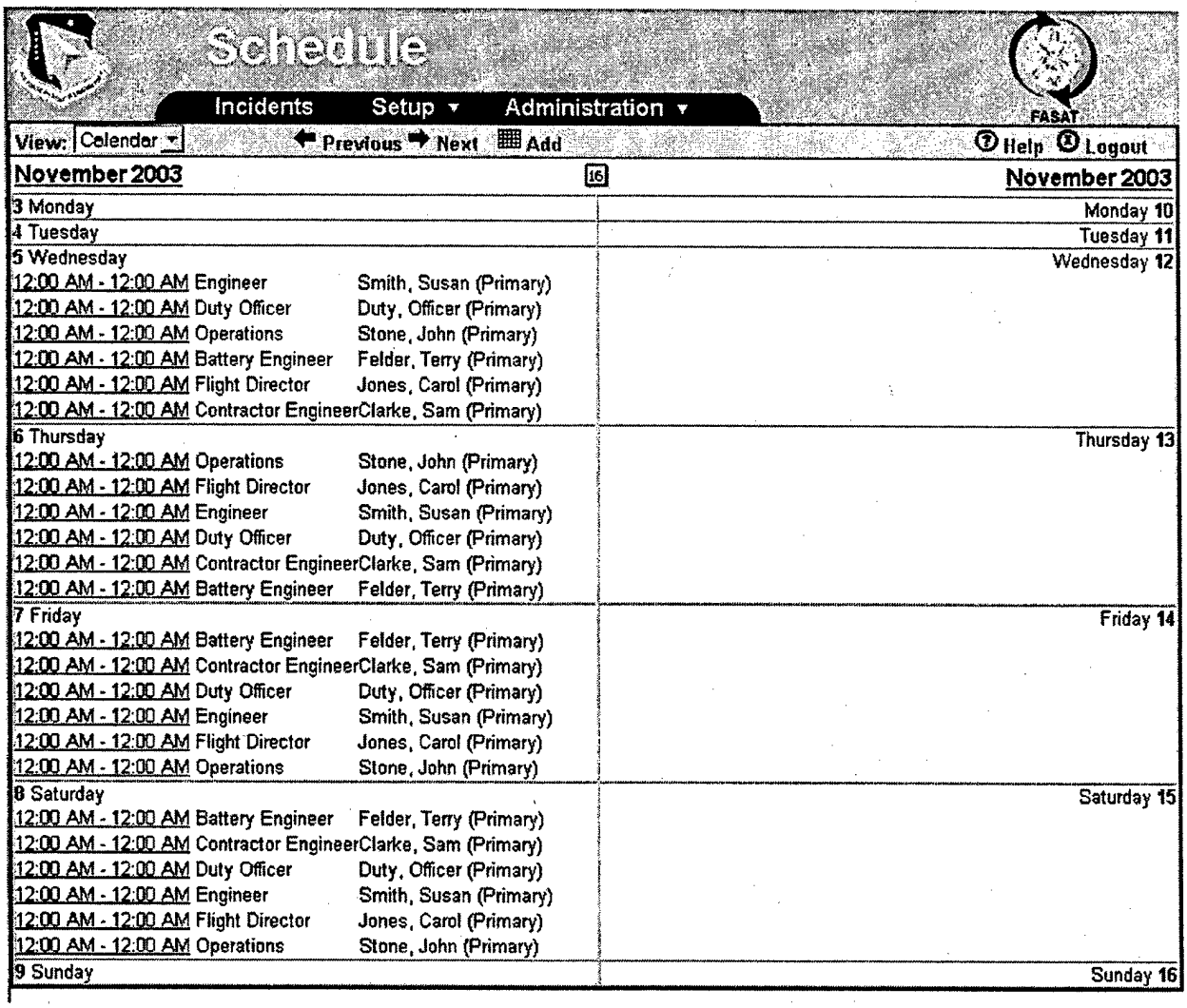


Figure 14. Calendar View for People Assigned to Shifts by Position

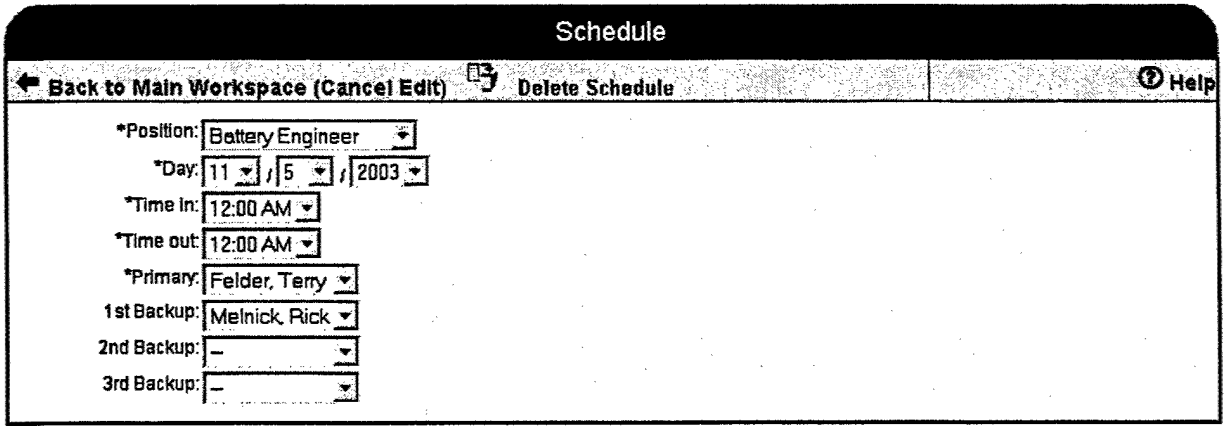
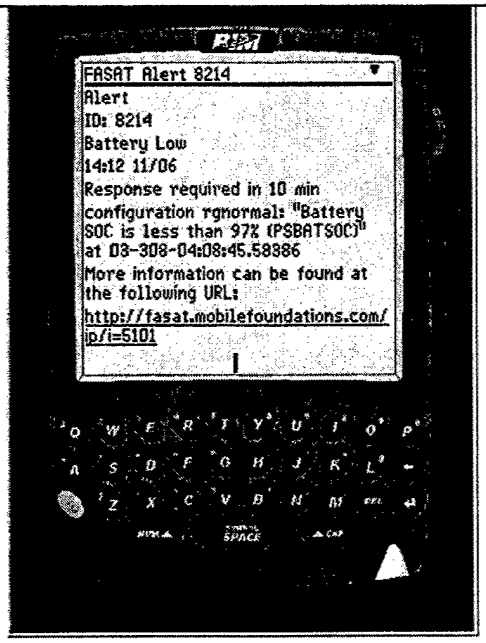


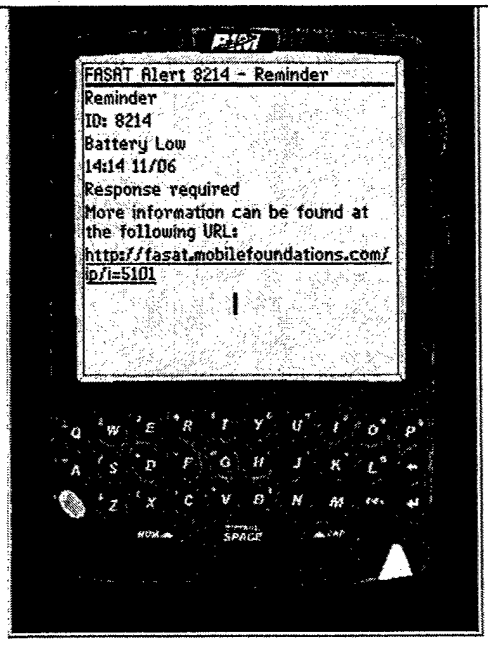
Figure 15. Edit Mode for Defining a Shift Schedule

4.2.4 Wireless Alert Notifications and Responses

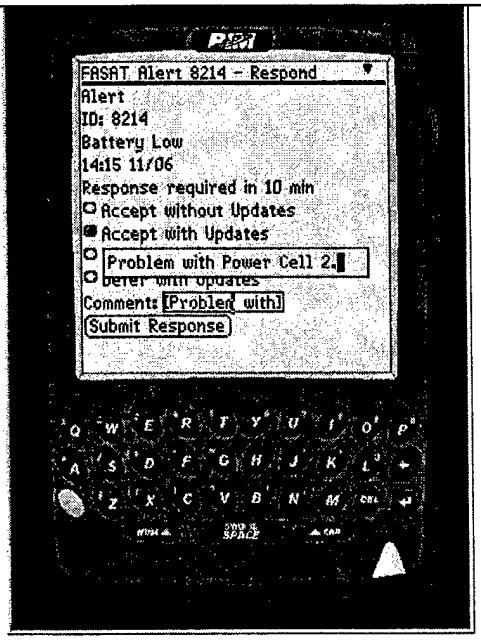
The series of figures below show sample interactions on a RIM Blackberry device:



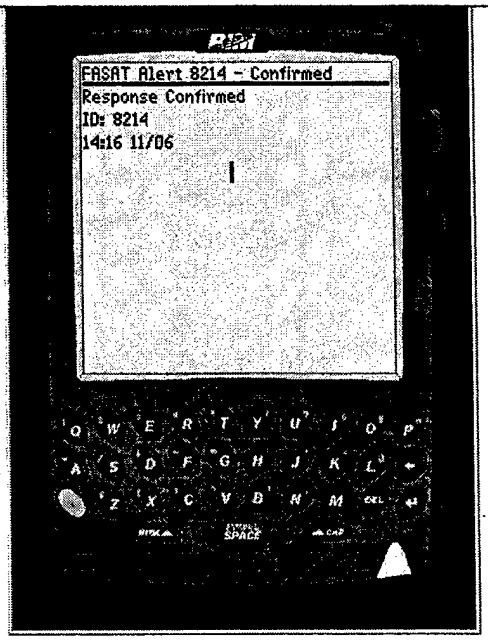
The user receives an initial notification displaying the alert information and the time window in which to respond.



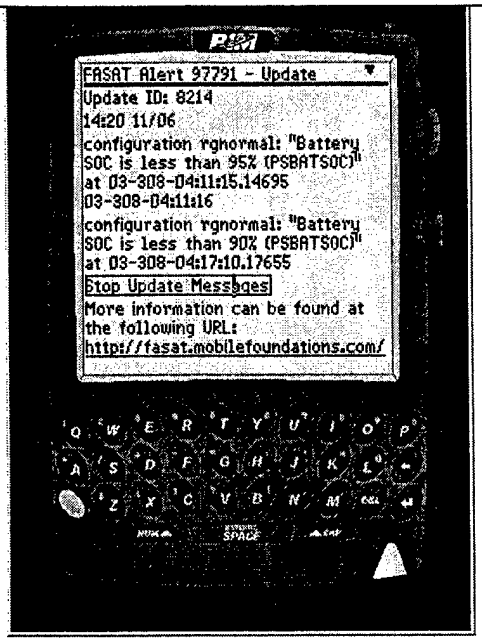
The User receives an auto-reminder to respond to an alert with updated information.



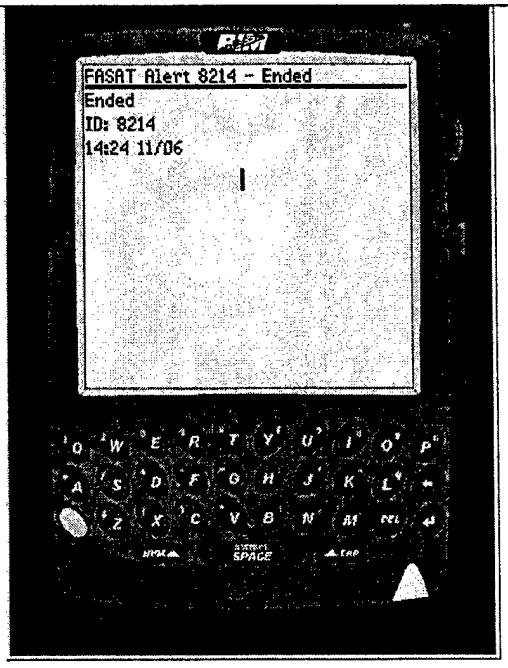
The responds to the alert with "Accept with Updates" and enters comments that will be automatically added to the FASAT portal.



The user receives Confirmation from FASAT that his/her response was received.



The user receives an Update alert. The user then opts to Stop receiving future updates.



The user receives a notification that the incident associated with this alert has ended.

Figure 16. Series of Images for Wireless Alerts and Responses

4.2.4.1 Dealing with the Limitations of Wireless Displays

A key component of FASAT is its wireless alerting functionality. However, the small screens and limited display capabilities of wireless devices present a challenge when designing interfaces to maximize SA. In a typical situation served by FASAT, users would receive an initial alert that there is a problem and would be prompted to choose a response from a range of options. The size and capabilities of displays on wireless devices limit the amount of information that may be conveyed to the user and limit the options for the users' response. Small screens also place a burden on the users' short-term memory (STM) due to the limited amount of information immediately visible on the screen (Albers and Kim, 2000).

It is therefore important to identify the most valuable pieces of information for the operators and engineers who may need to diagnose problems from remote locations. We have to be sure that when users view the displays and integrate that information into their mental model of the situation, they can gain an acceptable level of situation awareness in order to make informed, intelligent decisions.

In order to address these design challenges, FASAT's notifications are succinct, user-configurable messages that describe the event for the user. In FASAT, the information in initial notifications and updates can be tailored to meet the needs of the users and the limitations of their devices. In addition, we accepted that there may be some tasks that would need more information than would fit on a pager or in a Short Message Service (SMS) text message. In these cases, FASAT still provides the basic data to the users, but they might have to browse to the incident report on the Web to get all of the information necessary to resolve the issue.

FASAT also allows users to browse into a version of FASAT's key screens optimized for wireless access on devices with small screens and slow Internet access.

4.2.5 Preferences

FASAT has a Preferences screen for users to define key settings for FASAT. As shown in Figure 17, the Preference screen allows users to set:

- Whether to use the Scheduler
- Operation of Round Robin alerting
- When and how to send Auto-Reminders. "Auto-Reminders" provide additional opportunities for users to realize that they have an alert. Responders may be in a loud environment, unable to hear their cell phone, or they may have put down their pager for just a moment. For these and similar situations where users may miss an individual alert, we designed FASAT's Auto-Reminders. If a user does not respond to an initial notification, FASAT can be set to send additional notifications (the Auto-Reminders) to the users. Users can set the frequency and number of Auto-Reminders appropriate for their organization.
- Whether to use confirmations. Confirmations provide feedback to wireless users that FASAT has received their responses.
- The episode length. Episode length defines the period of inactivity before additional activity is considered a new incident.

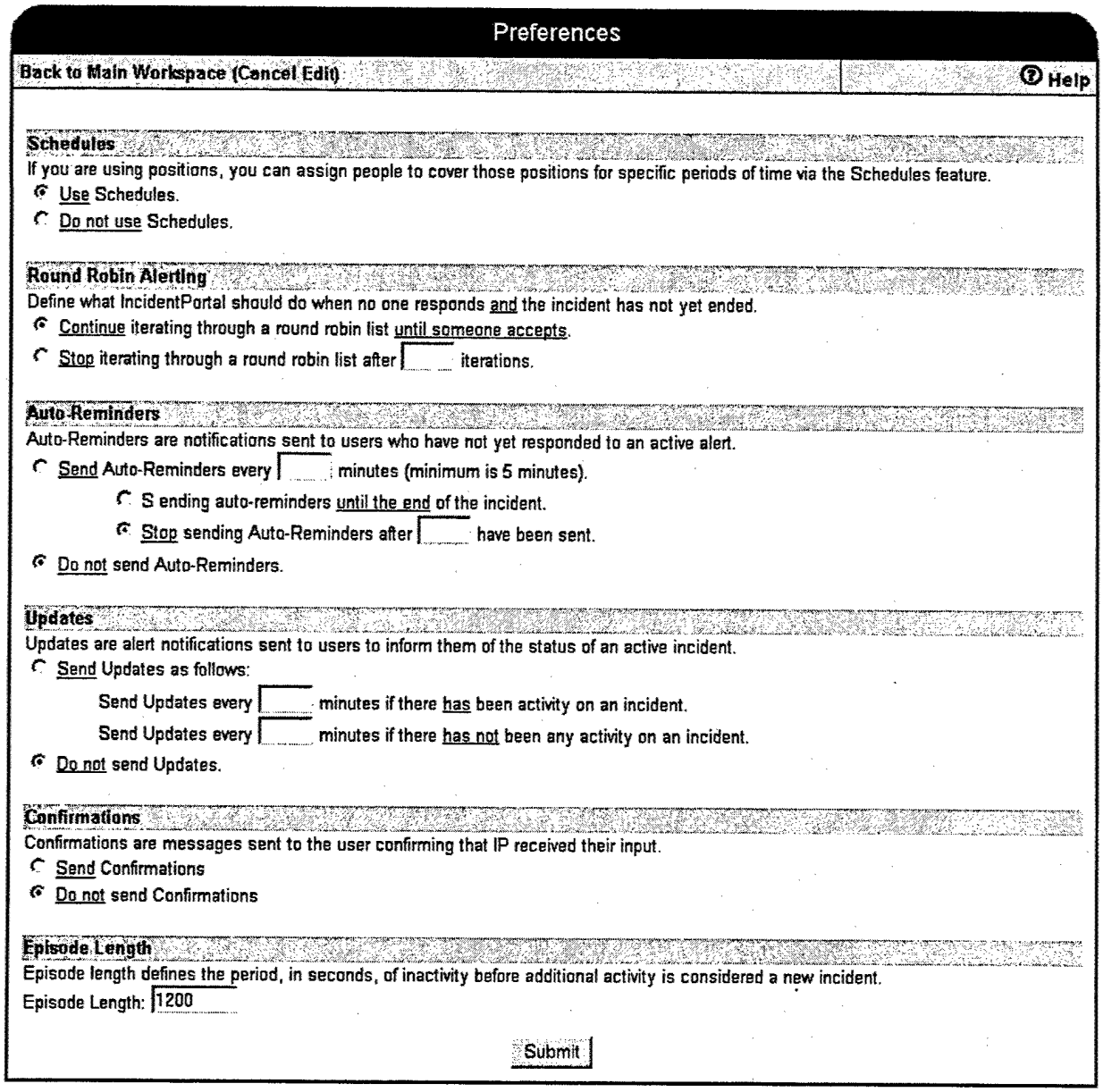


Figure 17. Form Defining the FASAT Preferences

Most of the parameters related to how often to update, when to remind, etc. are user-configurable and are set in the Preferences section of FASAT

4.3 The design must support follow-on analysis of the problem to verify that a correct decision was made and that the overall situation is proceeding in the expected manner.

FASAT supports users in their follow-on analyses of incidents. By monitoring all data at all times, FASAT continually tracks the status of any incident it identifies. With the FASAT Web portal, users can investigate the tracked incidents at any time. FASAT provides three key features to support this aspect of SA: (1) automated tracking of the status of alerts and responses, (2) automated reporting and updating of incident data, and (3) real-time collaboration tools.

4.3.1 Tracking of Alerts and Responses

FASAT automatically tracks when alerts are sent and responses are received back. It also tracks all rollovers and the status of incidents. All of this information is graphically displayed to the user (Figure 18).

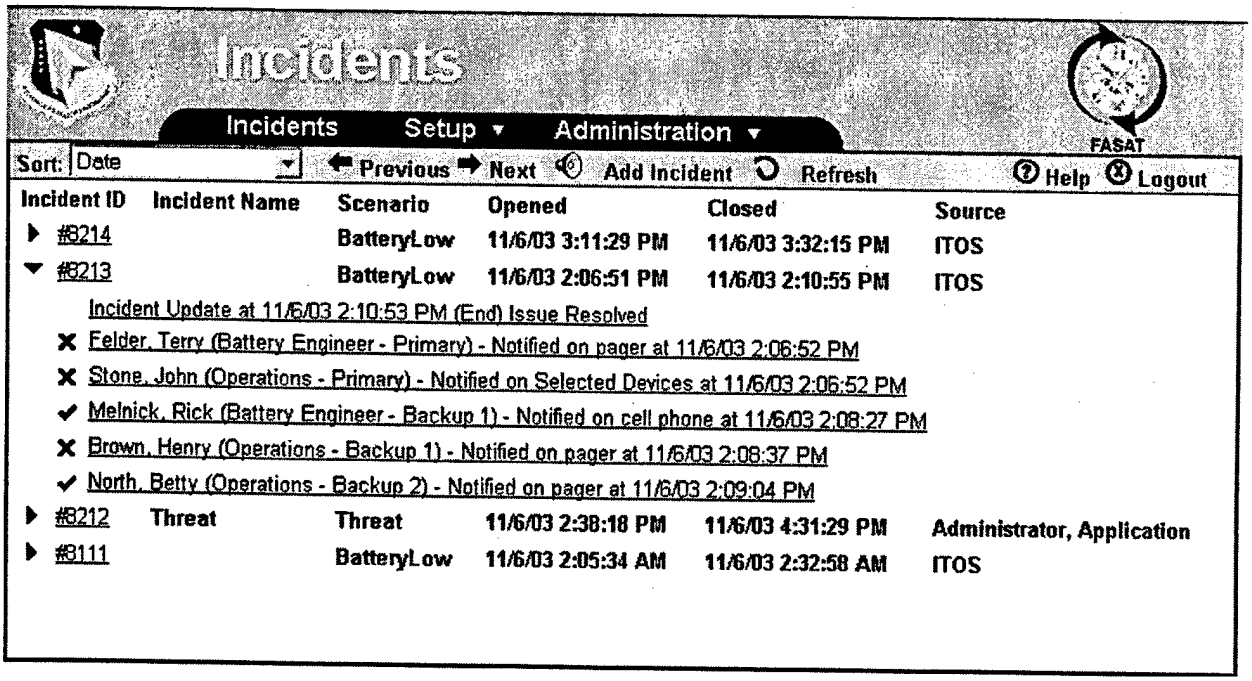


Figure 18. Incident Summary View of the Status of Incident #8213

If the user wants detailed information for any given alert, he/she can click on the alert from the view to display the Alert Notification screen (Figure 19), which displays:

- When the alert was sent
- How it was sent
- Any rollover across devices
- The response to the alert
- The content of the alert.

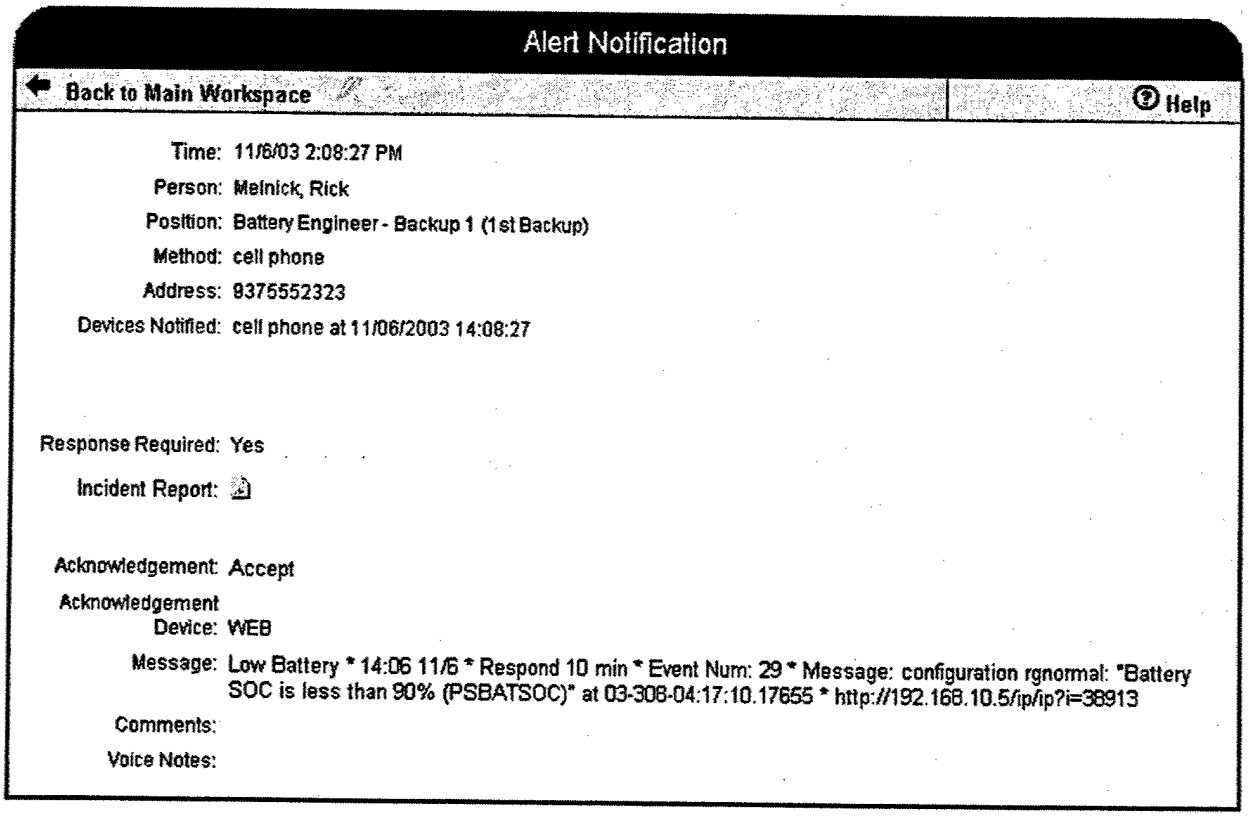


Figure 19. Form Showing Detailed Status and Content for an Alert Notification

4.3.2 Automated Reporting and Updating

FASAT automatically creates an Incident Report as soon as FASAT receives a trigger. That report contains background information (like the source of the data), as well as the actual data that triggered the event. Figure 20 shows a report. FASAT then automatically updates the report during the incident, as shown in the circled section of that same figure.

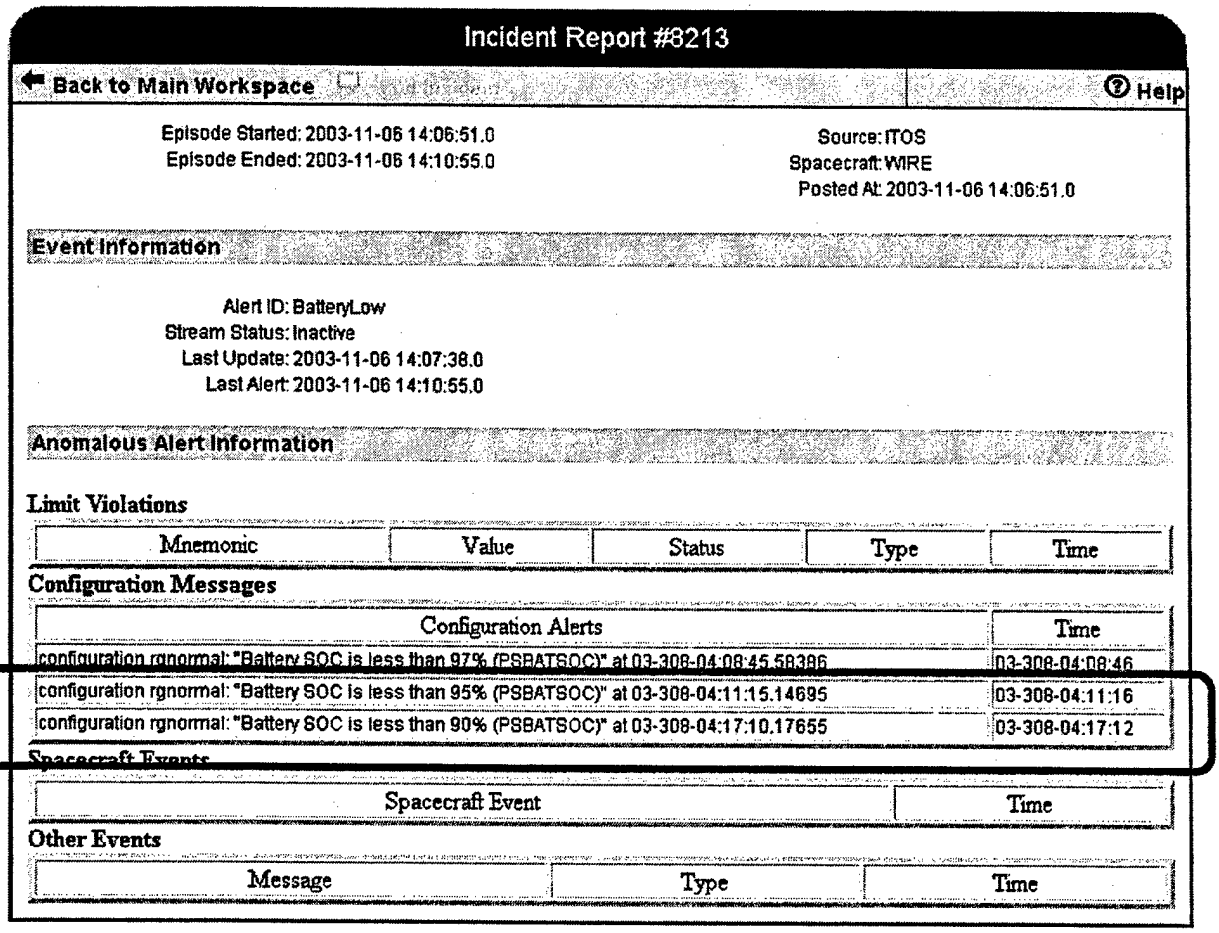


Figure 20. Updated Incident Report

4.3.3 Integrating Collaborations Tools

In Phase II, mFI integrated the Lotus Sametime real-time collaboration tool into FASAT (Figure 21). The collaboration tools are integrated as a window into the larger FASAT portal. In addition, mFI incorporated a single sign-on so that once users login to FASAT, they are automatically logged into Sametime. Though we chose to use Sametime for the Phase II effort, any Web-based collaboration could be integrated.

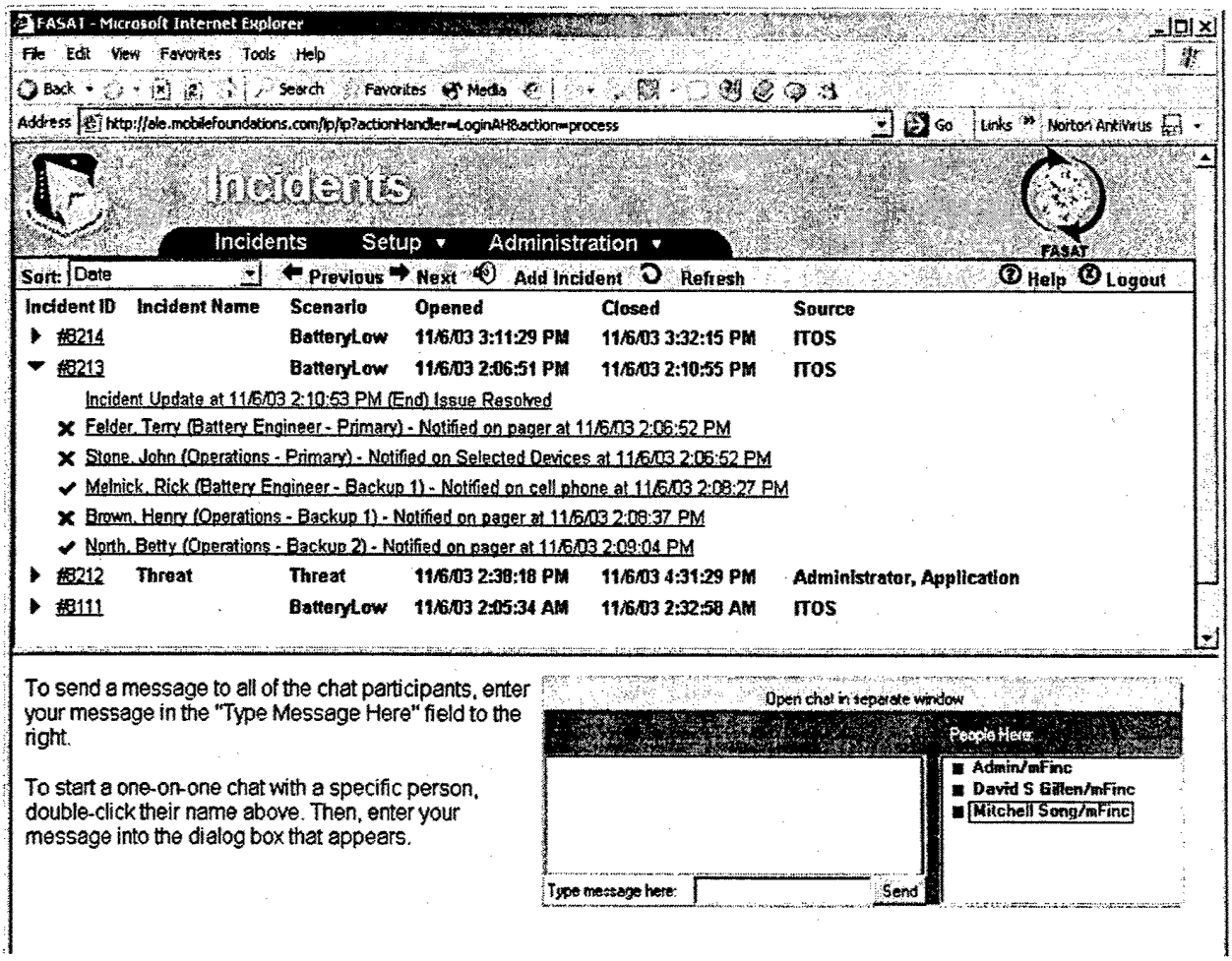


Figure 21. Incident Summary View with Embedded Real-Time Collaboration Window

In summary, FASAT provides a flexible and configurable interface that can meet individual users' information needs. FASAT facilitates each user's ability to access the appropriate mental model to develop an initial awareness of the situation. The closed-feedback loop from FASAT's portal to the responders' wireless devices keeps the responders informed and connected. FASAT also provides a range of information access and sharing tools that allow users to maintain SA when solving problems. Thus, through extensive research into Situation Awareness and designing to support SA, the *m*FI design team has crafted the options available and the displays of information in FASAT to help support users' development and maintenance of SA.

5.0 Design Methods

5.1. Alert Notification and Response Workflow Logic Charts

One of our early activities was to design the logic for FASAT's alerting process. Compared to a post-pass system (like SERS), the workflow process related to a near-rear-time system is much more sophisticated. Therefore, in FASAT, we added:

- Features for near-real-time alerting,
- Options for users to request additional data to maximize Situation Awareness (SA), and
- Additional notifications of the status of the operator's responsibility (e.g., notification when FASAT rolls over to the next contact).

The human effectiveness team led this effort. They provided input on what would help the users, based on the team's experience with: (1) SERS, (2) our Phase I SBIR effort, and (3) on initial feedback from a focus group of senior NASA operations staff. The team used flowcharts to represent the logic. The flowcharts allowed all the design team members to quickly understand the proposed logic and discuss improvements.

After each major iteration, the human effectiveness team led design review meetings with the PI and the software development staff. They also made suggestions for the FASAT logic to facilitate development. In addition, they provided information on system limitations (such as the amount of text allowed on pagers) that were critical to consider in FASAT's design. This process was particularly helpful in addressing two difficult problems:

- What the system will do if an operator does not respond immediately to an alert
- What options the system will provide for responses.

5.2 Use Cases

As part of the human effectiveness effort, mFI developed a series of "use cases." Each use case describes a situation of particular interest and how FASAT would work that situation. The use cases provided a variety of benefits. For example, they offered concrete examples of how users would interact with FASAT. This understanding was critical for both interface designers and for developers. Second, developing the use cases helped us identify issues we needed to address before we designed screens or wrote any code. Third, the use cases provide a good way for us to explain FASAT to new team members.

We developed the use cases by analyzing what FASAT should do once it identifies a problem. Based on our experience with NASA operators and our interactions with Air Force operators in Phase I, we determined how the users would likely want FASAT to operate. In creating the use cases, we considered issues such as:

- The type of data being monitored (continuous vs. state vs. discrete)
- The number of filters and data sources in a given scenario (one vs. many)
- The number and types of notification lists (a series of individuals vs. a whole group at once)
- The ways to determine the end of a scenario (e.g., Loss of Signal (LOS) vs. passage of time [episode] vs. manual input).

The use cases were very helpful in identifying issues that were not uncovered in previous design efforts (e.g., the flow charts) and those which needed further refinement. Several of the issues we identified and how we resolved them are described below.

5.2.1 Rollover Procedures

This involves (1) rolling over to the next device of one responder and (2) rolling over to the next responder. Although the flowcharts helped us make significant progress on this issue, the use cases revealed there were additional issues regarding notifications with multiple respondents.

5.2.2 Type of Data

FASAT would have to handle three types of data:

(1) Continuous data – where FASAT is monitoring streaming data, usually for situations where the variable goes above or below some pre-set threshold.

(2) State data – where FASAT receives information about the state of the system or component being monitored and stores that state until it changes.

(3) One-time events – which occur at a given point in time.

As a result of our analysis of the use cases, we determined that FASAT must maintain some state data (e.g., that a value went out of bounds and stayed out of bounds). Post-pass systems have no need for state data. To handle these state conditions, we developed a component to maintain that state information called the Incident Engine that is now an integral part of FASAT.

5.2.3 Updates and Accepting or Deferring Responsibility

We determined that users should not be able to request additional information (e.g., updates) before accepting or deferring responsibility for the alert since incidents occurring in a military satellite system are of enough consequence that they should be immediately addressed.

5.2.4 Timing of updates

Originally, we had planned for users to have one setting to simplify specifying the frequency of updates. However, in developing the use cases, we realized that users may want updates more frequently when there is activity than when there is not. Therefore, we determined that there should be two settings: one for the frequency of updates when there is activity, and another for when there is no activity. We felt that users would want the option of sending at least an occasional notification that nothing has changed, just so they are certain of the incident's status. This should help to improve situation awareness by keeping users informed of changes, but not overwhelming them with messages when nothing has changed.

6.0 Wireless Security

6.1 Introduction

A key element of FASAT is its alert notification and response functionality. When FASAT detects an incident, it can rapidly deliver alert messages to remote users on almost any commercial wireless data device. One of the major issues related to wirelessly transmitting mission critical data (e.g., a problem with a satellite) is the vulnerability the data. Unauthorized eavesdropping and device theft are just two of the many security vulnerabilities found with these types of devices. The good news is that as wireless technology continues to advance, the options for securing the devices and their data are advancing as well. This section of the report focuses on the potential security risks of using wireless devices, and steps that can be taken to mitigate or eliminate these risks. We have also provided recommendations to maximize productivity gain from these devices, while still being cognizant of various security risks, and military regulations and policies regarding wireless devices.

Note: In this section of the report on wireless security, some commercial products are named by brand. Those mentioned are done so for illustrative purposes. This section is not intended to be a comprehensive product survey. The inclusion of any product in this section is in no way an endorsement by mobileFOUNDATIONS or the U.S. Air Force. Nor do mobileFOUNDATIONS or the U.S. Air Force verify the performance of any product. This section should not be viewed as Federal policy.

6.2 What is Wireless Security?

When one thinks of wireless security, unauthorized eavesdropping usually comes to mind (e.g., a hacker using a RF scanner to "listen" to wireless airwaves). However, wireless security includes much more than just eavesdropping. DoD defines Information Assurance with five axioms [Pentagon Area Common IT Wireless Security Policy, Sept 2002, p2]: confidentiality, integrity, authentication, nonrepudiation, and availability. These can be described as follows:

- Confidentiality: Information is private and can only be accessed by the intended recipients. Confidentiality is usually accomplished with encryption techniques.
- Integrity: The information received is the same information originally sent. Integrity is often implemented using digital signatures.
- Authentication: The user accessing information is really the authorized user. Authentication is usually implemented using passwords, or some other challenge mechanism.
- Nonrepudiation: A user cannot deny sending or receiving information. This is often implemented using central logging or other monitoring techniques.
- Availability: Information and services are available when they are needed. The most common risk to availability is a "Denial of Service" attack against a resource.

When selecting wireless products or installing a wireless infrastructure, these five axioms should be considered at all times.

6.3. Specific Aspects of Wireless Security

As part of our research on wireless security, we thoroughly evaluated the impacts of security as related to:

- DOD requirements
- Specific vulnerabilities
- Impacts on specific types of devices (e.g., pagers) and the methods for securing them.

The details on the results of this work are presented in Appendix A of this document.

6.4. General Impacts of Using FASAT with a Wireless Security Mindset

As mentioned in the introduction above, a key element of FASAT is its alert notification and response functionality with commercially available wireless devices. When working with data that is unclassified and not sensitive, an organization is not necessarily limited by wireless security concerns, and can select a wireless device that provides the best features, capabilities, and coverage for their members. But when wireless security is required, it has several impacts on the organization.

A perceived impact might be the loss of choice an organization has when selecting a device for their members to use. But as described in Appendix A, there are secure wireless options for pagers and a variety of PDAs that have little or no impact on the way someone uses the device.

A real impact is the extra steps users will go through to access their data. They might be challenged more frequently to identify themselves, either by entering passwords or providing other information. Another impact is when users forget their passwords. When data gets

encrypted, the loss of a password sometimes means that the encrypted data can never be recovered. Backdoor schemes to unlock a locked device are handy in situations like this, but also detract from the total security scheme.

A final impact is the way information is sent, displayed, and stored on wireless devices. Regardless of the security schemes employed, an organization needs to decide how much data they wish to transmit to wireless devices. An organization might elect to configure FASAT to send minimal information to the wireless device, and rely on other, more secure means (like LAN-connected PCs), to get all of the FASAT incident data to the user. In this case, the user has an extra burden to go through a Web browser to get the information they need. Another organization might make a policy decision to store none of the data on the wireless device, due to risk of loss of the device. This creates an extra burden on the user to remember to delete messages after reading them.

However, in general, wireless security only minimally impacts the usage of FASAT. Users may perceive wireless security measures to be a nuisance, but in the end, users will still be able to accomplish everything in a secure, protected environment, as they could in an unprotected environment.

7.0 Conclusion and Future Work

In summary, FASAT represents the state-of-the-art in monitoring and alert notification for aerospace systems. It delivers the *right data* to the *right people* at the *right time, anytime* and *anywhere.* The technologies developed by mFI under this Phase II SBIR enable FASAT to monitor data from ground systems for user-defined events of interest. It can then log the data and distribute that data (via alerts) to any commercial wireless data device. It then autonomously monitors responses to the alerts (via wireless devices) and performs any rollover or call-down functions necessary to build the appropriately staffed team of on-call personnel. FASAT's architecture allows for the seamless integration of COTS collaboration tools so that the on-demand team can collaborate electronically. All told, FASAT represents the state-of-the-art in on-demand mission operations systems. In addition, FASAT technologies can be adapted to more general command and control environments.

The Phase II FASAT software can be viewed as a solid foundation on top of which additional command and control technologies can be layered. For example, logical follow-on activities of FASAT are:

- Conducting in situ usability analysis and testing of FASAT
- Designing advanced user interface concepts for visualizing the state of an incident.
- Adding an advanced decision support module that will provide FASAT with enhanced methods for determining alerting logic
- Integrating FASAT with non-space data sources

- Integrating other Collaboration tools.

In conclusion, the Fast Access Situation Awareness Toolkit is a set of capabilities that has the potential to assist the Air Force in modernizing and transforming Space Command space support capabilities to provide "...continuous deterrence and prompt global engagement for America and its allies ... through the control and exploitation of space" (*Air Force Space Command (AFSPC) Strategic Master Plan (SMP) FY04 and Beyond*).

8.0 Acknowledgements

We would like to acknowledge the support of the US Air Force Research Laboratory's Human Effectiveness Directorate. In addition to sponsoring this research, they were also partners in the success of this effort. In particular, we would like to thank Dr. June Skelly for her guidance and leadership throughout the Phase II effort, and Don Monk for his guidance in our Phase I effort and transitioning FASAT into the new domain of Air Force Space Operations.

9.0 References

Adams, M. J., Tenney, Y. J., and Pew, R. W. (1995). Situation awareness and the cognitive management of complex systems. *Human Factors, 37*(1), 85-104.

Air Force Space Command (2002). *Strategic Master Plan (SMP) for FY04 and Beyond.*

Air Force. (1999). *Air Force Instruction 33-106: Managing High Frequencey (sic) Radios, Land Mobile Radios, Cellular Telephones, and the Military Affiliate Radio System.* Supplement 1. November 5, 1999. Found at http://www.afmc.wpafb.af.mil/pdl/afmc/interg/33series/33-106/33010600.pdf.

Albers, M. (1999). Information design considerations for improving situation awareness in complex problem-solving. In the *Proceedings of the 17th Annual International Conference on Computer Documentation*, 154-158.

Albers, M. and Kim, L. (2000). User Web browsing characteristics using palm handhelds for information retrieval. *Technology and Teamwork, IEEE*, 125-135

Baker, P., Chu, K., Starr, C., Breed, J., Fox J., and Baitinger, M. (1997). Handling Emergencies in Autonomous Systems with an Episode-Incident-Alert Workflow. *2nd International Symposium on Reducing the Cost of Spacecraft Ground Systems and Operations*, Oxford, England.

Breed, J., Baker, P., Chu, K., Starr, C., Fox, J., and Baitinger, M. (1999). The Spacecraft Emergency Response System (SERS) for Autonomous Mission Operations. *The Third International Symposium on Reducing the Cost of Spacecraft Ground Systems and Operations*, Tainan, Taiwan.

Certicom. (2003a). *Extend Your VPN to the Wireless World.* Found at http://www.certicom.com/products/movian/movianvpn.html.

Certicom. (2003b). *Secure Data on Your Handheld Device.* Found at http://www.certicom.com/products/movian/moviancrypt.html.

Cingular. (2003). *User Information.* Found at http://www.cingular.com/beyond_voice/tm_user/

Commerce on the Move. (2000). *Privacy Concerns Plague Emerging Location Technology.* Found at http://www.telecomWeb.com/reports/cotm/lcommerce1.htm

DoD. (2002). *DoD Directive: Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG).* DRAFT 7/15/2002. Summarized at http://www.itaa.org/infosec/presentations/531.pdf.

Fox, J. A., Breed, J., Baker, P., Chu, K., Starr, C., and Baitinger, M. (1998). Web-based Emergency Response Systems for Lights Out Operations. *Proceeding of the Fifth International Symposium on Space Mission Operations and Ground Data Systems: SpaceOps 98*, Tokyo, Japan.

Fox, J. A., Donkers, A., Moe, K., Murphy, E., Pfister, R., Truszkowski, W., and Uehling, D. (1999a). User-Centered Design of Spacecraft Ground Data Systems at NASA-Goddard. *2nd International Symposium on Spacecraft Ground Control and Data Systems (SCD II)*, Foz do Iguaccu, Brazil

Fox, J. A., Gillen, D., Hoxie, M. S., Parkinson, C., Breed, J., Nickens, S., and Baitinger, M. (2000). New Human-Computer Interface Concepts for Automation in Mission Operations. *SpaceOps 2000*, Toulouse, France.

Fox, J. A., Starr, C., Chu, K., Baker, P., Breed, J., and Baitinger, M. (1999b). Web-based Automated Reporting: Saving Time, Money and Trees. *2nd International Symposium on Spacecraft Ground Control and Data Systems (SCD II)*, Foz do Iguaccu, Brazil.

Endsley, M. R. (2000). Theoretical underpinnings of situational awareness: A critical review. In M. R. Endsley and D. J. Garland (Eds.) *Situational Awareness Analysis and Measurement*. Mahwah, NJ: Lawrence Erlbaum Associates, Inc.

Endsley, M. R. (1995). Toward a theory of situational awareness in dynamic situations. *Human Factors, 37*(1), 32-64.

Fracker, M. L. (1988). A theory of situation assessment: Implications for measuring situation awareness. In *Proceedings of the Human Factors Society 32nd Annual Meeting.* 102-106.

Go America. (2001). *Go.Web OnPrem: Behind the Corporate Firewall Server Solution*. Found at http://www.goamerica.com/onprem.

Getgen, K. (2002). *Securing the Air: A Security Odyssey*. Found at http://www-106.ibm.com/developerworks/library/wi-sec2.html?article=wir.

Hammers Corporation. (2003). *The Integrated Test and Operations System (ITOS)*. http://www.hammers.com/ITOSTechBrief.htm.

Harris Corp. (2003). *Secure Wireless Local Area Network (SecNet 11™)*. Found at http://www.govcomm.harris.com/secure-comm.

Herbsleb, J. D., Mockus, A., Finholt, T. A., and Grinter, R. E. (2000). Distance, dependencies, and delay in a global collaboration. In *Proceedings of the CSCW Conference*, 319-328.

Hogan, M.O. (2000). *RSC and CERES SYSTEM DESCRIPTION: A GUIDE FOR CUSTOMERS AND USERS* (Aerospace Report No. TOR-2000 (1530)-1). Los Angeles, CA.

IT Asia One. (2001). *Authenticating Your Identity*. Found at http://it.asia1.com.sg/newsarchive/10/news005_20011015.html.

Marks, L. V. (2003). *The 802.11g standard – IEEE*. Found at http://www-106.ibm.com/developerworks/wireless/library/wi-ieee.html.

Mejdal, S., McCauley, M.E., Remington, R.J. (1999). *Advanced Interfaces for Space Operator Consoles*. Draft Final Report, prepared for Contract No. F41624-99-C-6016.

McNeese M. and Vidulich, M. (2002). *Cognitive systems engineering in military aviation environments: Avoiding cogminutia fragmentosa: A report produced under the auspices of the Technical Cooperation Programme Technical Panel HUM TP-7 Human Factors in Aircraft Environments (HSIAC-SOAR-2002-01).* Wright Patterson Air Force Base, OH: Human Systems Information Analysis Center.

Nofi, A. (2000). Defining and Measuring Shared Situational Awareness. *Center For Naval Analysis Report* CRM D0002895.A1/Final.

Palm. *Securing the handheld environment: An enterprise perspective*. Found at http://www.palmone.com/us/pdfs/securing_env.pdf.

Pentagon Area Common IT Wireless Security Policy, September 2002. Found at http://www.securitymanagement.com/library/Pentagon_Wireless0103.pdf.

Philippov, V. (2001). Pocket PC Password Protection. *Pocket PC Developer Network*. Found at http://www.pocketpcdn.com/articles/password.html.

Radding, A. (2001). Crossing the Wireless Security Gap. *Computerworld,* Found at http://www.computerworld.com/securitytopics/security/story/0,10801,55583,00.html.

Research in Motion (RIM). (2002). *Technical White Paper: BlackBerry Corporate Data Access.* Found at http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/7979/278390/BlackBerry_Corporate_Data_Access.pdf?nodeid=17286&vernum=0.

Research in Motion (RIM). (2003). *S/MIME Enhanced Blackberry.* Found at http://www.smimeblackberry.net.

Salas, E., Prince, C., Baker, D., & Shrestha, L. (1995). Situation Awareness in Team Performance: Implications for Measurement and Training. *Human Factors* 37 (1), 123-126.

Sectéra. (2003). *Sectéra Secure Wireless Phone for GSM.* Found at http://www.gd-decisionsystems.com/sectera/gsm/main.html.

Sheridan, T. (1980). Computer control and human alienation. *Technology Review*, MIT Press.

Trimble, S. (2000). NASA defends failures. *Federal Computer Week.* 14(7).

V-One Corporation. (2003). *Air SmartGate.* Found at http://www.v-one.com/air_smartgate.html.

Weill, N. (2001). Wireless Security Flawed, Researchers Report. *PC World.* Found at http://pcworld.com/news/article/0,aid,40442,00.asp.

Wi-Fi Alliance. (2003). *Wi-Fi is Everywhere: Wi-Fi Protected Access Web Cast.* Found at http://www.wifialliance.org/OpenSection/pdf/Wi-Fi_ProtectedAccessWebcast_2003.pdf.

Appendix A. Wireless Security in Detail

A.1 Current DOD Policies and Regulations

A.1.1 Pentagon Area Common Information Technology (IT) Wireless Security Policy – September 2002.

This document provides a point of reference on how the Pentagon has addressed wireless security concerns for their facility. The document includes a comprehensive set of policies to address the use of all types of wireless devices, including cellular telephones, pagers, and Personal Digital Assistants (PDAs). The full text of the document can be found at the following location: http://www.securitymanagement.com/library/Pentagon_Wireless0103.pdf. Some highlights from this document include:

- Wireless devices (cell phones, PDAs) are permitted "in areas where unclassified information is electronically stored, processed, or transmitted."
- Wireless devices may be used only for Unclassified data, Sensitive But Unclassified (SBU) data, or For Official Use Only (FOUO) data.
- Wireless devices are prohibited to be connected to classified networks or computers (example: putting a PDA in a "cradle" connected to a classified computer)
- Wireless devices cannot be used where classified information is electronically stored, processed, or transmitted un-encrypted, unless the device's Infra Red (IR), Radio Frequency (RF), and microphone/audio capabilities are disabled
- Wireless devices that store, process, or transmit DoD information must protect their data with a password protection scheme using a strong authentication, such as CAC,

PKI, or Biometrics. Without proper authentication, the device must be rendered inoperable automatically.

- Devices that store, process, and transmit DoD information must encrypt data using NIST FIPS-approved or NSA approved mechanisms.
- Devices and/or infrastructure should provide a means for intrusion detection and auditing, as well as mechanisms for monitoring.

In addition to these guidelines, the Pentagon also has a moratorium on new wireless technologies, effective July 30, 2001. Support for wireless devices and wireless technologies already in operation at the Pentagon can continue, but no new wireless infrastructures may be put into place during the moratorium.

A.1.2 DoD Directive: Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG). DRAFT 7/15/2002.

This document, although still in draft form, provides policies for the use of commercial wireless devices and services within DoD. Devices covered by this directive include commercial wireless networks, portable electronic devices, laptop computers with wireless capabilities, cellular/Personal Communication System (PCS) devices, PDAs, and any other Portable Electronic Device (PED) capable of storing, processing, or transmitting information. A summary of this document can be found at http://www.itaa.org/infosec/presentations/531.pdf. Highlights of the document include:

- Identification and Authentication (I&A) must be accomplished with strong authentication, using a scheme in accordance with the DoD PKI schedule. I&A shall be implemented at both the device and the network level.

- Unclassified data will be encrypted for transmitting to and from wireless devices. Data must be encrypted using an end-to-end scheme that meets FIPS 140-1 or 140-2. It must meet the Level 1 or Level 2 (Triple-DES or AES) standard at a minimum.
- Devices must use file system encryption.
- Classified information can be transmitted using NSA approved encryption.
- Classified data stored on a PED must be encrypted using an NSA approved Type 1 encryption consistent with storage and treatment of classified information.
- Wireless devices may not be operated within a Sensitive Compartmented Information Facility (SCIF), whether permanent, temporary, or mobile.
- Wireless RF technologies or devices that store, process, or transmit information cannot be used in areas where classified information is stored, processed, or transmitted, without approval by the Designated Approving Authority (DAA).
- PEDs that are connected directly to a DoD wired network (example: in a cradle connected to a PC) may not operate wirelessly at the same time.
- Wireless Personal Area Networks (WPAN) and/or Wireless Local Area Networks (WLAN) may only be used for unclassified information if a FIPS 140-1/2 scheme is used. These technologies can be used for classified information only using NSA approved technologies.

A.1.3 Air Force Instruction 33-106: Managing High Frequencey (sic) Radios, Land Mobile Radios, Cellular Telephones, and the Military Affiliate Radio System. Supplement 1. November 5, 1999.

AFI 33-106 is a directive for Air Force bases to identify how each base will manage high frequency radios, cellular telephones (CT), and land mobile radios (LMR). The document

implements AFI 33-106 at Wright Patterson Air Force Base. While not as comprehensive as the previous documents sited, this document includes the following guidance:

- Cellular Telephones (CT) are not recommended for use in environments where classified, sensitive, or critical information may be inadvertently overheard and transmitted.
- Cellular secure telephone unit III (STU-III) should be used only when time constraints prevent the use of other secure telephone means.
- NSA/NIST approved devices should be used to secure classified traffic, or to protect unclassified information relating to national security.

A.1.4 Summary

One common theme among all of the documents described above is that they intentionally leave out recommendations for specific products or technologies, probably at the risk of making them seem like product endorsements. The next few sections attempt to examine each of the different wireless device types and specific technologies related to each.

A.2 State-of-the-Art for Securing Today's Wireless Devices

This section addresses each of the common commercial wireless devices available today, and discusses the state of the art techniques for addressing the wireless security concerns for each. This discussion will focus primarily on the interactions between wireless devices and an mFI application, primarily wireless data transmission, processing, and storage.

A.2.1 Cellular Phones

Cellular phones are more than just telephones. Cell phones are also capable of sending and receiving text messages, browsing the Internet using embedded Web browsers, and acting as a conduit for other devices (like laptop computers) to connect to the Internet from remote places. Some cell phones also have built-in Personal Digital Assistants (PDAs), and are capable of storing and processing large amounts of data. A discussion of data storage will be included in the PDA section, later in this document. The primary issue for cell phones is the transmission of data.

There are two primary mechanisms for transmitting data to and from a cell phone: short message service (SMS), also known as text messaging; and wireless Web browsing over a commercial data network (such as CDPD, CDMA, GPRS).

SMS

Short message service (SMS) is a mechanism for sending short messages to cell phones. SMS messages are usually limited to between 100 and 150 characters, depending on the device and the carrier. SMS is the easiest way to "push" information to a cell phone. Unfortunately, commercial carriers do not guarantee the delivery of SMS messages, so it is possible for SMS messages to not be delivered in a timely fashion, if even at all (e.g., Cingular, 2003). Also, there is no mechanism for securing the contents of an SMS message with encryption or any other means.

Wireless Web Browsing

Wireless Web Browsing via a cell phone is becoming easier as devices mature. Cell phones are being equipped with larger screens, allowing more visible content and greater usability. Web

browsing is a "pull" mechanism for users of wireless devices to go and fetch the information they are looking for. The most common mechanism for cell phones to retrieve information and transmit it to the phone is via the Wireless Application Protocol (WAP). WAP provides a set of standards for devices and carriers to allow micro-Web browsers to interoperate. WAP also provides standards for security, but the security solutions for WAP are often not sufficient for sensitive data. This is due to the "WAP Gap". The WAP Gap is a split second where transmitted data is unencrypted and available "in the clear". The WAP Gap exists because different encryption schemes exist for transmitting data over the wired Internet (Secure Sockets Layer - SSL), and for transmitting data using the WAP protocols (Wireless Transport Layer Security - WTLS). Although the gap is brief, and usually only exists within the memory of a computer system and no data is written to any persistent storage, the gap still exists (Getgen, 2002).

There are solutions to the WAP Gap today, but they are either relatively expensive, or they provide a burden to the organization wishing to implement the solution. One common solution is for an organization to procure and manage its own WAP Gateway behind its own corporate firewall. This solution allows an organization to be in complete control of the machine where the WAP Gap occurs, thus reducing the risk of an outside individual compromising the data during the Gap.

On the near horizon, a future version of WAP, version 2.0, incorporates Transport Layer Security (TLS) as an end-to-end security scheme. This allows the Web server to encrypt the network traffic using TLS, similar to how it does it with SSL today with wired Web browsers. The micro-browser in the phone will be able to decrypt the TLS messages directly, with no gateway in between to do any translations. Unfortunately, moving to WAP 2.0 requires upgrading older

handsets, and ensuring new handsets and respective carriers are WAP 2.0 compliant (Getgen, 2002).

Another solution is to install custom software onto the phone to achieve end-to-end encryption with an application server. When an application handles the security, the underlying transport layer does not need to be secure. While this achieves full end-to-end security, it is often not practical to do so, due to the limited resources available on a cell phone. Cell phones are almost like computers with small amounts of memory and a CPU that is optimized for certain functions. Unfortunately, encryption algorithms are rather complex, and require more resources than are usually available on such a device (Radding, 2001). As cell phones become more powerful, and have more capabilities, this may become a more viable option. See the discussion below about Hybrid Cell Phones/PDAs for more information on this topic.

Another option is to use a Sectera cell phone, which has been approved by the NSA for use in classified environments. The Sectera phone is a Motorola Timeport that has been modified to use Type 1 encryption for both voice and data communications. This phone could be used to exchange classified data with other Sectera devices (wireless and wireline) that support Type 1 encryption (Sectéra. 2003).

A.2.2 Two Way Pagers

Pagers were one of the earliest types of wireless devices. The early pagers only allowed a sender to transmit a series of numeric digits to a recipient's device – the numeric digits were typically a phone number. As pagers evolved, they allowed for alphanumeric messages to be sent to the pager. The latest pagers now allow for responses (replies) sent from the pager back to the sender, allowing the recipient to acknowledge the receipt of the page, to answer a simple

question, or to perform some other function. Also, advanced pagers allow users to send and receive email.

In the United States, there are four prominent network carriers that provide access to two-way paging services: Skytel, Arch Wireless, Weblink Wireless, and Metrocall. Each of these carriers supports one or more of the following protocols for sending a message to carrier's network center: WCTP (Wireless Communication Transfer Protocol), SNPP (Simple Network Paging Protocol), or SMTP (Simple Mail Transport Protocol). Many of the carriers also support TAP (Telelocator Alphanumeric Protocol), but this protocol is not a two-way protocol. We will not discuss this protocol here since mFI utilizes two-way paging technology in its applications to allow users to acknowledge the receipt of their pages.

A message to a pager typically consists of three pieces of information: the actual message content, a pager PIN number to designate the recipient, and a designation of how the response from the pager can be routed back to the originator. Each protocol listed above has a different way of packaging this information for transmission to the carrier's network center. Each of the protocols transmits the information over the Internet (TAP uses a phone line – another reason mFI solutions probably will not). Upon receipt of the message, the carrier validates the message, then queues the message for delivery to the pager. Upon successful delivery, the recipient views the message and can reply to the message. Any reply to the message is routed back to the carrier's network center, where it is then forwarded back to the sender of the message.

By default, the transmission of the message over the Internet to the carrier's network operations center is not encrypted – the message is sent "in the clear." Additionally, the wireless transmission of the message to the pager is not encrypted; many devices lack the capabilities to

perform encryption/decryption functions. Traditionally, because of this vulnerability, pagers are not used for sending sensitive information. However, specific carriers have introduced solutions that can enable some level of security for transmitting messages as described below.

An additional vulnerability is the loss of a pager. If a pager falls into the wrong hands, any new messages, as well as the contents of any previous pages stored on the device, could be accessed and read by someone else. This is because most pagers lack the capability for password protecting access to stored messages, or authenticating the current user when reading new messages.

The following sections discuss a couple of specific solutions designed to address these vulnerabilities. These solutions include:

- Skytel Secure Protocols
- V-ONE Air Smartgate®

Skytel Secure Protocols

As discussed earlier, messages transmitted across the Internet using WCTP or SNPP are sent in the clear. Skytel accepts these unencrypted messages, but also has special "listeners" setup to receive messages encrypted with SSL.

Encrypting the messages with SSL as they are transmitted over the Internet provides some level of security against someone using a network packet analyzer to intercept a message in transit. However, since the message is decrypted at the Skytel network center, and then transmitted in the clear over the airwaves, this solution does not provide an end-to-end secure channel. This type of security might be sufficient for certain applications.

Response messages can also be encrypted with SSL. WCTP and SNPP can use a polling mechanism, meaning the mFI Messaging Gateway periodically connects to Skytel to look for pending response messages. If the initial connection to Skytel is made with an SSL-encrypted WCTP or SSL-encrypted SNPP session, the response messages will be transferred back to mFI via the encrypted channel.

As of the writing of this document, no other carriers allow for secure connections to be made to their network centers for secure transmission of messages.

V-ONE Air Smartgate

Air Smartgate is a product by V-ONE (a subsidiary of FirstVPN) that permits secure, end-to-end encrypted paging. Messages are routed through an Air Smartgate server (located within an organization's firewall), which encrypts the message and transmits the message to the paging carrier. The carrier then transmits the message to the pager, which has special software loaded on it to decrypt the message. Any reply messages are also routed through the secure channel. The paging carrier never decrypts the contents of the message.

Air Smartgate also authenticates the sender and recipient of all messages. This ensures that only an authorized recipient can read the message, and the recipient is assured that the sender is legitimate. This product was used for secure paging at the Salt Lake City Olympics in 2002 (V-One Corporation, 2003).

A.2.3 Pocket PC and Palm OS® Based Personal Digital Assistants

A Personal Digital Assistant (PDA) is a handheld device, most commonly used to store calendar "to do" items, and perform email operations. The first PDAs were typically used in offline

settings, where a user would synchronize the information between their PDA and their desktop PC, then disconnect the PDA and go work disconnected from any other machines or networks. The more PDAs were used, the more types of information people would store on them. Securing this information became a challenge, since the loss of a PDA would mean the compromise of information stored on it.

The next generation of PDAs can be used in offline settings like those described above, but they can also be configured to use wireless receivers in the PDA to have continuous network connectivity while still disconnected from any other PCs. This gives the PDA user much more flexibility, but also makes the task of providing security to the device more complex. The next aspect of security relates to the transmission of the data.

Data Protection

Both Palm OS and Pocket PC have built in functions to require a password to be entered to "unlock" the device before you may use it (Palm; Philippov, 2001). This type of security function may deter a casual user from snooping, but a serious hacker can gain access to the memory of these devices because all data is stored unencrypted within the device. To prevent a hacker from compromising the contents of the device, a solution that incorporates authentication with confidentiality is required.

For both Palm OS and Pocket PC PDAs, there are a variety of commercial products that allow you to encrypt data on a device. For example, Certicom has a product called movianCrypt™, which provides strong encryption on Pocket PC and Palm OS devices. It uses 126-bit AES encryption, and has been validated for FIPS 140-2 (Certicom, 2003b).

New technologies are emerging to allow different forms of authentication techniques for PDAs. Traditional authentication techniques involve entering a password. Unfortunately, a very complex encryption scheme can be easily defeated if the user selects a password that can be guessed easily. Advanced authentication techniques involve using biometrics, handwriting analysis, and voice analysis to provide more authoritative results (IT Asia One, 2001). However, an advanced authentication scheme without a data encryption component provides little value. If a hacker is able to bypass the authentication scheme, the device still needs to protect the data on the device. Fortunately, most implementations of strong authentication take this into account.

Data Transport Protection

A PDA with a wireless network adaptor can provide users with access to data at any time from any place there is coverage for that adaptor. A PDA with network access uses the same network protocols that a desktop PC would use, such as HTTP with TCP/IP. Although SSL is often supported on PDA devices, not all Websites support SSL. Also, a PDA user on a commercial wireless network may want to access a resource internal to the organization's firewall. The best solution for this is a VPN connection.

A VPN connection provides multiple benefits to the user and the organization. First, the channel between the PDA and the organization's network is encrypted. Second, VPN often provides strong authentication techniques, such as requiring a smartcard or using PKI, so an organization's assets are better protected. For example, Certicom provides movianVPN™, which is a VPN client for Palm, Pocket PC, and Symbian OS PDA devices. Their solution has been certified to be FIPS 140-2 compliant (Certicom, 2003a). In addition to Certicom, there are other VPN solutions available for PDA devices.

One important consideration with VPN solutions is that authentication is usually done for the individual using the device, as opposed to the device itself. This means that if a device is lost or stolen, and a password was compromised, a system administrator cannot restrict the device from connecting to the VPN server. VPN solutions that are based on PKI authentication schemes are preferred since they require more than just knowledge of a password.

With a VPN solution, data is decrypted behind an organization's firewall. End-to-end security is maintained while the data travels over the wireless space, but the data is not end-to-end encrypted between the device and the application server the user is ultimately communicating with. This kind of end-to-end security must be accomplished using a specific application's end-to-end security means, such as using SSL between a Web browser and a Web server.

A.2.4 Hybrid Cell Phones/PDAs

Devices with PDA technology incorporated into a cell phone have the challenges of protecting both a cell phone and a PDA. Fortunately, the solution is not as complex as it may seem. Although the device has cell phone capabilities, most application functions are performed through the PDA, using the cell phone data network as the network layer. This provides two advantages over using a cell phone without a PDA. First, applications for a PDA can include application layer security, since the PDA device has more capabilities than a non-PDA cell phone. Second, you can apply a VPN connection, so all network traffic, regardless of application or protocol, becomes encrypted. Thus, the PDA capabilities allow the cell phone to function more easily in an end-to-end encrypted fashion, than a cell phone without a PDA.

A.2.5 Blackberry PDA

The Blackberry™ PDA is being treated separately from other PDAs because of some unique characteristics of the device, the technology behind the device, and a unique relationship between Research in Motion (RIM), the makers of the Blackberry, and the National Security Agency (NSA).

The Blackberry PDA is an "always on" device that is always connected to the wireless network. The device gained popularity with mobile users looking for efficient ways to have new email messages "pushed" to them while away from the office. However, the Blackberry can be used for much than just reading email. Some Blackberry devices support Internet Web browsers for easy data access from anywhere there is coverage, and have support add-on custom applications, such as sales force automation tools.

Fundamentally, the Blackberry PDA has the same security related issues as other PDAs do, but the Blackberry has a different set of solutions.

Data Protection

The issues relating to protecting data stored on a Blackberry are the same as the issues for protecting data stored on a PDA. The solutions are also similar to those for other PDAs, with the notable exception of the S/MIME Enhanced Blackberry (see description of this device below).

One interesting feature the Blackberry devices have is an automatic memory erase feature if too many password attempts are tried. For the Blackberry, if ten bad password attempts are tried in a row, the Blackberry automatically deletes all user data on the device.

Data Transport Protection

The Blackberry is an "always on" device, and has network connectivity built-in to the device, unlike other PDAs which do not always have built-in networking capabilities. The Blackberry comes in two types: an Internet edition (like a Personal edition), and an Enterprise edition. The Internet edition uses commercial wireless networks (like Mobitex or DataTAC) to connect to commercial wireless gateways which then connect you to Internet resources. The Enterprise edition, when used with a Blackberry Enterprise Server, uses commercial wireless networks to connect securely with the Blackberry Enterprise Server at your organization via a commercial wireless gateway (RIM, 2002). This discussion will focus on the Enterprise edition, since that is the version that supports encryption.

The Blackberry Enterprise Server (BES) complements the Blackberry PDA by providing end-to-end security between the wireless device and the BES. The BES acts as a secure conduit for email messages, and integrates seamlessly with Microsoft Exchange or Lotus Domino mail systems. It also acts as a secure wireless gateway, permitting Triple-DES encryption between the Blackberry PDA and the BES. Additionally, the Web browser embedded in the Blackberry PDA includes support for SSL, so all network traffic between the Blackberry PDA and an application Web server can be end-to-end encrypted (RIM, 2002).

Organizations with Blackberry PDAs and Palm/Pocket PC PDAs

In many respects, the Blackberry Enterprise Server is analogous to using a VPN connection with other PDAs. The capabilities are very similar, and the security benefits are virtually identical. However, the two technologies mentioned above (VPN for non-Blackberry PDAs and BES for Blackberry PDAs) are not compatible with each other. A BES can only be used with Blackberry PDAs, and there are no VPN clients for a Blackberry.

Fortunately, there are third party tools that can protect the transport of data over wireless networks from both types of devices. These tools perform end-to-end encryption between a wireless device and a machine behind the corporate firewall, using a scheme similar to VPN or a BES. One solution is from GoAmerica, called Go.Web OnPrem. An organization installs a Go.Web OnPrem server behind their firewall. The organization's wireless devices are configured to tunnel all network traffic through the Go.Web OnPrem server using Triple-DES encryption. The Go.Web OnPrem server behind the firewall then decrypts the request, acts as a proxy for the user to fulfill the user's request, re-encrypts the data response, and sends the encrypted data back to the device (Go America, 2001).

S/MIME Enhanced Blackberry

Research in Motion (RIM) manufactures a special Blackberry PDA, the 957-8MB, also known as the S/MIME Enhanced Blackberry or the "Cryptoberry." This one-of-a-kind device is the only wireless device currently approved by the NSA. It is the only wireless device to provide true writer-to-reader security for wireless email, and has been approved to protect up to sensitive but unclassified (SBU) / For official use only (FOUO) email. This device complies with the DoD Public Key Infrastructure (PKI) policy and the DoD Overarching Wireless Policy (RIM, 2003).

The S/MIME Enhanced Blackberry is basically a RIM 957 PDA with extra memory and a special version of the Blackberry operating system. These upgrades permit the device to be used to send S/MIME email (Secure/Multi-purpose Internet Mail Extension). S/MIME is a certificate based extension to email that provides writer-to-reader security, including confidentiality, message integrity, and non-repudiation. The S/MIME Enhanced Blackberry can only be used for email – all other functions of the device have been disabled. Even the use of file attachments in

email, normally supported by the Blackberry PDAs, is disabled on the S/MIME Enhanced Blackberry.

The S/MIME Enhanced Blackberry system uses a Blackberry Enterprise Server to communicate between an organization's email system and the wireless devices. But since S/MIME is used by the sender of an email message and by the user of the Blackberry device, data is encrypted at the source, and decrypted at the recipient, providing true end-to-end encryption. This addresses the NSA's concern about an internal attack on a BES.

The S/MIME Enhanced Blackberry is also compatible with the Common Access Card (CAC), a Smartcard distributed to DoD personnel for maintaining keys for the DoD PKI system.

The S/MIME Enhanced Blackberry is an example of a third-party manufacturer working closely with the NSA to design a device to meet the strictest of wireless security standards. Hopefully, more vendors will take this route to develop truly secure wireless devices.

A.2.6 802.11

IEEE 802.11 is the Working Group for Wireless LANs. This working group has defined a number of standards for Wireless LANs. The most notable standard is 802.11b, also known as Wi-Fi. Wi-Fi networks are appearing everywhere: at offices, at homes, at coffee shops, airports, and hotels, just to name a few. This section focuses on the wireless security implications of using an 802.11 Wireless LAN.

There are many different types of devices that can connect to an 802.11 wireless LAN. These include traditional computing devices like desktop PCs, laptops, and PDAs. But with the popularity of 802.11, other types of devices can connect too, including home appliances and

MP3 music players. Like other wireless technologies, the data transmitted across a wireless 802.11 network must be protected properly. This document will focus on transmitting data on an 802.11b wireless LAN.

Wireless security was part of the 802.11b standard from the beginning. 802.11b network cards and access points can be configured to use the Wired Equivalent Privacy (WEP) encryption standard. WEP is optional in 802.11b, and is not always used. WEP implementations provide either 40-bit, 64-bit, or 128-bit encryption key. This key is common to all wireless cards and access points on a given 802.11b LAN, and each device must be manually configured with the key to allow connectivity to take place.

When 802.11b became a standard, it was known that WEP had certain limitations, but it was the best available at the time. WEP has since been proven to be inadequate for securely protecting data sent on the wireless LAN (Weill, 2001). WEP should still be used, since it does provide other benefits, like preventing rogue devices from connecting to a protected 802.11b network. But the best hackers with the right tools can exploit the weaknesses in WEP and are able connect a device to a WEP protected 802.11b network. Other data encryption mechanisms need to be used to properly protect the data.

The easiest way to securely protect network traffic on an 802.11b network is to utilize a VPN product. As mentioned earlier, a VPN product creates a secure conduit between the VPN client and the VPN server, which is presumably behind an organization's firewall. This conduit covers the entire wireless path the data must take, and thus protects the data across the wireless path. Additionally, VPN software can be configured to take advantage of an organization's PKI infrastructure.

The 802.11 working group has released a new standard called Wi-Fi Protected Access (WPA). WPA is actually a subset of 802.11i, which is being made available for 802.11b equipment. WPA fixes all of the weaknesses with WEP, and enhances key management that is lacking with WEP. Many 802.11b products available today for WEP encryption are flash-ROM upgradeable to support WPA, providing network administrators an easy migration path. However, even with the promise of WPA, corporate policies may dictate the additional use of a VPN solution to provide a higher level of security or for stronger authentication, such as utilizing PKI (Wi-Fi Alliance, 2003).

Another solution is to use products developed by the Harris Corporation. Harris Corporation has developed SecNet 11™, a Secure Wireless Local Area Network (SWLAN) product that has been certified by the NSA for use in classified environments, to the Secret level. Special network cards and access points can be used to transmit data encrypted using Type 1 encryption (Harris Corp, 2003). Standard 802.11b cards and access points are not compatible with those made by the Harris Corporation.

802.11a has all of the same issues as 802.11b, and some vendors are providing flash ROM upgrades to 802.11a devices to add WPA to fix the problems in WEP (same solution as 802.11b).

802.11g has WPA built into it, so it is inherently more secure than 802.11b. One of the benefits of 802.11g is that 802.11g is backwards compatible with 802.11b, so 802.11g networks can be setup to allow both 802.11b and 802.11g devices to connect to each other. Unfortunately, when 802.11g devices interconnect with 802.11b devices, the network is reduced to support the lower

standard of 802.11b, which doesn't include WPA. A WPA environment is not truly secure until all devices are 802.11g devices (Marks, 2003).

A.3 Location Based Services

One of the new buzz phrases heard with many cellular phone carriers is "location based services." These services have drivers from two different areas: public safety and corporate marketing. For public safety, there is a requirement by the FCC for 911 dispatch centers to be able to determine the location of a 911 caller who is using a cell phone. Cellular phone carriers have put equipment into place to pinpoint a caller's location, and relay that automatically to the 911 dispatch center. This equipment usually relies on triangulation between different cellular towers, or it could utilize GPS technology. For corporate marketing, the vision is that as a person walks past a store front, their cell phone could beep alerting them of a special offer inside the store. Corporations would pay cellular carriers to have these messages be sent to users' phones when they are within a certain range of their store.

The bottom line is that regardless of whether you are using your device or not, the network carrier knows where you are located. As long as your device is turned on, your device is in semi-continuous communications with one or more towers, and the carriers can track where you are located. And this technology extends beyond cell phones to pagers and PDAs also.

What if a hacker was able to also track where your device is? A lot could be gained by knowing if several of high-level officials were all at the Pentagon at 3:00 am.

Some network carriers allow their users to opt-in to location based services, and also allow them to opt-out of them when they want to. Allowing users to opt-out of these location services tells

the device to stop sending location-based information to the carriers, giving the device owner more control over what information is sent from their device at different moments in time (Commerce on the Move, 2000). It is important to be cognizant that these capabilities exist, and to see how they might affect the security requirements of an organization.

A.4 Conclusions and Recommendations

There are a lot of choices that face an organization when it comes to selecting a wireless communications product and/or technology. Each has its benefits and drawbacks, strengths and weaknesses. Through our own experience in the field of wireless devices, based on the current DoD regulations, and based on the characteristics of various wireless devices, mFI presents the following conclusions and recommendations for the Air Force in considering the procurement of wireless devices for use with mFI's software.

A.4.1 Working with Classified Data

When working with classified data, choices are limited. Only devices approved by the NSA and perform Type 1 encryption can be used. This limits the choices to the Sectera model of cell phones, or the Harris Corporation line of 802.11b products. The other alternative is to use a more proprietary self-contained Land Mobile Radio (LMR) system that handles Type 1 encryption.

A.4.2 Working with Sensitive but Not Classified Data

In the non-classified world, there are many more choices for working with data in a wireless environment. Often, there are factors other than security to consider when selecting a product.

The following sample of commercial products/capabilities address wireless security issues in an equivalent fashion:

1. Using 2-way pagers with V-ONE's Air SmartGate
2. Using PDAs with strong authentication and encryption, plus a VPN solution
3. Using a Blackberry with a Blackberry Enterprise Server
4. Using 802.11 wireless device, plus a VPN solution

Each of these methods provides a secure end-to-end tunnel for data between a wireless device and a corporate infrastructure. V-ONE uses a 128 bit RC4 encryption algorithm. VPN solutions typically use AES, Triple DES, IPSEC, and/or RC4. The first three schemes allow devices roaming on commercial wireless networks to have secure two-way channels back inside a corporate firewall, without compromising any of the flexibility of using these devices. The fourth scheme allows wireless devices on a local 802.11b corporate network to exchange data securely, without the risk of compromise by a hacker attempting to infiltrate the 802.11b network.

Air SmartGate encrypts messages locally on the pager. For the second scheme, using strong authentication and encryption, like Certicom movianCrypt, protects the data on the device and restricts access to authorized users. For the third solution, the optional S/MIME extension locally encrypts messages on the Blackberry using PKI. Without this S/MIME extension, the default protections of the Blackberry would be used to protect locally stored data. For the fourth scheme, a suitable product should be used to protect the data on the wireless device.

Note that using PDAs with or without cell phone voice capabilities is equivalent in this configuration. A PDA with a built-in cell phone will use the cellular data network as the network transport. A PDA without a built-in cell phone will require access to some other commercial data network, such as CDPD, CDMA, or GPRS. But the security benefits provided by the authentication, encryption, and VPN solution will apply universally across all configurations.

Using any of these schemes, users will notice little impact when using FASAT with sensitive data vs. using FASAT in a non-sensitive data environment, except the user may have to enter extra passwords to establish extra connections (like VPN) to decrypt messages sent to them. Using any of the schemes listed above, full FASAT functionality will be available to users.

A.4.3 Where does this leave cell phones?

Cellular phones are probably the most common wireless device seen on the market today. Some of the security flaws in cellular phones lie with cellular carriers, while others lie in the devices and in the technology itself. SMS has no guaranteed delivery provision, so it cannot be relied upon for mission critical applications. Wireless Web browsing lacks an end-to-end security mechanism, unless a certain trust is placed in the cellular carrier that they will not exploit the WAP Gap. Future versions of WAP will eliminate the WAP Gap. Until then, cellular phones should probably not be used for mission critical applications or for applications where end-to-end security is a major concern.

However, organizations often justify cell phones for their employees because the device owner can get the most bang for their buck, having everything in one device. If a user chooses to use FASAT in an environment with an emphasis on wireless security, and a user wishes to use a

cellular phone as their notification device, the user might be negatively impacted with some usability constraints.

Fortunately, FASAT is very flexible, and attempts to overcome these constraints as much as possible. mFI's software has the ability to contact a user on a variety of devices, using rollover schemes. mFI recommends that if an organization wishes to use cellular phones, they should send notifications to the device that minimize the amount of information sent. For example, transmit only a URL or an id code that can be used to reference the Incident. They should configure mFI's software to send the notification first via SMS. The user should then acknowledge their notification using either the Wireless Web capability on their cell phone, or even use a more secure device to respond to their notification. Since SMS is not a guaranteed delivery mechanism, the mFI software should be configured to use voice communications as a backup notification means.

The organization should also realize that the contents of SMS messages stored in the memory of a cell phone are not secure. Also, while the contents of an individual message may not be considered sensitive, the combination of multiple messages might be considered sensitive. Where security is a concern, mFI recommends deleting each message as soon as possible after viewing it.