AFRL-HE-WP-TR-2002-0079

UNITED STATES AIR FORCE RESEARCH LABORATORY

AN AUTOMATED TOOL TO ENABLE THE DISTRIBUTED OPERATIONS OF AIR FORCE SATELLITES

Jeffrey A. Fox
Jean E. Fox
Neil M. Baitinger
David S. Gillen

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

JANUARY 2002

FINAL REPORT FOR THE PERIOD 14 MAY 2001 TO 22 JANUARY 2002

Human Effectiveness Directorate
Crew System 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.

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

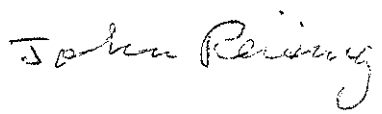
This Technical Report is published as received and has not been edited by the Air Force Research Laboratory, Human Effectiveness Directorate.

TECHNICAL REVIEW AND APPROVAL

AFRL-HE-WP-TR-2002-0079

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

FOR THE COMMANDER



JOHN M. REISING
Acting Chief, Crew System Interface Division
Air Force Research Laboratory

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	January 2002	Final Report , 14 May 2001 - 22 January 2002

4. TITLE AND SUBTITLE

An Automated Tool to Enable the Distributed Operations of Air Force Satellites

5. FUNDING NUMBERS

C: F33615-01-M-6043
PE: 65502F
PR: 3005
TA: HC
WU: 1B

6. AUTHOR(S)

Jeffrey A. Fox , Jean E. Fox, Neil M. Baitinger, David S. Gillen

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Mobile Foundations, Inc
103 W. Broad Street
Suite 600
Falls Church, VA 22046

8. PERFORMING ORGANIZATION

MFI-2002-01

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. SPONSORING/MONITORING

AFRL-HE-WP-TR-2002-0079

11. SUPPLEMENTARY NOTES

88ABW Cleared 08/20/2015; 88ABW-2015-4051.

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution A: Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

Report developed under SBIR contract for topic AF01-062. This report summarizes mobile foundations Phase I SBIR project entitled "An Automated Tool to Enable the Distributed Operations of Air Force Satellites." The overall goal of the project was to proved the feasibility of enhancing US Air Force space operations through the use of advanced automation to provide distributed situational awareness. Such an approach will help the Air Force meet the vision of "Next Generation Space Operations" laid out in the Air Force Space Command (AFSPC) Strategic Master Plan. This report documents the human effectiveness and systems analyses mobile foundations used as a basis for its proof-of-concept prototype. The report also describes the software prototype (called FASAT, Fast Access Situational Awareness) that mobile foundations developed and demonstrated to prove the feasibility of its approach to developing a next-generations distributed operations system.

14. SUBJECT TERMS

Satellite Operations, Situational Awareness, Automation, FASAT, Wireless Communications, Human Effectiveness, SERS, SBIR Report

15. NUMBER OF PAGES

65

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLAS	UNCLAS	UNCLAS	UNLIMITED

This page intentionally left blank

Table of Contents

List of Figures

List of Tables

This page intentionally left blank

1. Introduction

The Air Force Space Command (AFSPC) Strategic Master Plan (SMP) (Air Force Space Command, 2000) lays out the Air Force's plan for achieving its Vision of "A globally integrated aerospace force providing continuous deterrence and prompt engagement for America and its allies ... through control and exploitation of space and information." The Vision is clear in its message that space will play an increasingly more important role for the Air Force. The intended result of the Vision is a fully "Integrated Aerospace System" that

- "Provides Global Real-time Situational Awareness"
- "Maintains Space Superiority"
- "Provides Prompt Global Targeting and Strike."

The *SMP* lays out a strategy for reaching the Vision by setting near-term, short-term, and far-term strategies for improving Battlespace/field management and situational awareness. It is important to note that in the *SMP*, the predicted budget increase for "mission support" is very modest in comparison to the budget for "new programs." Therefore, the Vision specifically notes that to achieve the Vision the Air Force must

- "Leverage Partnerships"
- "Reduce the cost of doing business" via "cost-effective mission operations"
- "Support Installations and People"
- Have "Total Space Situational Awareness."

To that end, the Vision's priorities call for modernization in the near-term and new, more radical concepts and capabilities in the far-term, such as:

- "Global Real-Time Situational Awareness"
- "Next Generation Space Asset Operations Capabilities;" in particular, "Autonomy" and "On-Demand Operations."

The proper design and development of tools to support advanced automation and remote collaboration can significantly reduce the operators' burden, while increasing distributed situational 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 do occur, the tools can assemble appropriately skilled distributed response crews dynamically. 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.

NASA has faced a similar challenge for the past several years. NASA has been trying to maintain the same quantity and quality of space research, but on dramatically reduced budgets. In response to the operational challenge, NASA's Goddard Space Flight Center (NASA-GSFC) has introduced a new paradigm of operations called "lights-out" operations, which calls for complete automation of the ground segment of a mission during most routine operations. In order to make lights-out operations a reality, NASA tasked *mobile*FOUNDATIONS' (mFI) staff

to develop the Spacecraft Emergency Response System (SERS), an innovative Web-based suite of tools that automates many of the monitoring, reporting, notification, and team management activities required in a lights-out environment. When SERS detects an anomaly, it dynamically builds an appropriate response team based on (1) the type and severity of the problem and (2) the skills, availability, and communications devices of the on-call team members. SERS then enables them to work together as a remote, distributed team via wireless devices.

This Phase I SBIR effort explored the feasibility of using a SERS-like system for the Air Force. We found that such a system holds much potential for meeting the challenges faced by the Air Force. However, such a system cannot simply be deployed in the Air Force environment. The Air Force faces greater and more complex challenges in human engineering (e.g., near-real-time alerts that are meaningful) and in architecture (e.g., end-to-end security). Only through a user-centered design approach can the appropriate level and allocation of automation be determined in such a complex environment as an Air Force satellite control center.

Under the Phase I program, mFI proved the feasibility of the concept of deploying a significantly more advanced SERS-like tool (called FASAT: Fast Access Situational Awareness Testbed) for the Air Force by (1) better understanding the unique Air Force user requirements and appropriately mapping those requirements in a distributed system; (2) understanding the system requirements (hardware and software); (3) studying the impacts of critical current high-risk technology issues, such as real-time processing and security; (4) demonstrating a proof-of-concept functional prototype; and (5) identifying essential research capabilities required for a successful Phase II operational prototype. This document serves as the final report for our Phase I effort. In it, we discuss our approach, our findings, and our recommendations for follow-on work.

2. Background

2.1 Space Operations Overview

Traditional satellite operations are typified by dedicated operators, engineers, support staff, and managers stationed in dedicated, specially built rooms (hereafter called mission operations centers or MOCs), using dedicated, custom built, expensive one-of-a-kind equipment. These centers are staffed 24 hours per day, seven days per week by rotating crews (the size of which often corresponds to the complexity of the satellite). Typically separate crews are responsible for specific satellites. This traditional concept is shown in Figure 1 below.

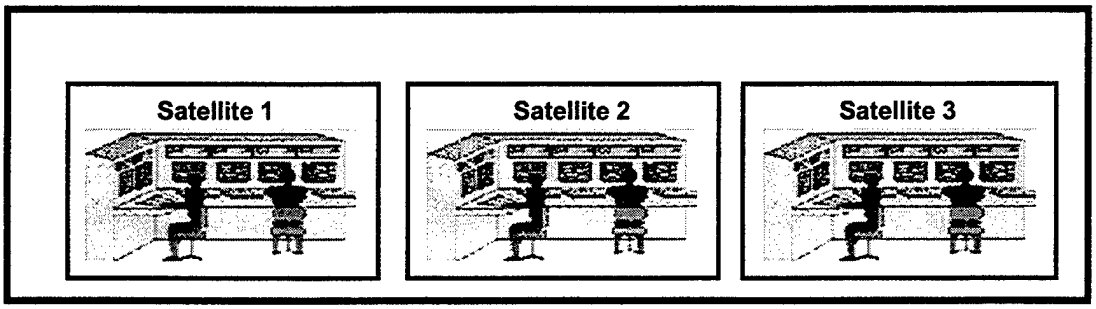


Figure 1. Traditional Operations

The operations crews can be thought of as intermediaries who take requests for specific data from the end users of the satellite. The requests are then mapped to schedules of opportunities. The crew then translates the requests into specific commands that they send to the satellite and its payload (e.g., they send commands to an on-board imaging device to capture an image of a specific location).

Many missions automate some of the crews' activities, but sometimes the automation is not as effective as it could be. For example, it is inefficient for operators to watch thousands of mnemonics on large screens constantly, looking for out-of-bounds conditions during routine operations, when it is so easy for the computer to simply notify the operator when such a condition occurs. On the other hand, hands-on "on-console" time is critical during special one-of-a-kind maneuvers to ensure that the satellite functions as planned. This is a matter of the appropriate allocation of tasks, based upon the strength and weaknesses of human and machine (Price, 1985). Depending on the level of sophistication of the satellite and the ground system, varying forms of basic automation have been introduced as job aids, such as on-line schedulers. However, in most cases, these augment the full-time crew, as opposed to reducing the size of the crews.

2.2 Automated Operations

Typically, full-time human monitoring is viewed as the safest and most accurate approach to satellite operations. This approach has been highly successful in the past, but it is becoming unviable due to budgetary reductions, evolving ground system and range architectures, and the

increased number and complexity of missions. Traditional mission operations have historically been expensive and inefficient. Much of the expense is from having crews stationed "on-console" around-the-clock, performing mundane work, such as watching for changes in parameters (i.e., limit violations), instead of performing more complex, and rewarding, tasks such as planning.

To address these issues, researchers have been exploring various means of improving the efficiency of mission operations through the use of advanced automation. These efforts tended to be theoretical and exploratory. While producing interesting models and theories, at least at NASA, little of the research made it into operational MOCs, due to NASA's risk-adverse institutional climate and the difficulty of converting theoretical models into deployable systems.

Further, many research efforts were conducted "in a vacuum" and did not involve actual users (operators) in the design process. In such efforts, there is a lack of *human-centered automation* (Jones, and Mitchell, 1991). All too often, research focused on the impossible goal of completely and forever removing the human from the loop through complete autonomy. Until the day that "true" autonomy (the computer decides everything, ignoring the human) (Wickens, et. al., 1998) is practical and affordable to deploy, it makes more sense to deploy ever-increasing levels of more capable automation (Breed and Fox, 2001).

2.3 Human Effectiveness Issues in Automated Operations

To eliminate the problems caused by conducting research in a vacuum, developers of automated satellite monitoring systems must consider the roles and needs of the users. If they do, the systems will be able to provide the users with automation and information they need to identify and respond to anomalies quickly and effectively. When anomalies occur, missions deploying advanced automation need to be sure that the problems are detected, and that on-call team members can rapidly understand the current situation (i.e., gain situational awareness) and respond appropriately from their remote locations.

A user-centered design (UCD) approach is of utmost importance to meet these goals (Fox, et. al., 2000, Fox, et. al., 1997) and to minimize the likelihood of incorrect decisions and actions by satellite operators. Operator errors can result in problems as insignificant as the delay in receiving data or as severe as the loss of a billion dollar satellite. In a UCD project, development revolves around the users' needs. In this way, the final product can facilitate the users' jobs.

The first stage in a project following a UCD approach is to learn about the users and the tasks they would perform with the system. To fully understand the work the operators perform, it is necessary to conduct user and task analyses. A *user* analysis will reveal characteristics of the users and their strengths and weaknesses. The results describe the users' knowledge, skills, and abilities (Goldstein, 1992). A *task* analysis will indicate what activities the users perform to reach a particular goal for their job. This is done by dividing tasks into subtasks, then describing who performs the task, when, what aids they use, and the importance of the task (Dumas and Redish, 1993). Information for both the user and task analyses can be obtained using a variety of methods including interviews, observations and contextual inquiry, focus groups, or even surveys (Kirwin and Ainsworth, 1993).

The user and task analyses guide the proper allocation of functions to exploit the strengths of both the computer and the human operator. Over the years, the computer's capabilities have expanded with improvements in technology, but there are still some tasks, which are best performed by human operators. For example, humans can use their creativity to respond to novel situations, which the computer cannot do. In some cases, however, it may be beneficial to assign tasks sub-optimally. For example, Price indicates that developers may want to "allocate for cognitive support" (Price, 1985). That is, sometimes tedious and monotonous tasks should remain under manual control so that operators know exactly what is going on should a problem arise. Thus, it is important to consider the user, the task, and the technology when deciding how to allocate functionality.

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. The operators must use a selective monitoring strategy (Doyle, et. al., 1992). In other words, as systems have become more complex, the operators' roles have evolved from "active manager," 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, 1991).

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 "situational awareness," is critical for the operators to respond appropriately to problems (Adams, Tenny, and Pew, 1991). 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 the operator perceives all the relevant information without being overloaded (Adams, Tenny, and Pew, 1991).

The automated monitoring system must provide the operators with more than just a notification of a problem. It must provide enough information, in a usable format, for operators to be able to respond to the problem (Adams, Tenny, and Pew, 1991; Sheridan, 1980). The challenge is to select carefully which information is displayed, so the operator is not overwhelmed. 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).

2.4 NASA-Goddard's Approach to Crew Automation

During the early 1990's, budget cuts at NASA shifted the focus of much of its operations automation research. NASA moved away from pure research toward applied research that focused on the practical applications of leading-edge technology that supports its new "smaller, faster, cheaper" approach to mission operations. This shift led to a major change in the way NASA's Goddard Space Flight Center (GSFC) did business. The operations staff now looked to the research community for new tools and technologies to help them reduce the costs of operations. At the same time, the researchers sought to embrace the operators in the design of new technologies.

One of GSFC's more detailed analyses of where it could appropriately apply automation was part of its Virtual Mission Operations Center (VMOC) program (Fox et. al., 1997; Bane and Fox, 1996; and Moore and Fox, 1993). The results led to the concept of a virtual distributed operations environment, in which cross-trained staff are dynamically allocated to missions, as needed, from remote locations. This concept is represented in Figure 2.

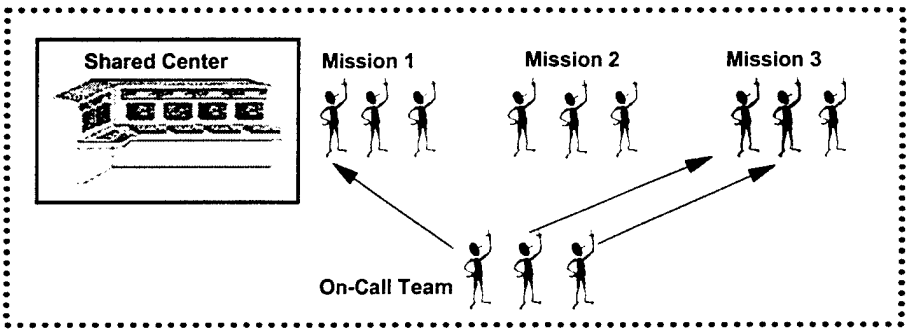


Figure 2. Virtual Distributed Operations

mFI's staff have translated this concept into an operational system for NASA-GSFC. GSFC has moved into the era of "lights-out" operations for unmanned satellites, during which the ground segment is run autonomously during most routine operations. Members of the operations team need to be involved in only those tasks that are too costly or too risky to automate. The rest of the time, the team members are on-call to respond to anomalous events. When the automated ground system detects anomalies, it immediately alerts the appropriate on-call team members and provides them with current information so they can assess the implications and, when necessary, start to resolve the anomalies remotely via wireless devices.

2.4.1 Monitoring, Alert Notification, and Response with SERS

Going to lights-out operations can save money, but it must not significantly degrade the quality of operations. That is, a lights-out environment 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). Thus, NASA-GSFC determined that in order to meet these sometimes-conflicting demands, lights-out software 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 lights-out automation. When SERS detects a problem, it:

- Contacts appropriate on-call personnel
- Synthesizes and presents the status and history of events and actions for rapid resolution
- 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 wireless device, but also allows the team members to respond via the 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, 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. For every mission, a SERS-enabled ground system reduces the time operators are required to spend in the control center by 15,000-25,000 hours/year, saving approximately $1 million/year.

2.4.2 User-Centered Design and SERS

SERS' real success is derived from the user-centered design (UCD) philosophy that was used to create the software. As the operations paradigms change, so too must the tools to support the mission operations team's tasks. Tools need to be built not only to automate routine tasks, but also to communicate varying types of information to the part-time, generalist, or on-call crew more effectively. Thus, the proper design of the user-system interface (USI) becomes even more important than before (Fox et. al., 2000). Many UCD techniques were used in the design of SERS, including task analyses, function allocation, focus groups, scenario-based design, and prototyping. Based upon the results of the UCD activities, system functions were allocated to

the humans or software subsystems. Also, through an extensive iterative design process, the interface designs were prototyped, tested, and revised until they met the users' needs.

Another key to the success of SERS is its adaptive interface. Because the users access these systems from various locations (e.g., control center, home, on the road) via different devices with varying display capabilities (e.g., workstations, home PCs, PDAs, pagers) over connections with various bandwidths (e.g., dial-up 56k, wireless 9.6k), SERS has different USIs to support the different types of users, their equipment, and their environments.

2.5 Air Force Needs for More Advanced Systems

There are many similarities between satellite operations at NASA and at the Air Force. Although the objectives of the satellites can be quite different, most of the operators' fundamental tasks are the same (e.g., planning, fault detection). However, there are some key differences between operations, such as:

- Near-real time operations – Because of the demands of the Air Force operators, an on-call crew must be notified almost immediately of any anomalous behavior of a satellite. Currently, NASA's SERS system can have a latency of up to 6 minutes.
- Security – The Air Force places a premium on securing its data and communications. The SERS system has no security beyond a web login screen for editing certain forms.
- Synchronous collaboration – The Air Force mode of operations depends heavily on the collaboration of its crews. The crews actively (i.e., synchronously) share information in performing their tasks. Currently, SERS has no tools to support this capability, since at NASA these tasks often are performed serially.

Thus, while a SERS-like system holds much potential for meeting the Air Force's challenges, further research is needed into how to build a more sophisticated and capable system that can support features the Air Force will require. The remainder of this document describes mFI's Phase I SBIR objectives and activities involved in proving that an enhanced versions of SERS (called FASAT – Fast Access Situational Awareness Testbed) could in fact provide substantial assistance in helping the Air Force move towards and on-demand, next generation space operations environment.

3. Phase I Technical Objectives & Approach

3.1 Objectives

The objective of mFI's Phase I research was to prove the feasibility of a distributed crew interface for autonomous satellite operations for the US Air Force. Since mFI's staff has already built a system for NASA, the focus of this effort was to leverage our existing technologies as a core system, so that we could concentrate in Phase I on the high-risk aspects of building a system to support the more demanding human engineering and architectural (software and hardware) requirements of the Air Force.

To address these challenges, the objectives of the proposed program are as follows:

1. Determine the high-risk user interface design challenges.
2. Determine the high-risk architectural design challenges.
3. Modify (enhance) a baseline SERS system to address the core user interface and architectural challenges identified in 1 and 2 above.
4. Demonstrate a proof-of-concept system prototype that would:
    a. Simulate an anomaly from an Air Force satellite
    b. Automatically log the anomalous event(s)
    c. Determine which on-call team members to contact and alert them
    d. Allow those team members to respond to alerts via wireless devices
    e. Allow distributed crew members to share data (on PCs) in real time.
5. Recommend an approach for Phase II follow-on work.

In the course of meeting those objectives, we set out to answer the following questions to determine the system's feasibility:

- Can Air Force operators work in a distributed and wireless environment?
- Can software be developed to support synchronous (same-time) crew collaboration?
- Can software be developed to respond to triggers in near-real-time?
- Can end-to-end security be maintained?
- Can the current ground systems support a distributed system?
- What other new functionality will need to be developed to successfully deploy the system?

3.2 Overall Approach

To reach the goals defined above, mFI used a variety of technologies. mFI's staff leveraged its unique experience in designing, developing, and deploying the Spacecraft Emergency Response System (SERS), a "lights-out" autonomous anomaly alerting, tracking, and management system, for NASA. Then, we collected information from Air Force operations, primarily through observations, interviews, and documentation, to understand Air Force operations. From analyses of that data, we then developed our proof-of-concept prototype that showed the feasibility of such a system and our approach to developing it.

3.3 Air Force Space Operations at CERES

The first and most critical step in determining the feasibility of our approach was to gain an understanding of Air Force Operations. We already knew that our approach was successful for NASA mission operations; however, we needed prove that it would support the Air Force's more demanding space operations environment. In order to keep within scope of a Phase I SBIR level of effort, The Air Force and mFI both felt that this research effort should focus on the operations environment at the Center for Research Support (CERES) at Shriever AFB since: (1) the majority of the CERES' staff are ex-Air Force mission operations personnel, (2) it is the CERES' mission to support such technology demonstration and evaluation activities, and (3) CERES employs more modern and open ground systems than are currently deployed in the space operations squadrons (SOPS). The CERES website (Joint National Test Facility, 1999) describes that organization as follows:

> "The CERES complex located within the Joint National Test Facility (JNTF) is jointly sponsored by the Ballistic Missile Defense Organization (BMDO) Test & Engineering Resources (BMDO/TOT) Directorate and the Space and Missile Systems Center (SMC) Test and Evaluation Directorate (SMC/TEO). CERES is tasked with providing satellite command and control support, to include satellite data processing, display and distribution. Its mission is to provide payload support of orbital flights, perform orbital experiments, perform simultaneous flight experiments, develop operations center software, and support common requirements between multiple programs. This facility provides a cost effective Satellite Operations Center (SOC) to command and control space vehicles and distribute sensor data to Shield, Space Warfare Center (SWC), and BMDO initiatives."

Since CERES was our test environment for this Phase I effort, our data collection efforts focused on the CERES operations environment, its operators, and its primary mission operations ground system called COBRA (COTS-Based Realtime Architecture) (Hogan, 2000). While CERES is in the process of evaluating other ground systems, COBRA is the system that they currently use for supporting live passes.

4. Results of Analyses

The findings of our research and prototyping demonstrate that Air Force space operations can benefit from tools that provide advanced automation and distributed operations. We came to this conclusion based on performing human effectiveness and software architecture studies of available documentation and a site visit to the CERES. These studies provided us with the necessary understanding of Air Force space to enable us to identify basic needs and candidate opportunities for technology infusion.

Those findings formed the basis for performed a feasibility study to determine if an enhanced version of our SERS system could be adapted to satisfy the more complex requirements of Air Force operations. We concluded that indeed our approach is feasible and we provided the following answers the questions posed in Section 3.1 above:

- Yes, Air Force operators can function in a distributed and wireless environment.
- Yes, software can be developed to function seamlessly with SERS to satisfy the synchronous (same-time) needs of crew collaboration.
- Yes, software can be developed to respond to triggers in near-real-time. Although we did not develop such software in this phase of our SBIR, we defined some approaches towards satisfying this need.
- Yes, end-to-end security can be maintained using either COTS or custom tools.
- Yes, we demonstrated that our software can interface with a modern Air Force ground system (CERES' COBRA).
- We identified new functionality that will need to be developed. For some of this functionality, we defined the approach towards developing it, for others we demonstrated the feasibility of the new functions in our prototype.

In the following sections, we provide further details to support these findings. Section 4.1 (General Findings) makes some general observations about the current state-of-the-art of space operations at the Air Force. Section 4.2 (Human Effectiveness Analyses) provides the detailed results of our human effectiveness studies, and outlines the needs and deficiencies of current space operations at the Air Force. Section 4.3 (Architectural Analysis) applies the technical needs of the Air Force with the feasibility of developing and deploying a tool at the Air Force to satisfy the current needs and deficiencies. And Section 4.4 (Prototype) provides scenarios of how an automated operations tool can be applied to actual procedures encountered during space operations at the Air Force.

4.1 General Findings

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 its own 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 have 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, either 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 answer the *Air Force Space Command (AFSPC) Strategic Master Plan's* call for the SOPS to move towards "Total Space Situational Awareness," "Autonomy," and "On-Demand Operations." Fortunately, facilities like CERES are playing an important role in evaluating and pushing technologies into the SOPS. 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. Tools, such as SERS, modified to meet the needs of the Air Force, can enable further progress toward the Air Force's vision.

Compounding the difficulty in moving towards a distributed on-demand operations environment is the Air Force's need for end-to-end security. In addition to the real challenges of securing wireless data, there also is a perceived threat from the *change* associated with doing work wirelessly.

The technologies being researched under this SBIR can play a significant role in helping the Air Force achieve both nearer-term goals of improved efficiency and longer-term goals of on-demand operations. Thus, we have concluded that distributed operations will need to be phased-in. The first phase should be distributed operations across a single base (e.g., crew access from anywhere at Schriever AFB). The next phase would be to provide remote access off base (e.g., from home or other facility).

4.2 Human Effectiveness Analyses

4.2.1 Approach

mFI maintains a focus on the users for every development project. While in the end it is the technology that will free crews from spending countless hours monitoring mnemonics and allow them to work as on-demand supervisors, wholesale automation without regard to its impact on the remaining human elements of an organization is doomed to failure. As Sheridan (1980) points out, "Designers...must choose a level of automation from a spectrum ranging between no computer participation to total automation" (Sheridan, 1980, p. 65). Our work with NASA has shown (Fox et. al., 1997; Fox et. al., 2000; and Fox et. al., 1999c) that a user-centered design (UCD) program is an effective way to successfully design and deploy an automated automation.

For these human effectiveness analyses, mFI utilized its expertise and lessons learned in creating and deploying SERS at NASA. In order to understand how the Air Force operators, and in particular those at CERES, perform their work, mFI reviewed information from several sources. First, we reviewed documents previously created by mFI's staff regarding the monitoring activities at NASA. Next, we reviewed additional documents. The Phase I report by MTI entitled "Advanced Interfaces for Space Operator Consoles" was particularly helpful. Finally, we learned a lot from the operators themselves during our visit to CERES. We observed the operators during several passes. They provided us with some additional (unclassified) documentation regarding their activities. As part of the contextual inquiry, we asked several operators a series of questions. The findings from these interviews are included in Appendix A and provide the basis for the summaries reported here. The results described in the remainder of the section are summarized in Appendix B.

4.2.2 Results

4.2.2.1 The Users

We found that the contextual inquiries were very helpful in soliciting information about the CERES operators. The operators we spoke with were mostly former SOPS crewmembers, so we were also able to learn about their experience and training at the SOPS operations centers.

Operators for the SOPS operations centers are chosen based on aptitude tests new enlistees must take. They participate in a 5-6 month training program, then receive on-the-job training for their particular job. There is generally no higher education requirement for this position. This background is in contrast to our experience at NASA, where most operators have earned college degrees from programs specializing in spacecraft operations.

The operators at CERES had previously worked in the SOPS as Air Force personnel. When they left the Air Force, they took positions in the mission operations center at CERES. All the CERES operators we spoke with were contractors who had learned many of their skills during their time as Air Force SOPS operators. The operators at CERES are classified into levels of certification. The certification level determines how much responsibility and authority an operator has. The document "CERES Certification Standards and Requirements" identifies the

skills and accomplishments required to reach each level. CERES provides on-the-job training so operators can advance through the levels of certification.

The CERES operators identified a significant difference between their responsibilities at the SOPS and at CERES. At the SOPS, operators had their own specific area of responsibility. At CERES, the operators had a wider range of responsibilities and more authority. The operators found this to provide greater job satisfaction.

4.2.2.2 The Work Environment

The CERES operators work in environments similar to those at NASA. The operations center is one big room with several workstations to manage several strings. Operators work with one string at a time, but other operators can be working with other strings. Most of the time, the environment is typical of an office environment, but on occasion the work area can get loud.

Another issue that the CERES operators mentioned is the formality of the work culture. At the SOPS, everyone had their own area of responsibility, and there were clear boundaries in terms of who does what. At CERES, the operators had more responsibility, and a little more flexibility in terms of how to respond to a situation. The operators are limited by their level of certification, but they still felt they had more freedom than at the SOPS. The operators appreciated this freedom.

One other significant difference from the NASA operators is the work schedule. Most of the "lights-out" missions using SERS need operators only during business hours. At CERES, the operators work a rotating schedule that changes every two weeks. At the SOPS, the schedules change even more frequently. Although shift work can lead to fatigue, especially with the shift changing so rapidly, the operators we met with didn't mind. They liked having time during the day to be with their families.

4.2.2.3 The Tasks

There are a variety of tasks involved with monitoring satellites. Many of the activities are similar to those conducted at NASA. Operators follow a common approach for all passes, addressing anomalies as they arise. A typical pass involves the following activities:

- The mission controller reviews the pass plan as much as a day before the pass.
- Approximately 30 minutes before the pass, the mission controller contacts the ground control network, the organization that receives the telemetry, to open the communication connection.
- During the pass, the mission controller uploads and downloads the data and commands.
- The mission controller also monitors data coming from the satellite to identify anomalies.
- At the end of the pass, the mission controller contacts the ground control network to shut down the communication connection.
- At CERES, after the pass, the mission controller manually enters anomalies into a database nicknamed "The tool". The tool is in no way tied into the operational strings. Also, the

tool provides little functionality beyond storing the anomaly data (as opposed to an anomaly management system).

There is a wide range of activities that can occur within this general framework. For example, the methods of uploading commands and downloading data can vary. At CERES, different satellites were monitored by different front ends, requiring different types of interaction. Some passes are controlled fairly manually, requiring operators to type in each command. Other front ends allow operators to work with a command file created by an engineer, enabling the operators to click a button to enact a series of commands.

During a typical pass, an operator sends a command, or a series of commands, then waits to see how the satellite responds. The operator monitors a group of mnemonics until the satellite reaches the desired state. When it does, the operator records one or more mnemonics for the engineer to review later. The operator usually either records the values by hand or by printing out a screen shot. Once the desired state is reached and the appropriate values recorded, the operator can send the next command(s).

Unfortunately, passes do not always go smoothly. As operators monitor the mnemonics, they are looking for unusual or out of range values. At CERES, the mnemonics are color coded so that nominal values are displayed in white, slightly out-of-range values are yellow, and those significantly out-of-range are red. The color-coding helps operators identify problem areas quickly. However, the color-coding helps the operators identify the symptoms of the problems, but not the cause.

During anomalous conditions, the operator's response depends on several factors. The operator must assess

- Their level of certification – the level will determine what conditions an operator can respond to and those they cannot
- Specific instructions in the pass plan – the pass plan may reference a specific contingency plan the operator should follow.
- Standard contingency plans or flow charts – these are instructions for the operator's response, which are standard across missions.
- Previous experience with the anomaly or similar anomalies – if an operator resolved an anomaly successfully in the past, they can use the knowledge gained from that experience if the anomaly occurs again.

The anomaly can be caused by a variety of problems. These problems include:

- A malfunction in the satellite
- A breakdown in the communication link
- An error in the command set
- A failure in the ground system

When operators are unable to resolve the anomaly with the knowledge, skills, and abilities they possess, they must determine an alternate response. The operator will most likely have to

contact an engineer. For minor problems, the operator may just leave a note for the engineer describing the problem. During business hours, the operator may request that the engineer come to the operations center for more serious anomalies. During evening and night shifts, the operator can telephone the on-call engineer. The conversation is worded carefully to avoid any breach in security.

4.2.2.4 Differences From NASA

The differences between NASA and the Air Force are highlighted in Appendix B. Because the Air Force users have a different background, and the work environment is somewhat different than NASA's, it will be important to maintain a strong human effectiveness program to ensure we build a system that meets the Air Force users' needs.

The major differences between NASA and the Air Force, as reported above, are the importance of security, near-real-time alerting, and synchronous collaboration. These must be addressed in any follow-on work.

4.2.2.5 Needs

This analysis revealed a variety of ways in which advanced automation could improve the efficiency and effectiveness of the operators at CERES, and also at the SOPS. The following tools would be useful:

- Improved situational awareness – tools that allow users to be quickly notified of problems (anomalies), assess the situation, and respond to the current status of any given situation from wherever they are located.
- Automation – tools to automate routine and mundane tasks (such as filling out standard forms), so that the personnel can perform more valuable work. This could eliminate the need for operators to take so many notes and print out screen shots for the engineer. At CERES, this would also eliminate the necessity of recording pass information in "the tool," an independent application.
- Job Aids – on-line tools that can guide the operators in decision support. The operators reported that their displays did little more than color code mnemonics. A system that could review mnemonics and identify possible failures would allow operators to work more efficiently.
- Distributed team collaboration – tools that allow any combination of operations personnel (console operators, on-site engineers, and offsite staff) to work together in a more efficient manner. This would eliminate the need for operators to leave notes to engineers or to take the time to find them.
- Interoperability – any new tools must be flexible enough to work with a wide variety of other tools.
- Security – tools that improve or enhance operations cannot do so at the sake of reduced security.

4.2.3 Conclusion on Feasibility

The results of the human effectiveness studies clearly show that: (1) there is a need for tools that provide advanced automation and support distributed situational awareness and (2) that an enhanced version of the SERS software (FASAT) could be used to assist in meeting those needs. The Air Force will need additional functionality that is not currently in the Phase I prototype. In follow-on work, mFI plans to conduct this development with a strong emphasis on the users' needs.

4.3 Architectural Analyses

4.3.1 Approach

The architectural analyses consisted of research into the software, hardware, and communications issues that would determine the feasibility of the proposed system. Since we chose to work with CERES for this Phase I effort, we focused our analyses on CERES' operational COBRA system.

mFI's approach was to:

- Document current and near-future capabilities and limitations to select an appropriate ground system with which to interface.
- Determine how our software could be interfaced into the COBRA architecture.
- Determine what new features would need to be prototyped to show feasibility of our approach.
- Define interface options (e.g., e-mail, database, CORBA) could be used for the proof-of-concept prototype.

4.3.2 Results

4.3.2.1 System Interface

The single most important aspect of our architectural studies was to determine which CERES ground system(s) our prototype would interface with and how the prototype would receive data.

We found that CERES primary ground system is called COBRA (COTS Based Realtime Architecture) (Air Force Space Command, 2000). CERES is also evaluating a number of other ground systems including: Lockheed Martin's SCS-21 and Braxton's ACE.

However, at the time we conducted our Phase I efforts, only the COBRA system was being used operationally to take satellite passes. Since we would be unable to receive data from either SCS-21 or ACE systems, our only choice for demonstration purposes was to use the COBRA system. An advantage of selecting the COBRA system is that it is also being used at the RSC at Kirtland AFB, which gives us other potential Phase II users. The COBRA system is discussed in more detail in the section below.

4.3.2.1.1 COBRA

COBRA, the COTS Bases Real-time Architecture, is the command and control system in use at the Center for Research Support (CERES) at Schriever AFB in Colorado Springs, Colorado and at the Research, Development, Test and Evaluation (RDT&E) Support Complex (RSC) at Kirtland AFB in Albuquerque, New Mexico. COBRA has been used to provide command and control services for a variety of DOD and RDT&E satellites.

COBRA was developed in 1995 by L-3 Communications Storm Control Systems, Inc (L3 Storm) in a joint effort with the Space Test and Evaluation Office (SMC/TEO) and Lockheed Martin. Since COBRA's initial delivery, four enhancements have been introduced to provide new versions of COTS products and major functional enhancements to the custom components.

COBRA's hardware and software COTS products are integrated through a common interface, database structure, and message-passing middleware. Both complexes that use COBRA use a similar configuration to simplify cross-site development, maintenance and training. They use the same COBRA architecture with additional hardware, software, facilities and procedures necessary to provide services.

The COBRA hardware components are arranged into strings, each consisting of all of the hardware and software needed to conduct a single spacecraft contact. Figure 3 below, from the COBRA Documentation, shows the components of a typical COBRA string.

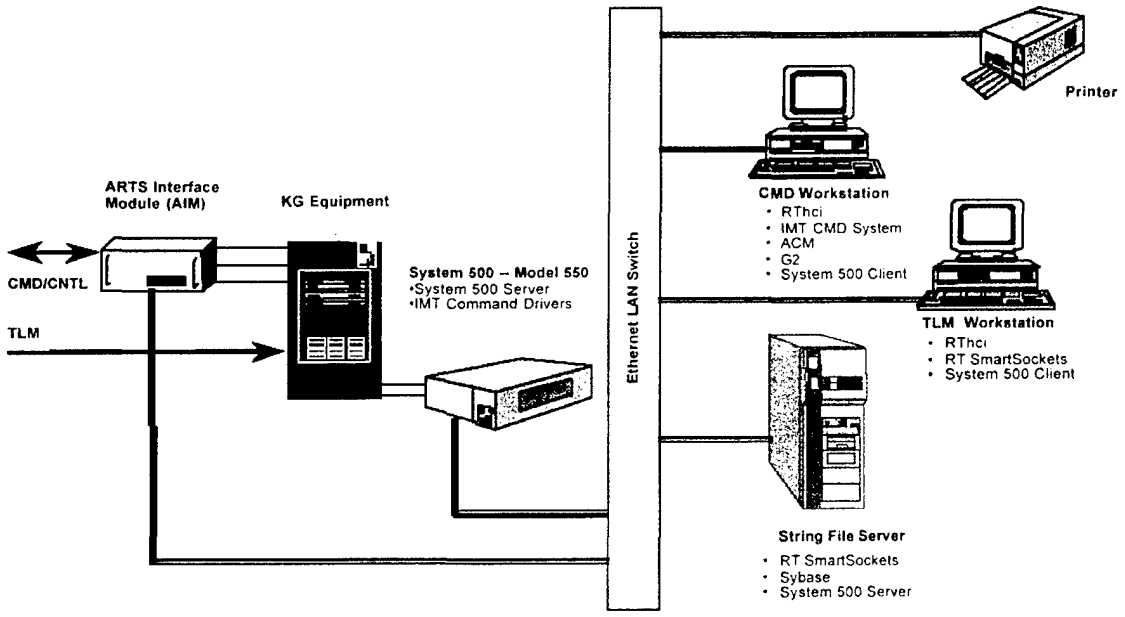


Figure 3. Typical COBRA String, From COBRA Documentation

COBRA's COTS software components are integrated as a "toolkit" to minimize custom software development. It consists of the following components:

- Sun UltraSPARC workstations running Sun Solaris
- Sybase for data storage of command bits, structures, parameters and pass plan information.
- Talarian SmartSockets provides a high-speed message bus for communication between COBRA components and to external clients.
- The ARTS Interface Model from L-3 Storm provides an interface to the AFSCN for SGLS command formatting and control and status of RGF antenna and RF equipment.
- Intelligent Mission Toolkit from L-3 Storm provides and expert system for vehicle commanding and telemetry commanding. It is implemented on Gensym's G2 expert system.
- The System 500 Model 550 front-end processor from L-3 Communications performs command formatting, KG control, and complete telemetry frame synchronizing, decommutation, and engineering unit conversion.
- Rthci Telemetry Display from Talarian provides graphical displays of vehicle telemetry and status data.
- The Satellite Toolkit (STK) from Integral Systems Inc. OASYS and Analytical Graphics (AGI) provides contact planning and orbit management functions.
- PV Wave from Wolfram Research provides telemetry data analysis.

The following figure from the COBRA documentation shows how the COBRA software components are organized by functional area.

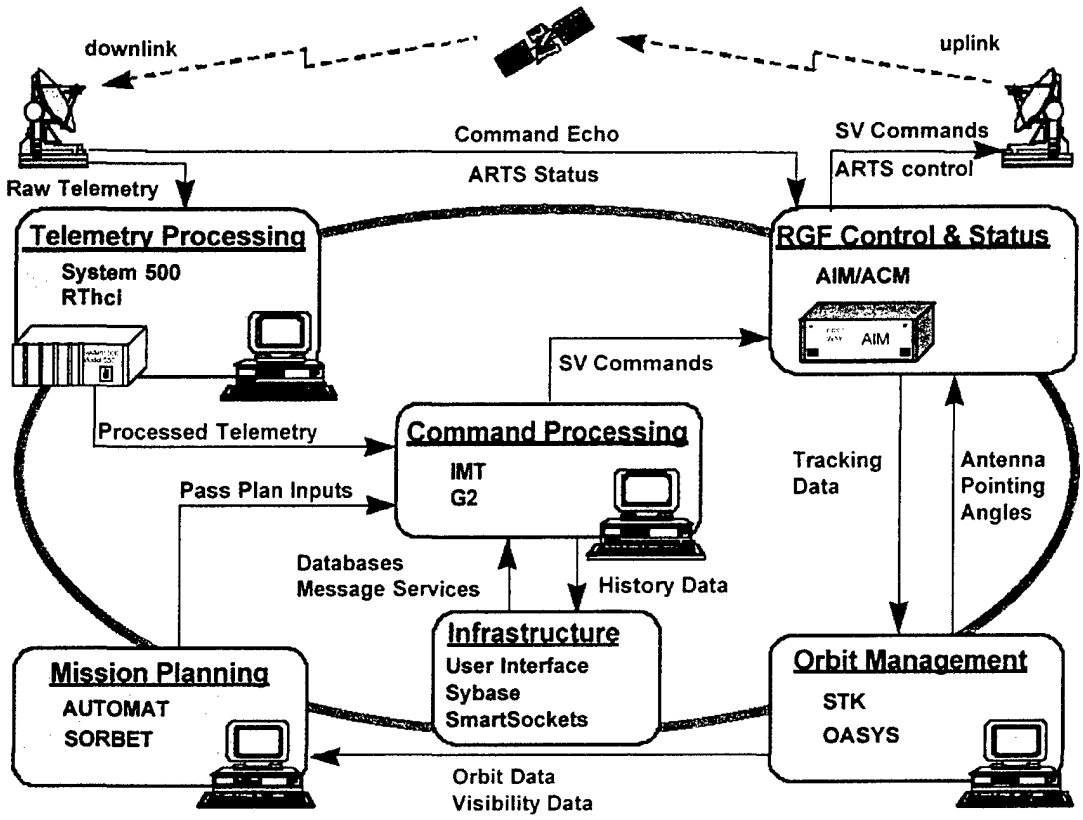


Figure 4. COBRA Software Components, From COBRA Documentation

4.3.2.1.2 Our Phase I method of interfacing with COBRA

Our Phase I effort was to prove the feasibility of building software for Air Force distributed mission operations by utilizing the core SERS technologies as the basis for a proof-of-concept prototype. To prove its feasibility, we needed to determine what data sources would "feed" our software and how we could distribute the data to distributed users in an effective manner. For the Phase I demonstration, we determined that we needed two types of data; telemetry data and pass plan data. The telemetry data can be retrieved from the COBRA system via Talarian SmartSockets. SmartSockets is a middleware application that allows clients to subscribe to different classes of messages in the COBRA system, such as telemetry data or AWE messages. The pass plan data is available from the Electronic Scheduling Dissemination (ESD) system as a file that is currently imported daily into the COBRA system.

Building all of the data interfaces into the COBRA system was beyond the scope of the Phase I effort, so we simulated the data from the different systems. A schematic of our Phase I approach is shown in Figure 5. We sent telemetry data in via a simulated event log file. The log file contained only of bounds telemetry points for the demonstration. It could however have contained other event information, such as AWEs, ground events, procedures run, or commands sent. The log files we used for the demonstration only contained telemetry data since that was the only data we had access to from an actual Air Force satellite

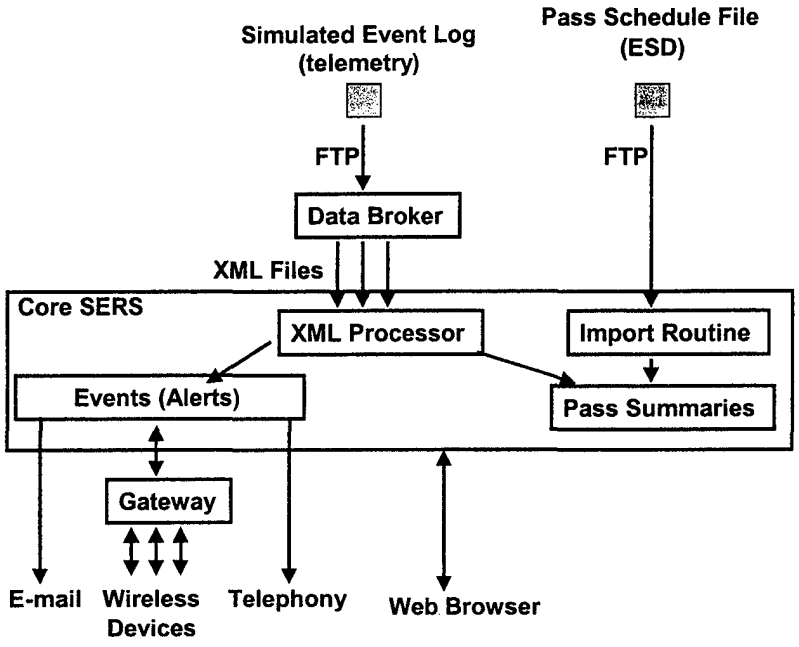


Figure 5. Phase I Approach to COBRA Interface

The simulated event log consisted of data files with the out of bounds telemetry that were produced from a single pass. The files were sent via FTP to our "DataBroker," which filtered them for important information and then formatted them into a standard XML format for FASAT to process. FASAT used the output from those files to automatically generate event reports and alert the appropriate users. The alerts generated from that data were sent via a wide variety of wireless devices, as well as a wired Web user interface. FASAT also used the DataBroker output to fill out pass summary reports detailing all of the activities that occurred during the pass.

Another component of the demonstration was the ability to process with pass plan data. We imported a file into FASAT based on the format of the file that is currently imported daily from the ESD system into COBRA. Our prototype joined the imported pass plan data with the data from the event log to produce pass summary reports.

In summary, the demonstration simulated data coming from the COBRA system, our software's processing of the data to produce event and pass summary reports, and the alerting of appropriate personnel based on the incoming data. Thus, we were able to prove the feasibility of our approach.

4.3.2.1.3 Near Real-Time Interface

During our Phase I feasibility study, we determined that post-pass analysis of data is not sufficient for the Air Force. An operational system will need to process data in near real-time.

Creating the interfaces into COBRA for near real-time would take considerable time and effort, and the interfaces were not necessary to prove the feasibility of using a FASAT system for the Air Force. Therefore the near real-time interface was beyond the scope of Phase I.

However in Phase I, we were able to define the high-level requirements for the near-real-time interface. More specifically, we determined that an operational version of FASAT would need to perform:

- Have an easy-to-use user interface for specifying how and when alerts should be sent during continuous data monitoring. In other words, users should be able to define the alert criteria for near-real-time data.
- Support an application program interface (api) plug-in for our software that can handle continuous data streams.
- Parse data in near-real-time to look for the criteria that the users specify.
- Include an alert engine that can dynamically manage changes to alert status.
- Include an effective pass summary capability that will support real-time data.

In Phase I, we also developed a possible approach to building a real-time interface to COBRA. The interface is summarized in Figure 6 below.

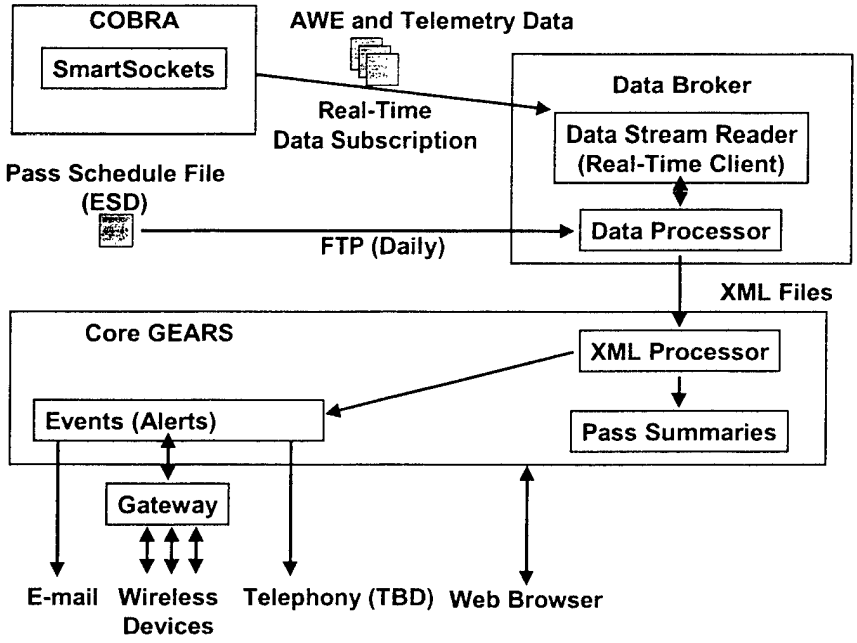


Figure 6. Approach to Near Real-Time COBRA Interface

The primary interface between COBRA and FASAT for near near-real-time alerting will be a Data Stream Reader. The Data Stream Reader will be the near-real-time client that receives data from COBRA via the Talarian SmartSockets. SmartSockets is middleware that allows clients, called RT Clients, to subscribe to different classes of messages in the COBRA system. The Data Stream Reader will be an RT Client that subscribes to the data. The Data Stream Reader also will be a plug-in to our FASAT DataBroker. The Data Stream Reader will store the data and

pass it to the data processing engine of the DataBroker for processing. The intervals for passing the data will be configurable for minutes down to near-real-time.

The figure also shows that the Data Broker will need to process schedule files from the Electronic Schedule Dissemination (ESD) system and pass them to the FASAT system. These files will be used to synthesize pass summary reports.

The output from the Data Broker will be XML files that will be sent to an XML processor in the core FASAT system for processing of alerts and pass summaries.

In order to synthesize the pass summary reports, the system will need to store the real-time feeds. It will need to be able to determine where in the feed a pass starts and ends, as well as what pass the data indicates. That will be based on the input from the ESD system or markers within the data feed itself. The data from that period of time will then be put into the pass summary report. The data could be stored and broken into passes by the Data Stream Reader before being sent to the data processing engine, or it could be processed and sent to FASAT, where it will be stored and broken into passes. Further study will be required to determine which method would be most appropriate to implement.

4.3.2.2 Support for AF Workflow

As part of our architectural study, we determined that with the addition of a near real-time interface into COBRA, the alerting schemes used in FASAT could effectively support the Air Force workflow. Based on the data from COBRA and triggers defined by the operations staff, FASAT could perform the alerting necessary for the Air Force.

Typical workflows typically follow one of two paths:

- Known problems, which can be resolved by an operator.
- Unknown problems, which require an engineer to resolve.

In the case of known problems, once detected, an operator would typically run a canned procedure to fix the problem and then notify management that a problem occurred and log the problem and resolution. FASAT can support this workflow in several ways.

FASAT can look for pre-defined conditions in the data that indicate that a certain problem has occurred. Once the condition is found, FASAT can alert the operator that the problem has occurred. Since the operators are typically on-console when problems are detected, FASAT can notify the operator via a window on the console that shows all of the problems that FASAT has detected. Optionally, FASAT could also display information to the operator on what procedures need to be run to correct the problem.

FASAT could then automatically alert management of the problem via a wireless device, e-mail, or another method. This would reduce the burden on the controllers by performing this task automatically and would keep management in the loop more quickly than if the controller had to manually notify them. FASAT could automatically log the problem and the procedure that was

run in event and pass summary reports. The exact workflow procedures would be developed based on human effectiveness analysis of the crewmembers and their environment.

When an unknown problem is encountered, the workflow is similar, except that an engineer must be notified to resolve the problem. FASAT can determine an unknown problem by detecting out of bounds conditions that do not fit any of the criteria for known problems. When this happens, FASAT notifies the operator and management and logs the problem as in the previous example, and also notifies an appropriate engineer.

FASAT can significantly decrease response time by the engineers by:

- Determining what types of engineer are needed, based on the subsystem that the out of bounds conditions occurred in.
- Figuring out what engineers are currently on-call, and how they should be notified.
- Notifying the engineers via two-way wireless devices or other methods.
- Providing on-line support synchronous distributed collaboration.
- And, if the engineers do not respond to their notifications within a certain period of time, notify the back-up engineers.

4.3.2.3 Anomaly Tracking

Besides being an alerting system, FASAT is also an anomaly tracking system used to log and track problems and resolutions. The anomaly tracking system allows operators to enter problem reports, and have them assigned to engineers for resolution. Once resolved, they are routed to for authorization.

FASAT's anomaly tracking function is similar to what is performed at CERES by the Operations Scheduling Tool (OST). However, FASAT's capabilities are more flexible and powerful since they are integrated into FASAT's event logging and alerting capabilities. Also, the anomalies entered into FASAT can be minded as part of any external knowledge management system.

In the prototype, the data entered into the anomaly tracking system was loosely based on the data currently entered into the OST.

4.3.2.4 Security

Security is an important consideration for most mission critical applications. When working with wireless devices, security becomes even more important because of the increased perceived risk of interception of data by a non-intended recipient. With the increased proliferation of wireless devices, and their varied types, communication models, and protocols, it is important to select the appropriate device and associated communication architecture to ensure the data transmissions are secured appropriately.

Wireless devices range from one-way pagers to interactive two-way web-browsing devices. Each of these devices receives its data differently, and the latter offers a way for the device to

transmit as well as receive. Consumer wireless devices have existed for some time now (pagers being the first to reach popularity). Early standards for transmitting pager data were not very secure, but they have improved over time. Now that these and other wireless devices are being used in mission-critical applications (e.g., financial, emergency response), more attention is being paid to security and integrity of the data with the use of technologies such as end-to-end encryption.

Wireless devices also include traditional computing devices, such as PCs and PDAs that have been equipped with wireless Ethernet cards (802.11b protocol). Security is very important for these types of devices and networks, since a compromise to this type of network makes an organization's entire LAN vulnerable. Fortunately, the manufacturers of wireless devices and the network providers supporting wireless networks now recognize the importance of security, and these companies continue to make advancements in areas of wireless security.

The security concerns for the Air Force are especially critical. The Air Force must ensure that telemetry or other spacecraft-related data cannot be intercepted (this is true for land-line communications as well). Today, the Air Force already uses manual notifications of personnel of critical incidents via phone lines and pagers. To ensure security in the current environment, policies regulate what information is transmitted so as not to reveal sensitive data. This is a policy or an administrative way of controlling data.

Despite the fact that wireless technologies are being deployed (outside of this Air Force program) today, there is more work to be done to protect sensitive data. Often, enhanced security solutions come at the expense of ease of use. Security solutions can often give the impression of "getting in the way" of a system's normal function, and may impede the use of the system. In-depth evaluations are needed to determine (1) whether the security provided by these systems is adequate for an organization's requirements, and (2) the impact on usability as a result of adding wireless security.

As part of our Phase I SBIR, mFI performed a high-level survey of a variety of these security technologies, and determined that there are no major obstacles to prevent an organization from transmitting sensitive data wirelessly. Sufficient protection exists to protect the authenticity of the data, to prevent the data from being intercepted, and to protect any data stored locally on a wireless device. Further, the industry continues to improve wireless security.

4.3.2.4.1 Pagers

Pagers were once the most common wireless device. Users like their small size and low cost. Even with the proliferation of other devices, pagers are still very popular today, often due to their longer battery life, nationwide coverage (without roaming charges), and better reception of data within buildings.

There are two steps involved with sending information to a pager. The first step is the transmission of the information to the paging terminal. The second step is the broadcast of the information to the pager. Both steps of this transmission must be protected for the entire page to be secure. In addition, an organization must secure the data that are stored on the pager itself.

To maximize security in the first step of transmission, an organization would use its own paging terminal, rather than rely on a public system (Figure 7). When an organization has their own paging terminal, there is no risk in getting the information to the paging terminal, since this is all done within the organization's internal network. However, having an internal paging terminal can be an expensive investment. Most organizations depend on public paging carriers to manage the paging terminal (Figure 8). In this case, the information must be sent outside of the organization to the paging carrier. This is usually done over the telephone or over the Internet. Information should be encrypted when being transmitted outside of the organization to protect the contents of the page.

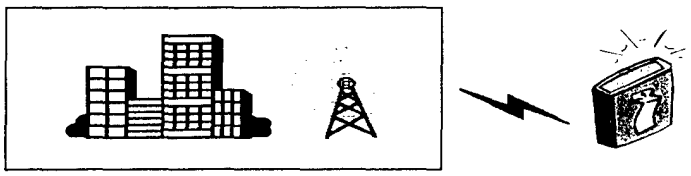


Figure 7. Using an Internal Paging Terminal

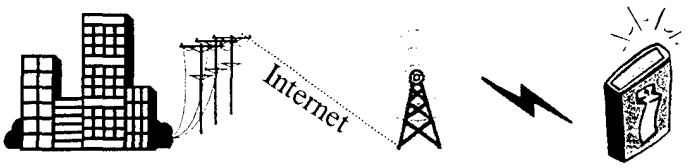


Figure 8. Using a Public Paging Carrier

Once the paging terminal receives the information to be paged, it sends the information over the airwaves to the pager. Since an organization's boundaries usually do not have control over airwaves, the transmissions through the airwaves should be encrypted to protect the contents of the page. If an organization owns their own paging terminal, they can use whatever encryption scheme they want. If an organization uses a public paging carrier, the organization should select a carrier that supports encryption.

Ideally, data should be encrypted end-to-end. With this type of encryption, the originating system encrypts the message before it is sent to the paging terminal, and the message is never decrypted until it reaches the appropriate pager. One commercial solution that implements this is Air SmartGate from V-ONE (http://www.v-one.com/products/airsmartgate.html). This solution uses 128-bit encryption for both the wired and wireless portions of the transmission. The message is never decrypted until it reaches the pager. V-ONE is currently implemented by SkyTel Communications, Inc., AirTouch/Vodaphone, PageMart, and Wireless Web (formerly PageNet. The pagers that can receive encrypted data include the Glenayre Access Link II with Secure Link, RIM 850, Motorola PageWriter 2000 / 2000x, Timeport TM P930 and the Timeport P935 (http://www.skytel.com/aboutus/pr_vone.htm). Another option is to use the Blackberry paging service that is part of the RIM devices. Blackberry has software that will encrypt data

from an organization's server , the RIM device using triple DES encryption. (Bb_security_technical_wp_domino.pdf - page 3)

Once the message is received on a pager, the pager itself must be protected to ensure the message is protected. If the message is encrypted as it travels to the pager, but then the pager falls into the wrong hands, wireless encryption will not prevent anyone from viewing the data on the pager. Therefore, the physical pager itself must also be protected.

The method in use today requires the pager owner to use a PIN. The owner must unlock the PIN to gain access to the data stored on the pager. While this is often sufficient to protect the data, it can be inconvenient for the pager owner, since an extra password or PIN must now be remembered.

Future technology may use biometrics to protect the data on a pager. For example, Indentix is currently working with Verisign to create a fingerprint reader that can be built into a cell phone. When the correct finger is placed on the reader, the device will be unlocked. (95292.pdf) Perhaps in the future, a device similar to this will be available for pagers as well.

4.3.2.4.2 Web-enabled Cell Phones and Personal Digital Assistants

According to a recent Gartner report, at the end of 2000, there were over 2.5 million subscribers to wireless web services via cellular phones in the United States (Skvarla and Dooley, 2001). With all of these devices in use, there is a lot of information traveling through the airwaves that needs to be protected. As with pagers, information stored on these cell phones also needs to be protected.

Most web-enabled cell phones and wireless PDA's access the web through a WAP browser. WAP (Wireless Access Protocol) is a set of specifications for producing web-based content for the form factor of a cell phone or PDA. One of these specifications is the Wireless Markup Language (WML), which is an XML-based specification for describing web content, layout, and navigation for a wireless device.

WML version 1.2.1 includes Wireless Transport Layer Security (WTLS), which is a wireless version of TLS (Transport Layer Security). TLS is equivalent to SSL 3.1 (Secure Sockets Layer). WTLS can be used to provide end-to-end encryption of wireless web data. Service providers can encrypt their information at their application server, and the information is not decrypted until it reaches the appropriate web phone or PDA.

There are many vendors that incorporate WTLS as plug-ins into existing web-enabled applications and application servers. Some of these vendors include Baltimore Telepathy (http://www.baltimore.com), Diversinet (http://www.dvnet.com), and EZOS (http://www.ezos.com). These vendors provide toolkits that allow developers to integrate WTLS with little or no knowledge of the underlying security technology.

One of the more common wireless web browsers in cell phones is the Openwave Mobile Browser, from Openwave Corp (formerly phone.com). The Openwave Mobile Browser supports WML and WTLS, so secure transmissions can occur with cell phones containing this browser. The Openwave Mobile Browsers are used in over 75% of the world's web-enabled cell phones, including AT&T Pocketnet-enabled phones, and Sprint PCS phones (http://www.openwave.com/about/customers/devices/device_chart.html)

A popular browser and service for wireless PDA's is the Go.Web browser and the GoAmerica service. The Go.Web browser, which is available for Blackberry RIM devices, PalmOS devices, PocketPC devices, and other devices, encrypts all web browser data between the PDA and the Go.Web proxy server (http://www.goamerica.net). This technology allows the wireless data to be encrypted, but sensitive data that is encrypted by a web server (using SSL) must first be de-crypted at the Go.Web proxy server, then re-encrypted for transmission over the wireless network. This security risk might be sufficient for most secure wireless access.

Another option for sending notifications to cell phones is through the use of SMS (Short Messaging Service). SMS allows a cell phone to act as a one-way pager; some cellular carriers have two-way SMS services. Someone can send a short amount of text to a wireless device (usually no more than 100-200 characters per message). Many cell phone carriers provide a unique email addresses for each phone so their customers can receive SMS notifications via email. An important security note is that SMS notifications are not encrypted. There is no encryption standard for SMS, and there is not likely to be one in the future.

A future area of security with web-enabled cell phones and wireless PDA's is in the VPN technology. In the future, these devices may come enabled with VPN (Virtual Private Network) technology, which will allow the device to create end-to-end encryption with a VPN server internal to an organization's network infrastructure. This would encrypt all data sent over the wireless network and the wired connection between the carrier and the application server. VPN software already exists for some PDA's, and perhaps soon it will exist for cell phone browsers too.

It was mentioned in the discussion above of pager security that protection of the data within the pager is also an important security consideration. With wireless web access, and especially with a PDA, protection of the data in the device is extremely important. A PDA can contain a user's address book, email, calendar, plus other personal data. Additionally, business applications and their data can reside on these devices.

As with the pager, the current solution is to use a password for the device. The owner must enter their PIN to gain access to the data and/or applications stored on the device. In the future, biometrics will be useful not only for PDAs but also for web-enabled cell phones.

Another technology that is being developed is the use of Smartcards to protect data and access to data on PDA's. Most PDA's have expansion slots that can accommodate PC/MCIA cards, other flash-ROM cards, or other types of accessory cards. Through these expansion slots, a Smartcard can be inserted into the PDA. Upon successful authentication with the Smartcard, the device would then grant the user access to stored information and applications. The Smart card

improves security by combining something the user physically has (the card) with something the user knows (a password). Both are required to unlock the device, and compromise of either one individually does not compromise the device.

4.3.2.4.3 Wireless LAN access

Until a few years ago, LAN access was limited to the wired world. With the advent of the 802.11b standard, almost any desktop or laptop computer can now connect to a LAN via a wireless network. All an organization must do is deploy access points throughout their location, and connect devices to them. The 802.11b standard ensures interoperability between wireless network interface cards (NIC) and access points from different vendors.

There are some security issues with 802.11b networking. This wireless network requires that the NIC be fairly close to the access point. However, it is possible for someone in a parking lot outside of a facility to use a wireless NIC to gain access to a wireless network inside the facility. Therefore, we must protect the wireless network, since access to a wireless network often gives access to the entire wired network as well.

The 802.11b standard provides for encryption through the WEP protocol (Wired Equivalent Privacy). Although WEP provides for medium encryption (40-bits) and higher encryption (128 bits), it has been proven that WEP encryption can be defeated (95680.pdf). Therefore, it is recommended that the wireless networks use Virtual Private Network (VPN) software, the same security measures used to protect wired networks. VPN software provides end-to-end encryption between two pieces of network equipment. VPN client software should be installed on any machine using an 802.11b wireless networking adapter. Before network access is granted, a VPN connection must be established to a VPN server inside the organization's corporate network. By using VPN in this way, a compromise to the wireless network would not permit access to the main corporate network. Further, any network traffic broadcasted over the wireless network cannot be intercepted.

Besides the 802.11b standard, there are several other technologies being developed as potential future standards. These include the Bluetooth specification, HiperLAN2, and the other protocols in the 802.11 family (802.11a, 802.11d, 802.11e, 802.11f, and 802.11g) (89978.pdf, pages 8,9)

4.3.2.4.4 Part 4 – Other

One vulnerability with wireless networks is denial of service attacks. All wireless devices operate at specific frequencies in the frequency spectrum. If someone wanted to maliciously prevent wireless communications from occurring they could use a frequency jammer to prohibit communications from occurring at certain frequencies.

Another vulnerability exists with traffic analysis. Without even knowing the specifics of what information is being transmitted, an intruder might be able to figure out certain characteristics of an organization's mission or plan. For example, periods of high activity in wireless transmissions from a military institution might tip off the enemy that a mobilization is about to take place.

DARPA is currently funding research at Texas A&M University to study these and other areas of wireless security. They are attempting to come up with countermeasures and detection schemes for both denial of service and traffic analysis for wireless networks. (Zhao and Duffee, 2000).

4.3.2.5 Real-Time Collaboration

Situational awareness for distributed operations extends beyond just providing alert notification and response. We found that many Air Force operational activities involve collaboration among team members (e.g., commanding, complex anomaly resolution), so our software must allow team members to work together from distributed locations.

In general, groupware refers to computer capabilities that enable or support group members in achieving their shared goals together, electronically (Ellis, Gibbs, Rein, 1991). Types of groupware support can be effectively categorized by sorting the user interactions by whether they: (1) occur in the same place or different places and (2) occur at the same time or different times, as shown below in Table 1.

SERS required only asynchronous, distributed communication. The NASA SERS system only provided the single rudimentary groupware capability of threaded discussions (e.g., posting of a primary document, and then posting responses to that primary document underneath the original post). This was sufficient for the NASA environment because the operations teams are very small and rarely need to collaborate when not in the same room. Most of the other interactions in NASA operations centers are asynchronous and fall into the lower right-hand box in Table 1, below. Thus, a threaded discussion tool has been sufficient for our NASA customer's needs.

Table 1. Groupware Taxonomy

	Same Time	**Different Time**
Same Place	Interaction: Synchronous (Face-to-Face)	Interaction: Asynchronous, Together
Different Place	Interaction: Synchronous Distributed	Interaction: Asynchronous, Distributed

In contrast to NASA, we found that the Air Force operations environment entails larger groups of people working more closely as teams. As such, groupware for Air Force operations will need to support both synchronous and asynchronous interactions.

In Phase I, we proved that synchronous groupware capabilities could be added to FASAT. We incorporated two basic capabilities: "awareness" and "chat" functions. These capabilities provide basic support for distributed synchronous collaboration. Awareness can be defined as the "understanding of the activities of others" which "provides a context for your own activities" (Dourish and Victoria Bellotti, 1992). Without awareness, electronic groups would find it difficult to know who is on-line and what they are doing. The Chat capability provides an electronic mechanism for group conversations.

The Air Force would benefit from real time collaboration tools. Satellite operators, engineers, and other staff involved with satellite operations could work together more effectively. There are a variety of tools available in the marketplace today. mFI selected Lotus SameTime as the recommended product because of its the rich feature set and because of its strong security capabilities.

Real time capabilities in the Sametime product include awareness, instant messaging, chat, a shared whiteboard, application/screen sharing, audio conferencing, and video conferencing. For Phase I of this SBIR, we have demonstrated how awareness and instant messaging and chat capabilities could be incorporated into FASAT. In future phases of SBIR activities, mFI will investigate how the other tools can be applied.

SameTime has several features, which enhance security. A basic feature of SameTime is password authentication. In order to gain access to the SameTime tools, one must login with a username and password. SameTime can also integrate seamlessly with a Domino-based application such as FASAT, so a single sign-on mechanism can be used to facilitate SameTime authentication.

When team members engage each other with personal instant messaging or group chat sessions, the text in these messages is encrypted when it goes across the network to each team member's computer. SameTime 2.5, the current version of SameTime, uses 128-bit encryption.

SameTime meeting facilities, which include shared whiteboard, application/screen sharing, audio conferencing and video conferencing also support encryption of information over the network. With the meeting facilities, encryption is optional, since the encryption has a greater impact on performance. An administrative option on the server can change all SameTime meeting facilities to always use encryption. When encryption is used, SameTime 2.5 uses 128-bit encryption.

SameTime supports situational awareness because the users know who is online at any given moment. This allows users to be aware of which of our team members to call for help, ask for support, or collaborate with. SameTime also includes security features that allow team members to specify which other team members can see if they are online or not. For example, if John Smith only wants Jane Doe and Jack Jones to know when he comes online or goes offline, John can specify Jane and Jack in his SameTime security options. If Cathy Clark wants to see if John Smith is online, she will not be able to determine his online availability since John did not grant this ability to Cathy. Each team member has three options: to allow anyone to see if they are online, to specify a subset of people who are permitted to see if they are online, or to specify a subset of people who are blocked from seeing if they are online.

4.3.3 Conclusion on Feasibility

From our Architectural Study, we determined that it is feasible to architect a FASAT system to be used for Air Force Operations.

The core alerting technology in FASAT is applicable to Air Force workflow. Several pieces of functionality added to the system in Phase I are of use to the Air Force, including the integrated anomaly tracking system based on existing Air Force tracking tools and the real-time collaboration tools for situational awareness.

Several other issues will need to be addressed for an operational FASAT system. They include building a near real-time interface to COBRA data and implementing the necessary wireless security, but none of these issues are insurmountable.

4.4 Prototype

mFI used the results of the human effectiveness and architectural studies to determine what capabilities needed to be prototyped to prove the feasibility of our Phase I research. We determined that the ability to maintain near-real-time situational awareness will be the key to enabling distributed on-demand space operations for the Air Force. This means that no matter where crewmembers or support personnel are located, when there are anomalous conditions, the required personnel can: 1) be reached to respond to unplanned events (i.e., anomalous conditions), 2) be able to access the necessary data from wherever they are physically located to perform their jobs, and (3) easily understand the information presented to them to rapidly respond.

In Phase I, the primary goal of our prototyping effort was to prove that situational awareness could be maintained in a distributed environment without jeopardizing high-value assets, like satellites. This focus on providing a platform to support near-real-time distributed situational awareness has lead us to name our software FASAT (Fast Access Situation Awareness Testbed).

Our basic approach was to prototype new capabilities on top of the operational Spacecraft Emergency Response System (SERS) software that our staff developed for NASA, as shown in Figure 9. SERS is an innovative Web-based suite of tools that automates many of the monitoring, reporting, notification, and team management activities required in a lights-out environment. When SERS detects an anomaly, it dynamically builds an appropriate response team based on (1) the type and severity of the problem and (2) the skills, availability, and communications devices of the on-call team members. SERS then enables them to work together as a remote, distributed team via wireless devices.

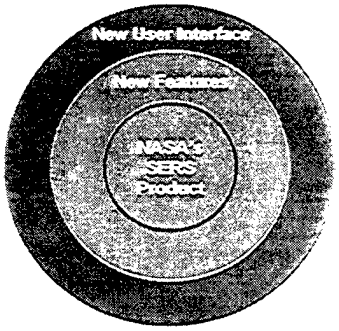


Figure 9. Prototype Design Methodology

The primary advantages of this approach were that mFI was able to:

- Transfer NASA's significant investment in the SERS system to the Air Force
- Focus on the key new technologies, instead of infrastructure
- Demonstrate a functional prototype, instead of just a conceptual design

In particular, the prototype demonstrates the ability to:

- Support distributed situational awareness through wired and wireless interfaces
- Have a tailorable user-system interface
- Work with Air Force satellite ground systems (i.e., CERES' COBRA)
- Support secure real-time distributed collaboration
- Automate routine reporting
- Support Air Force workflow

4.4.1 Scenarios

mFI decided to base its demonstration of the FASAT software on scenarios derived from the *Anomaly Resolution for Mission Controllers* (CERES Ops-006.doc) process flowchart. That flowchart, shown in Figure 10, provides the basic sequence of steps that should be followed for any anomalous condition.

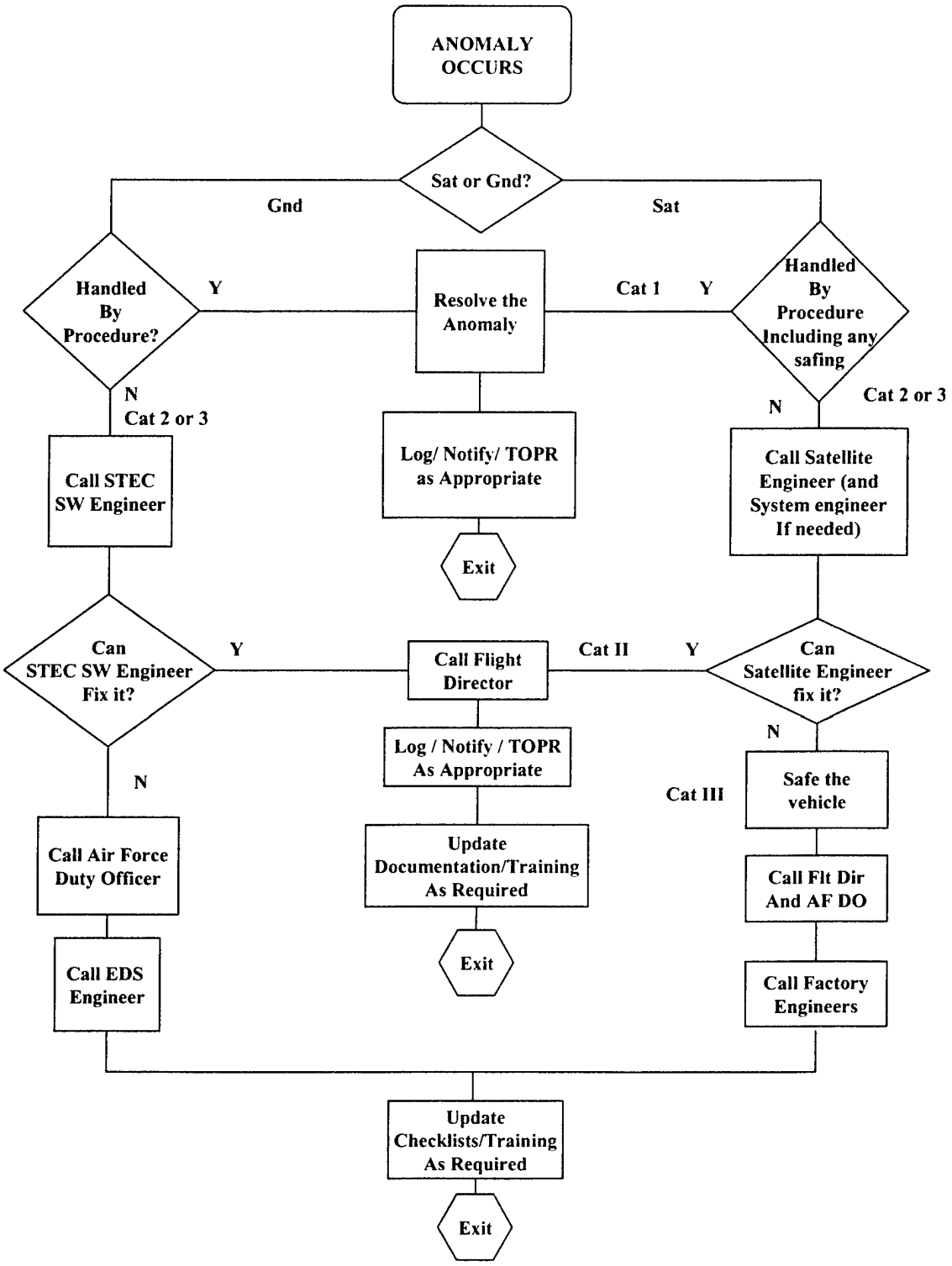


Figure 10. Anomaly Resolution for Mission Controllers

The first scenario demonstrates the workflow associated with identifying and responding to an anomaly which has a known corrective procedure, shown Figure 11.

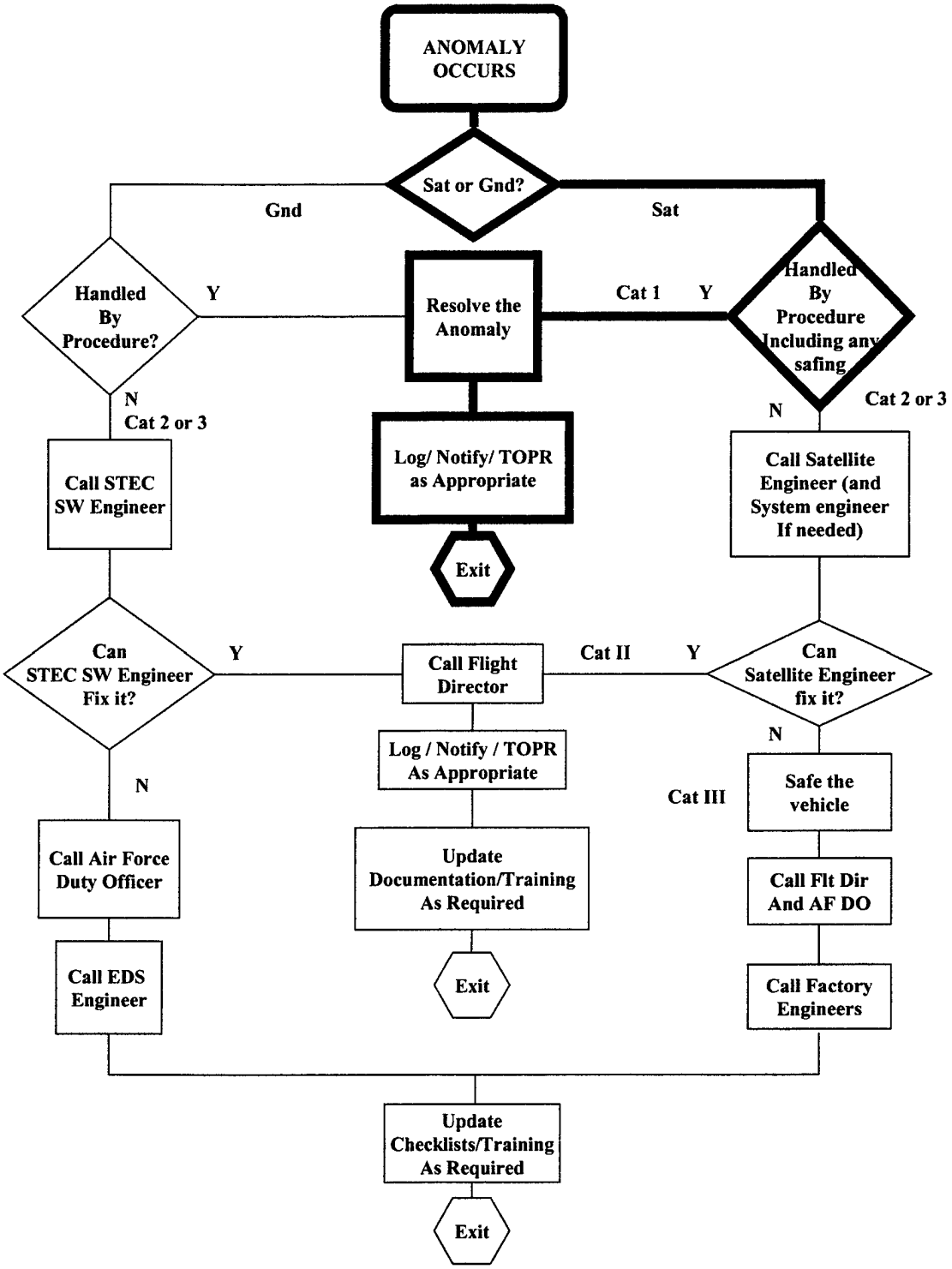
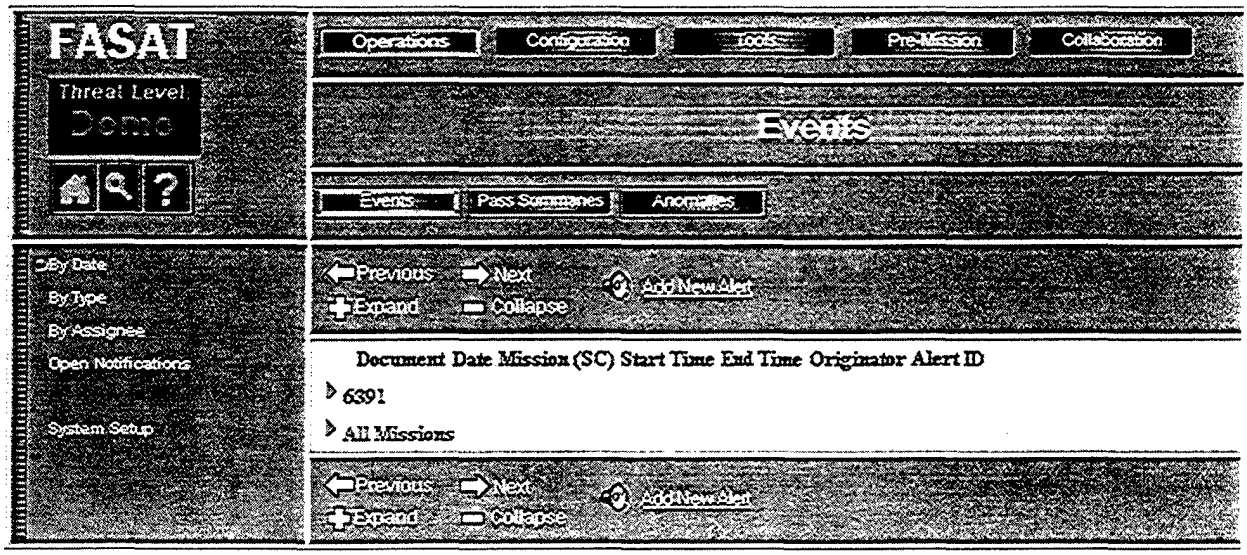
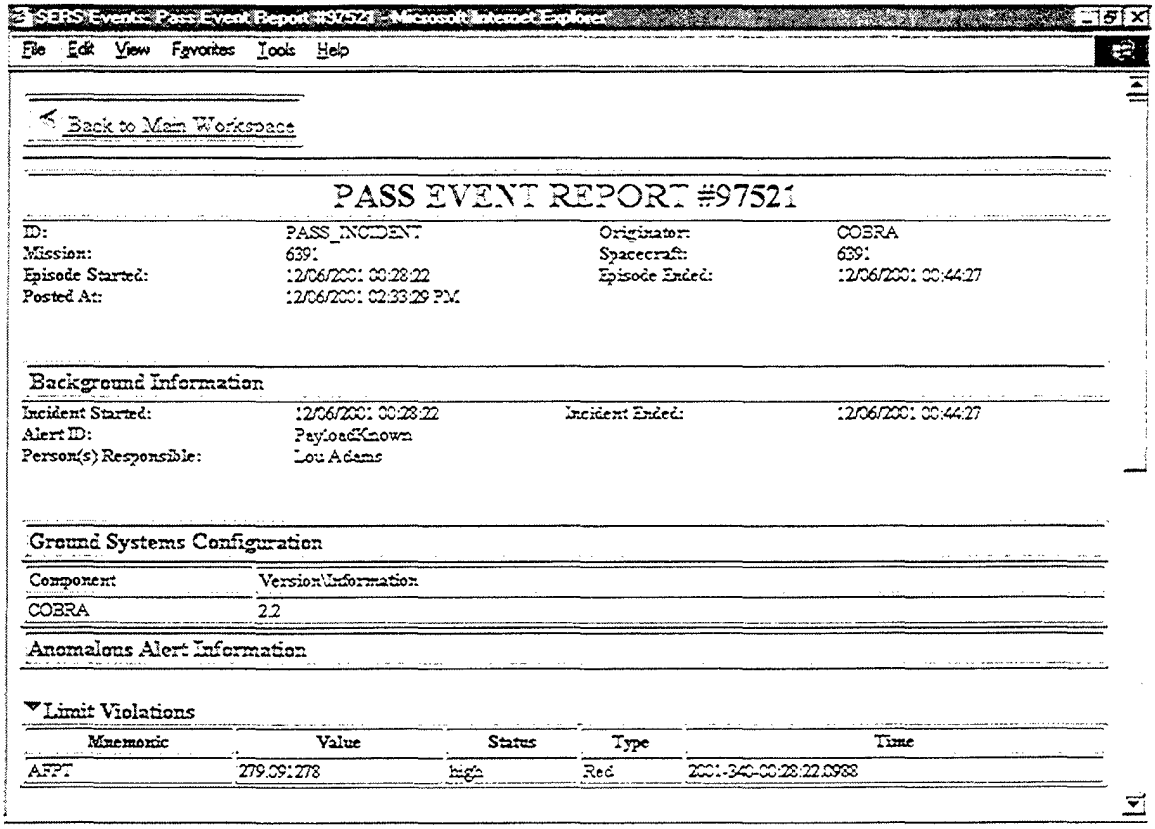


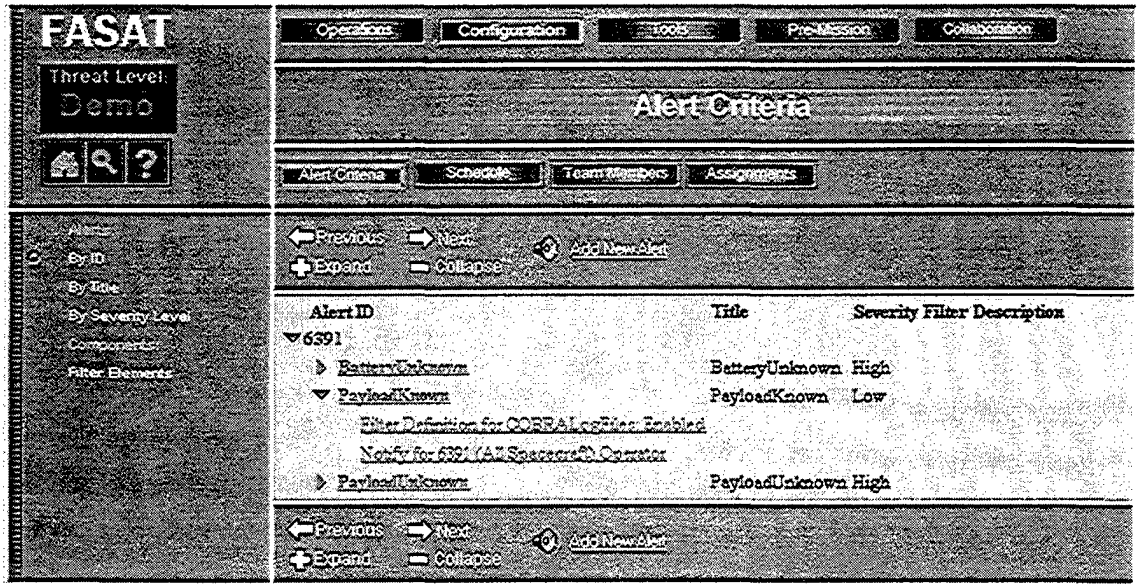
Figure 11. Flowchart for Scenario 1.

For this scenario:
1. FASAT parses a COBRA data file to identify anomalous data for Satellite 6391 (not shown).
2. FASAT automatically fills-in an Event report, logging the anomalous data.

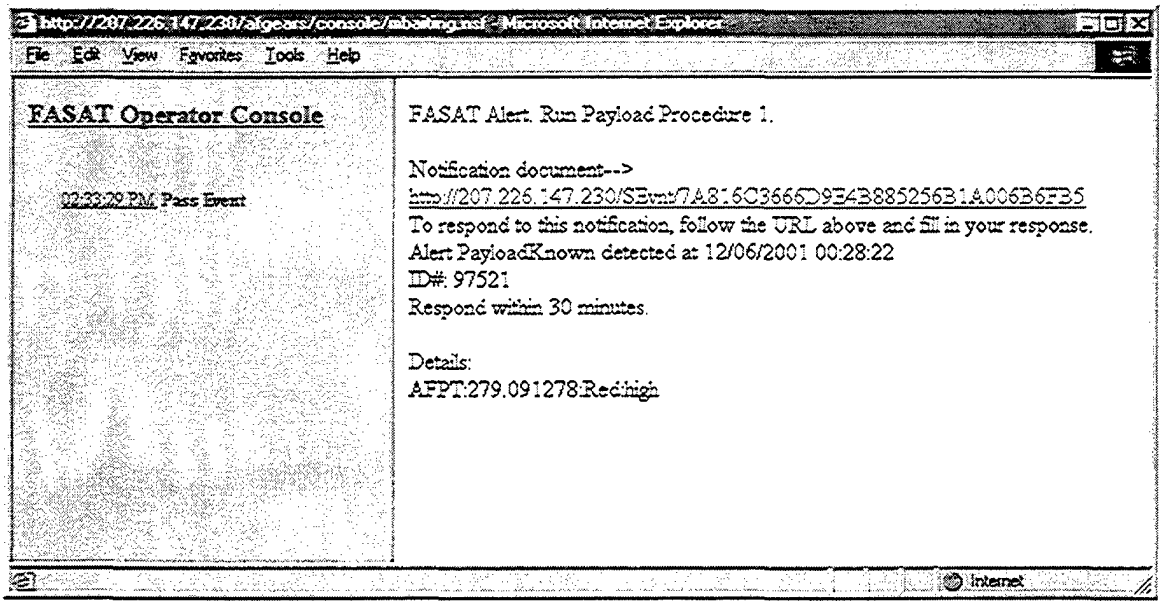




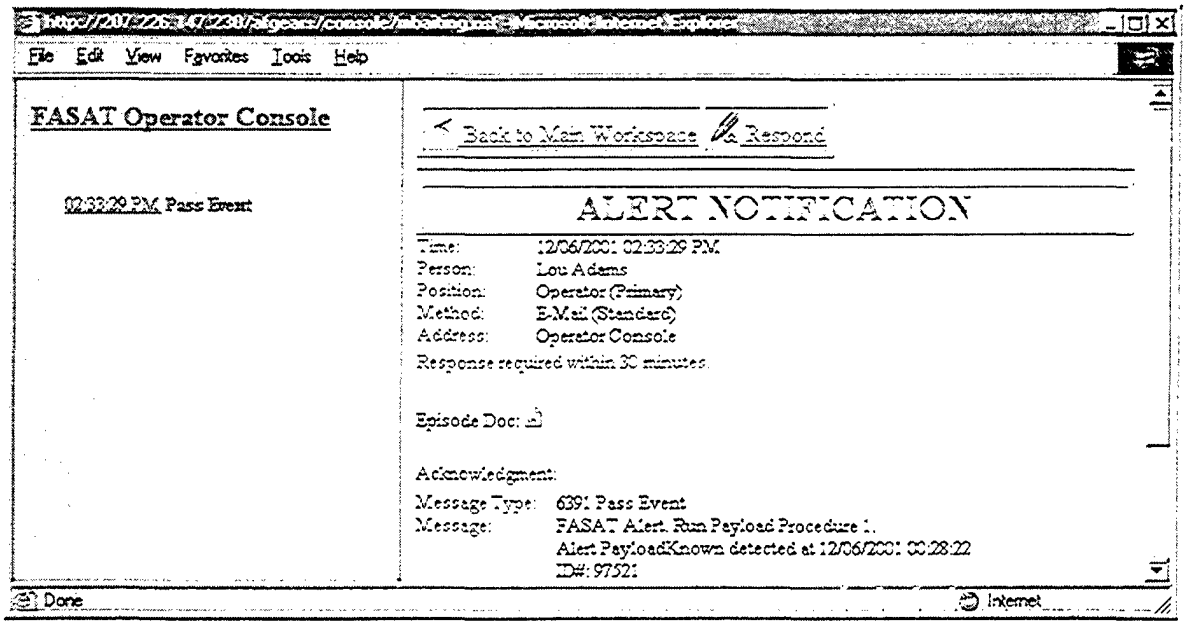
3. FASAT then checks its alert criteria to determine whom to notify for this known anomaly. In this case, only an operator needs to be notified.



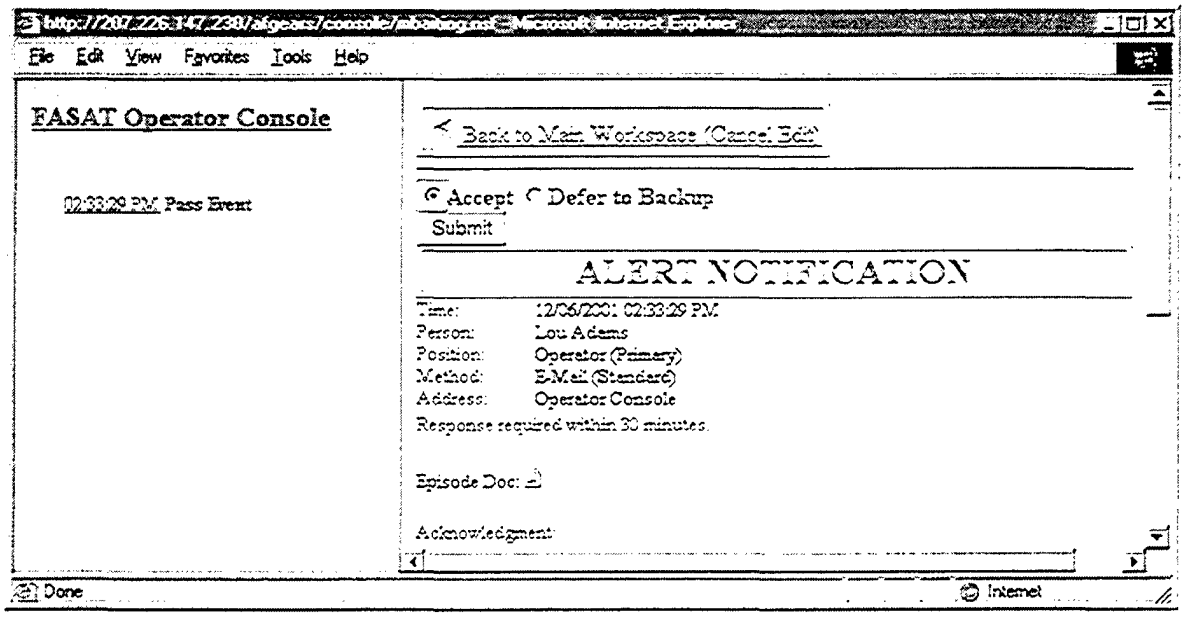
4. Next, FASAT pops-up an Alert Console for Operator in Control Center. The Alert tells the operator there this a KNOWN procedure that should be run in response to the anomaly.



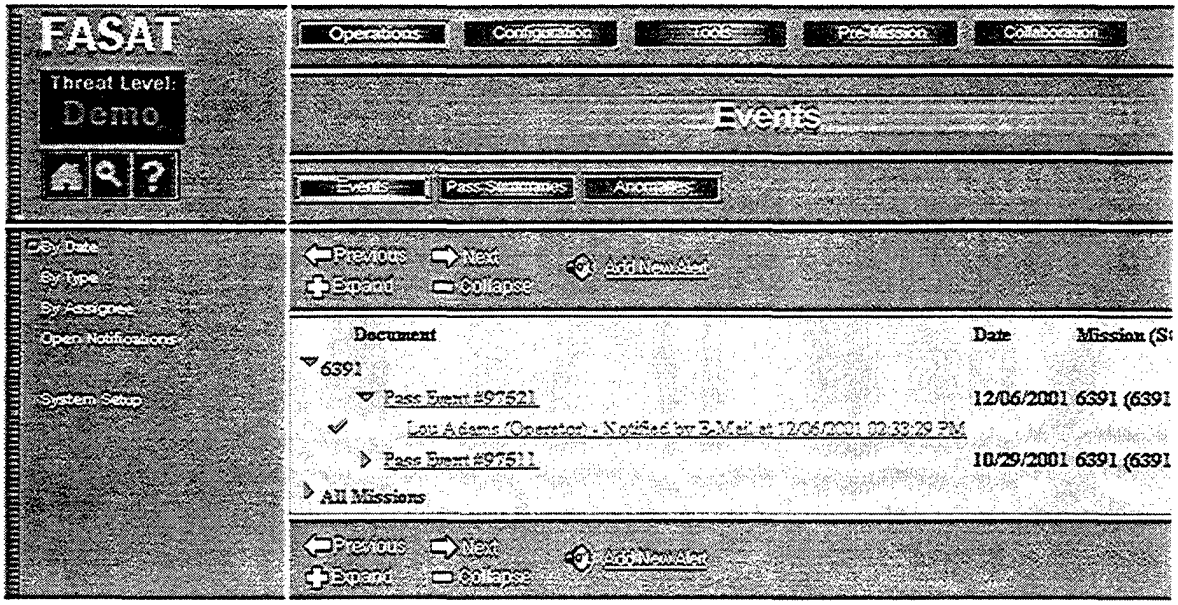
5. By clicking on the provided URL, the operator views the details of the alert notification



6. Next, the operator accepts responsibility for the alert notification.

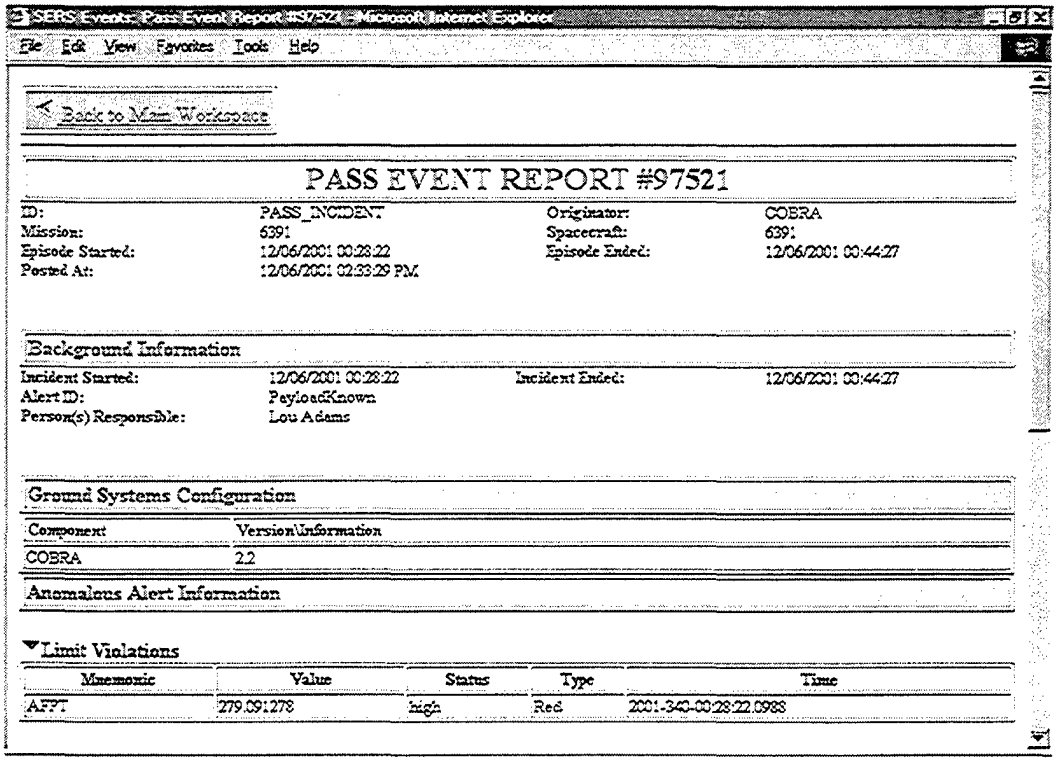


7. FASAT then logs the operator's acceptance (shown by the check mark in front of his name).

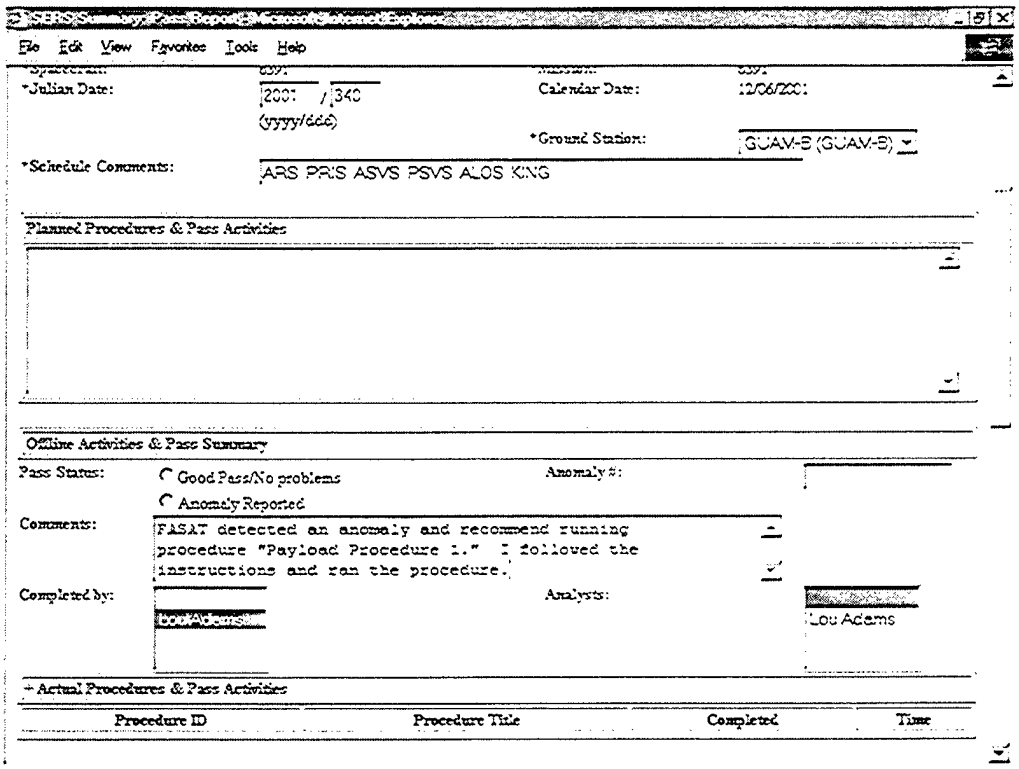


8. Next, the operator enters the corrective procedure in ground system (not shown).

9. FASAT automatically fills-in a pass summary.



10. The operator then modifies the pass summary to reflect that he ran the procedure.



The second scenario demonstrates distributed operations to resolve a new anomalous event with no known specified response procedure, shown in Figure 12.

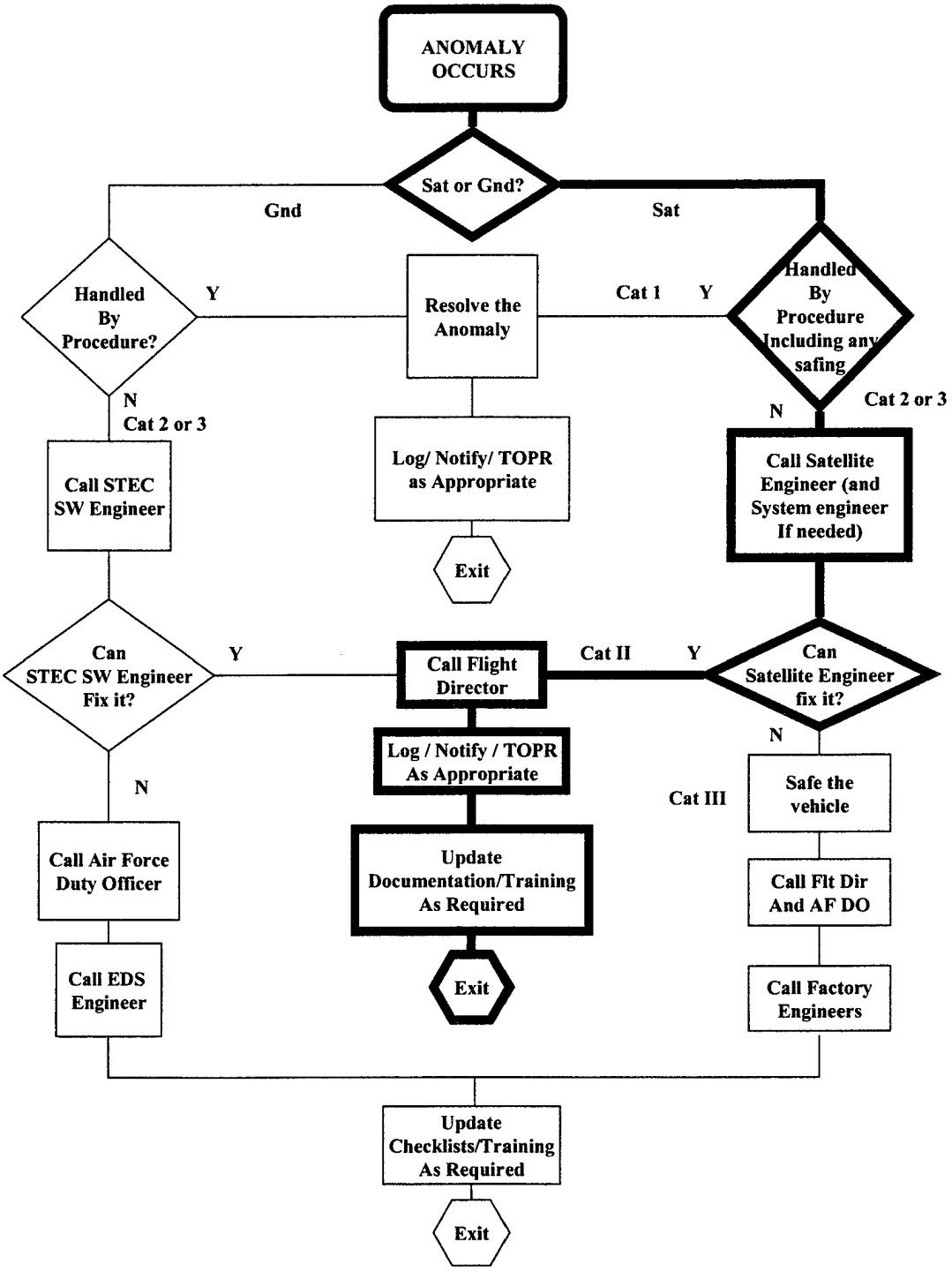
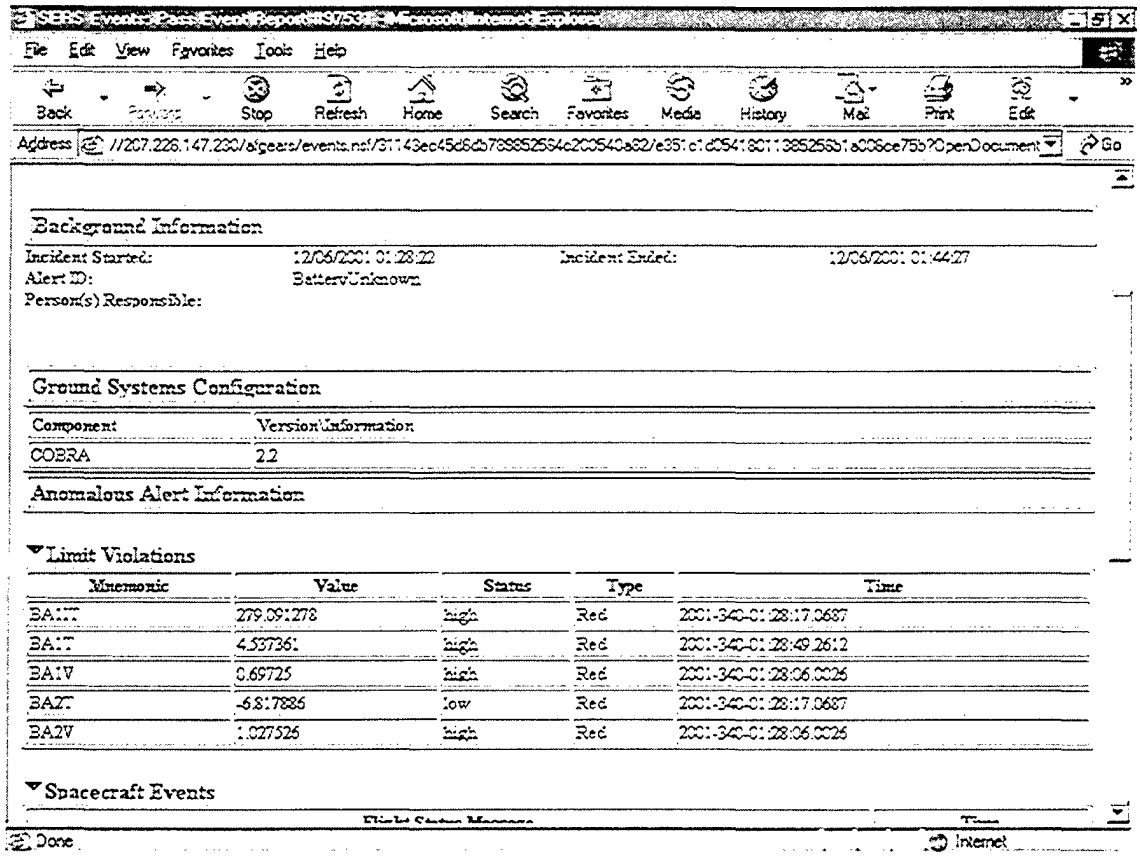


Figure 12. Flowchart for Scenario 2.

For this scenario:
1. FASAT parses a COBRA data file to identify anomalous data for Satellite 6391 (not shown).
2. FASAT then automatically fills-in an Event report, logging the anomalous data (note limit violations for the battery voltage).



Background Information

Incident Started:	12/06/2001 01:28:22	Incident Ended:	12/06/2001 01:44:27
Alert ID:	BatteryUnknown		
Person(s) Responsible:			

Ground Systems Configuration

Component	Version\Information
COBRA	2.2

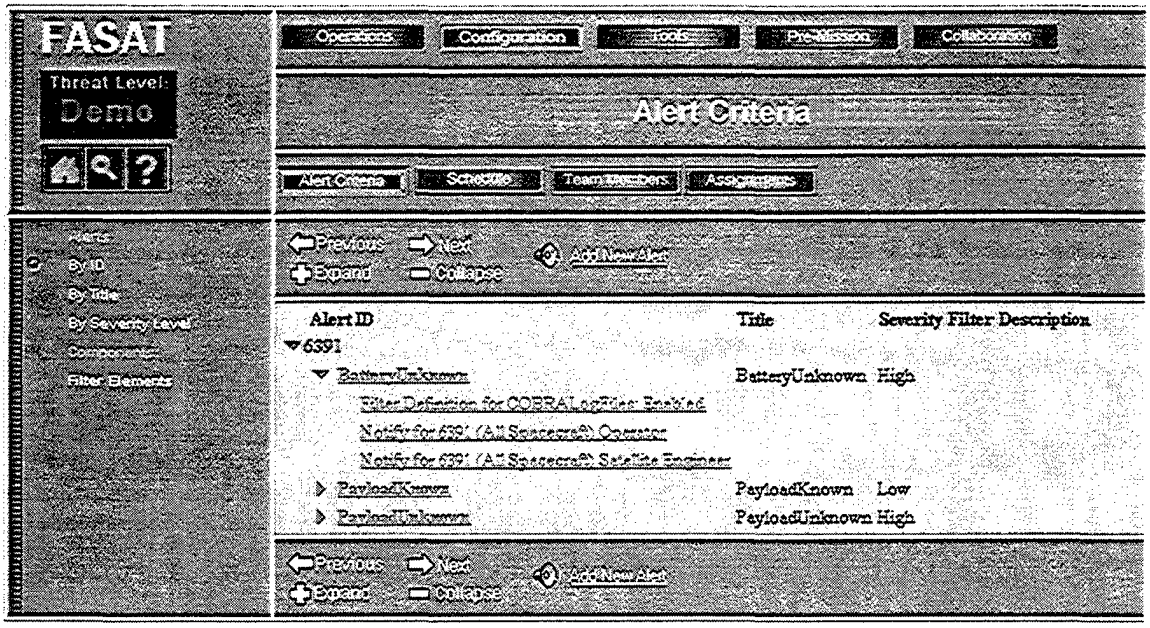
Anomalous Alert Information

Limit Violations

Mnemonic	Value	Status	Type	Time
BA1T	279.091278	high	Red	2001-340-01:28:17.0687
BA1T	4.537361	high	Red	2001-340-01:28:49.2612
BA1V	0.69725	high	Red	2001-340-01:28:06.0026
BA2T	-6.817886	low	Red	2001-340-01:28:17.0687
BA2V	1.027526	high	Red	2001-340-01:28:06.0026

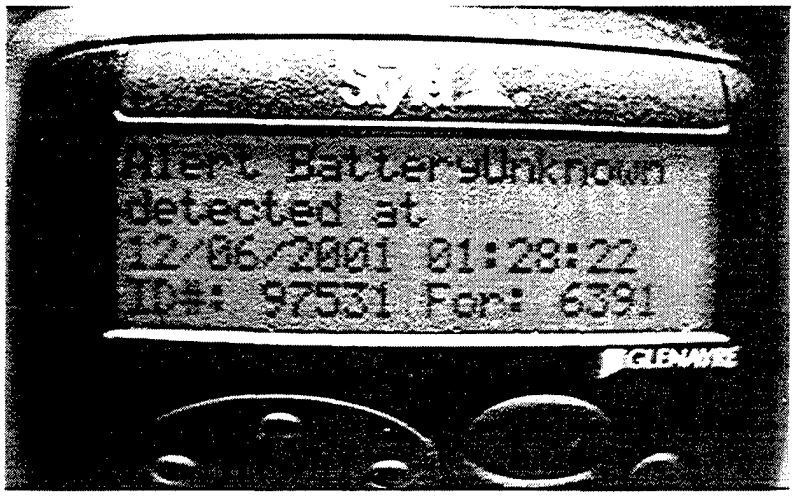
Spacecraft Events

3. Next, FASAT checks its alert criteria to determine whom to notify for this known anomaly. In this case, both an operator and an engineer need to be notified.



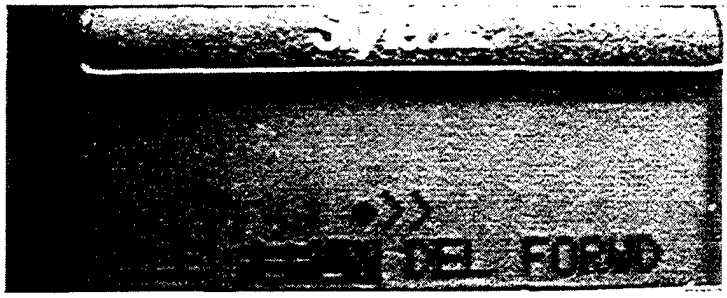
4. To notify the operator, FASAT pops-up an alert on the operator's console. The Alert tells the operator that there is an UNKNOWN anomaly, so no procedures are suggested. (Not shown, see step 4 in previous scenario).

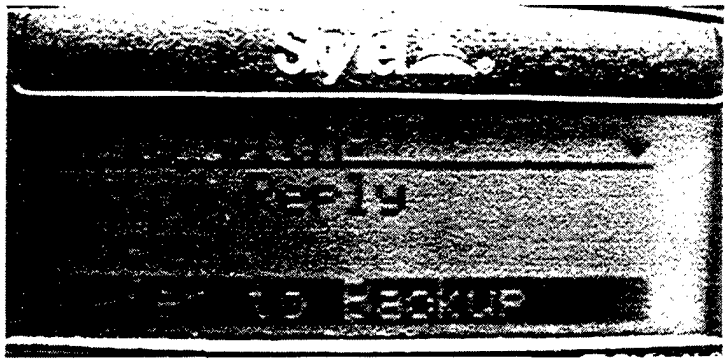
5. FASAT pages a satellite engineer.



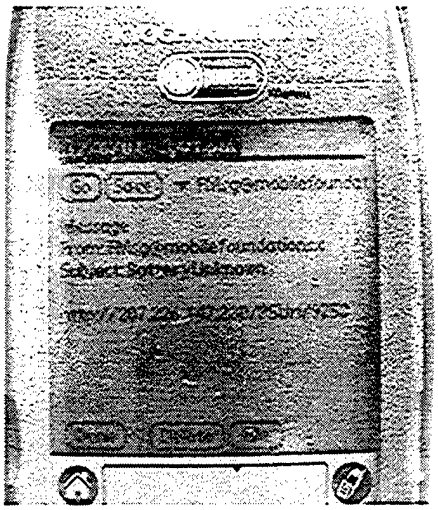
6. The engineer scrolls down to see that he has 10 minutes to respond. He also can see that the battery telemetry is included in the message.

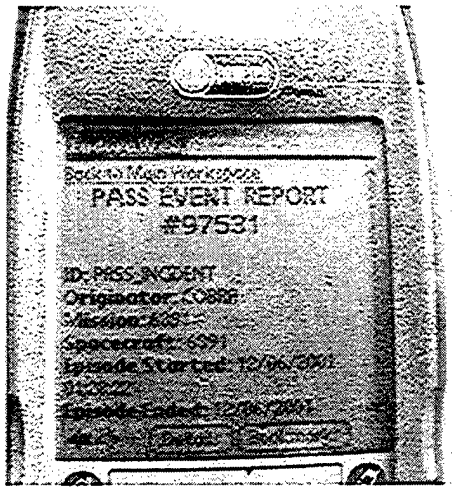
7. In this scenario, this engineer cannot handle this anomaly, so he replies to the page by deferring to another engineer.



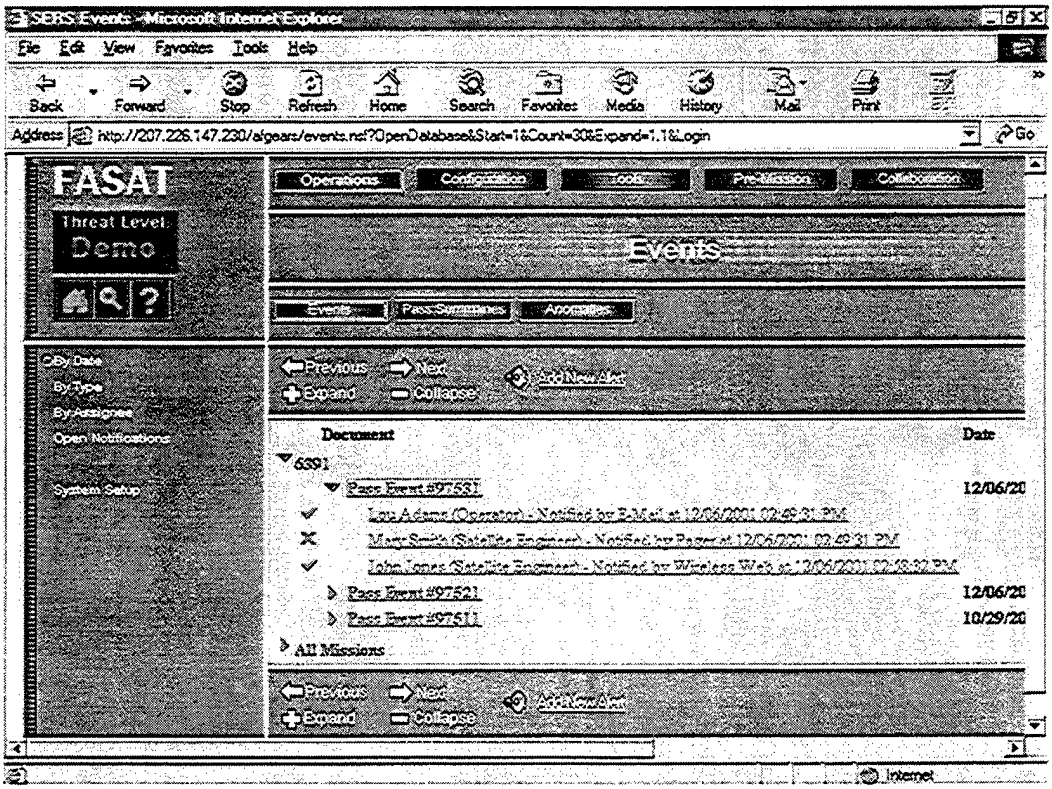


8. Upon receiving the wireless message back from the first engineer, FASAT automatically notifies a backup engineer via a Web-enabled phone. That engineer receives the alert as an SMS message. That message has a URL. By clicking on the URL, the operator can now browse back to FASAT on the phone.

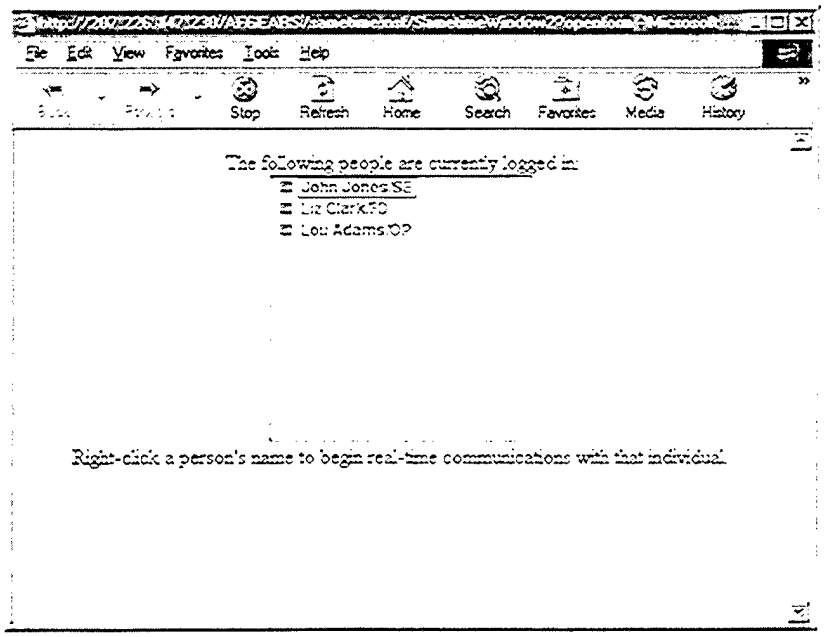




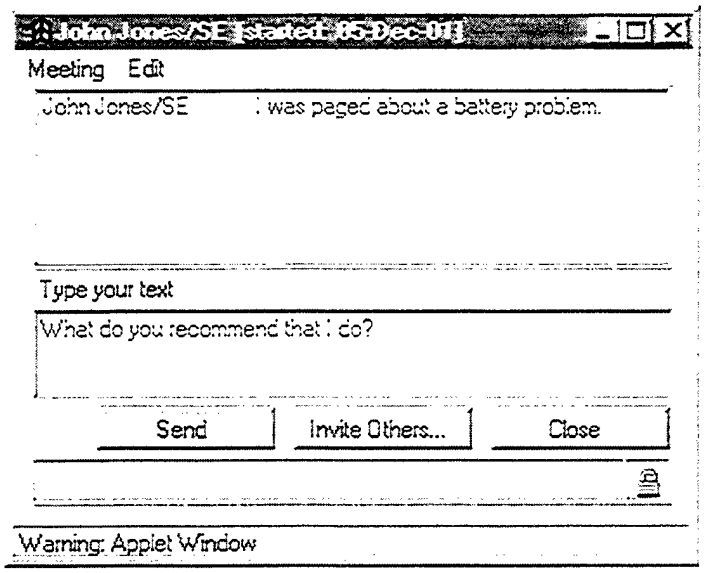
9. FASAT logs who has accepted and who has deferred.



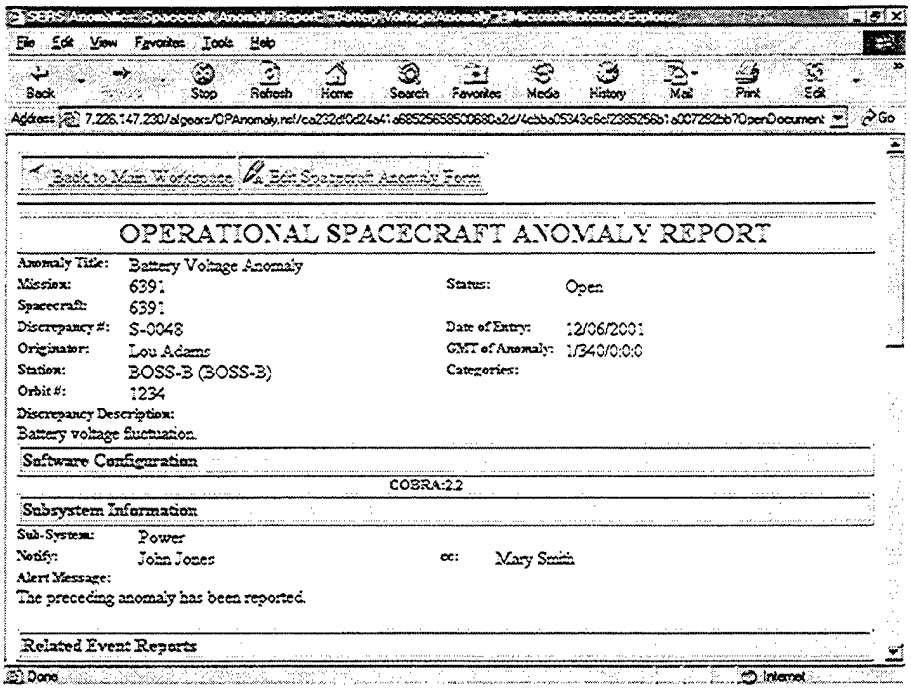
10. The engineer, located in another building, launches FASAT's awareness tool to see which operator is on console.



11. The engineer tells the operator to fill-in the basic elements of an anomaly report.



12. The operator fills-in basic elements of the report. The operator assigns the report to that engineer (John Jones).



OPERATIONAL SPACECRAFT ANOMALY REPORT

Anomaly Title:	Battery Voltage Anomaly		
Mission:	6391	Status:	Open
Spacecraft:	6391		
Discrepancy #:	S-0048	Date of Entry:	12/06/2001
Originator:	Lou Adams	GMT of Anomaly:	1/340/0:0:0
Station:	BOSS-B (BOSS-B)	Categories:	
Orbit #:	1234		

Discrepancy Description:
Battery voltage fluctuation.

Software Configuration

COBRA:2.2

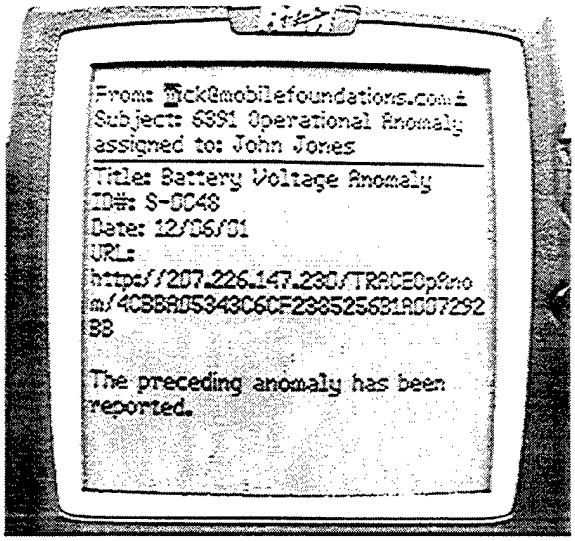
Subsystem Information

Sub-System:	Power		
Notify:	John Jones	cc:	Mary Smith

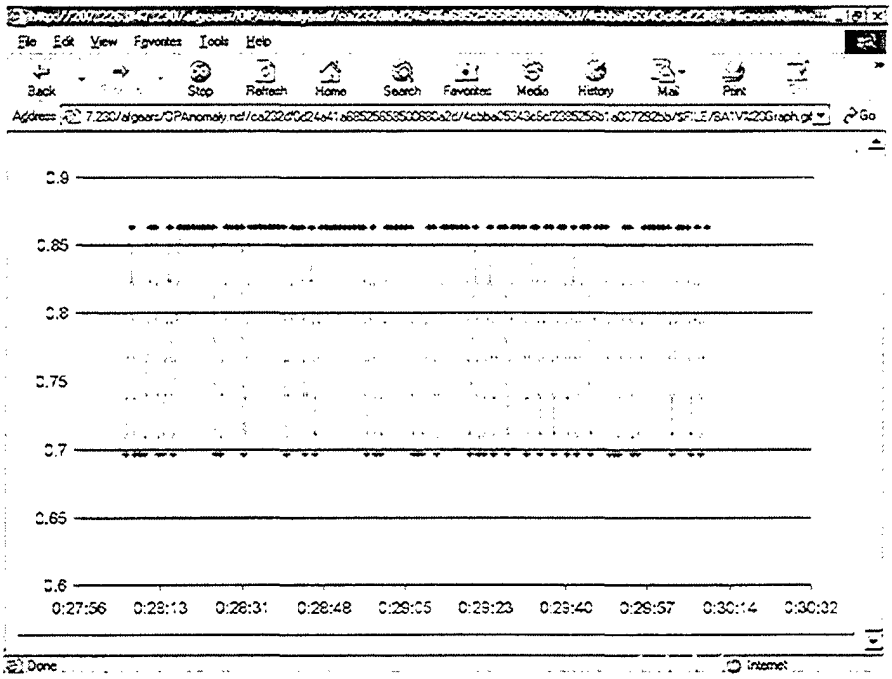
Alert Message:
The preceding anomaly has been reported.

Related Event Reports

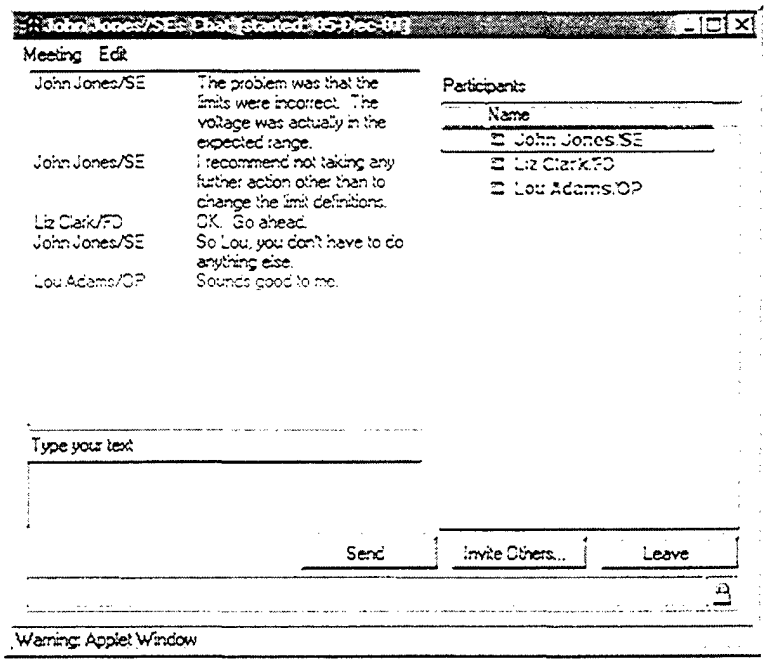
13. Once the operator submits the report, FASAT sends a message to the engineer (in this case to his RIM pager) telling him to enter his diagnosis.



14. After the engineer finishes his diagnosis, he inputs the results into FASAT, including the output of the model used to reach the conclusion.



13. The operator, engineer, and flight director discuss the engineer's diagnosis. The flight director then approves the engineer's recommendation. This chat capability allows people to communicate without being in the same location.



5. Recommendations for Follow-on Work

5.1 Human Effectiveness Activities

The main human effectiveness issue that will drive the success of FASAT for the Air Force will be how to design a user interface to support distributed near-real-time alerting. The critical challenge is how to handle cases where mnemonics fluctuate in and out of bounds multiple times and the inherent latency of alerting mechanisms. This is a new challenge that has not affected the NASA SERS users because the NASA software only performs its analyses of the spacecraft data one time, post-pass, for each satellite. Thus, the software only need to alert the users just once, no matter how many times a mnemonic goes out of bounds. For the Air Force, future human effectiveness analyses will have to address the frequency of alerting. It may be that some groups, such as the operators, need alerts more frequently than other groups such as engineers.

5.2 Architecture Activities

The four main architectural issues that need to be addressed in future work are (1) security, (2) real-time alerting, (3) real-time collaboration, and (4) integration into actual Air Force control centers.

Architecture specialists will need to survey the state of the art in wireless security and review the results from the human effectiveness studies. From that, a security scheme should be recommended and implemented.

Much of the human effective work will be to define an appropriate solution for real-time alerting, as discussed in section 5.1. The architectural issues will be to implement the solution defined by the human effectiveness specialist. In particular, the architectural work will focus on:

- How do we acquire the necessary data in real time?
- How do we process or filter that data for relevant information?
- How do we define and perform alerts on the data coming in real-time? When and how often do we alert on anomalous conditions?

The future work will also have to address real-time collaboration. In order to support a more distributed operations team, any system implemented will need to incorporate tools to help the team collaborate remotely. The architectural work will need to focus on building and implementing the tools that can help support that team collaboration, while not increasing the complexity of the software.

Architectural work will need to be done to implement a system in an actual Air Force control center. A system will need to be able to work with existing Air Force systems. It also must be able to work within and conform to existing network security within the control centers. In particular, it must work with any firewalls and private networks used in the control centers or by controllers.

Throughout this architectural work, it will be important to work with and receive input from the human effectiveness specialist. This will insure that the architecture developed will conform to the users needs and that user centered design process is maintained.

6. Conclusion

The general conclusion from our Phase I effort is that the Air Force is in need of new forms of automation to further improve the effectiveness of its mission operations. Many of the currently deployed ground system components are dated and have significant limitations. However, we also learned that over the next five to ten years, many of the older systems will be replaced. Thus, now is the perfect time to perform the research and development necessary to both infuse specific new technologies and help the Air Force define operations concepts for the future, including distributed operations. In particular, we found that the Air Force requires new tools to enable increased productivity, such as:

- Improved situational awareness – tools that quickly notify the users of problems (anomalies), and allow them to assess the situation and respond to the current status of any given situation from wherever they are located.
- Automation – tools to automate routine and mundane tasks (such as filling out standard forms), so that the personnel can perform more valuable work.
- Job Aids – on-line tools that can guide the operators in decision support.
- Distributed team collaboration – tools that allow any combination of operations personnel (console operators, on-site engineers, and offsite staff) to work together in a more efficient manner.
- Security – tools that improve or enhance operations cannot do so at the sake of reduced security.

Therefore, the Air Force has to address a variety of issues to make progress towards its Vision of next-generation mission operations. In particular, the Air Force needs more advanced tools to enable distributed operations. Our Phase I effort has shown that an Air Force software system based on mFI's' SERS product is not only feasible, but will prove to be successful in terms of providing essential new functionality in a cost-effective manner.

That software initial proof-of-concept software, called FASAT (Fast Access Situational Awareness Testbed), builds on the core SERS technology and added:

- A basic interface into CERES COBRA ground system
- A New user interface
- On-console situational awareness support (pop-up alerts)
- Basic synchronous collaboration tools
- Support for Air Force Workflow.

Thus, mFI was able to prove that its approach to infusing advanced automation and enabling distributed operations is not only feasible, but also practical and beneficial. Through follow-on reach and development activities, the FASAT software will enable the Air Force to achieve its nearer-term goals of maintaining space superiority and significantly help the Air Force to transition into its longer-tern goals of next-generation on-demand space operations that provide total situational awareness.

7. References

Adams, M.J., Tenny, Y.J., and Pew, R.W. (1991). *Strategic Workload and the Cognitive Management of Advanced Multi-Task Systems*. Wright-Patterson Air Force Base, Ohio: CSERIAC Report.

Air Force Space Command (2000). *Strategic Master Plan (SMP) for FY02 and Beyond.*

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 & Operations*, Oxford, England.

Bane, R. and Fox, J. A. (1996). The design and implementation of the VMOC prototype. *4th International Symposium on Space Mission Operations and Ground Data Systems: SpaceOps '96*, Munich, Germany.

Breed, J., Baker, B., Chu, K.D., Starr, S., Fox, J., & Baitinger, M. (1999). The Spacecraft Emergency Response System (SERS) for autonomous mission operations. *3rd International Symposium on Reducing the Cost of Spacecraft Ground Systems & Operations.* Taiwan.

Breed, J. and Fox, J. Enabling Advanced Automation in Spacecraft Operations with the Spacecraft Emergency Response System. To be published in the *2001 AAAI Spring Symposium Series on Robust Autonomy*, Stanford, CA

Dourish, P. and Bellotti, V. (1992). Awareness and Coordination in Shared Workspaces. In *Proc. ACM Conference on Computer-Supported Cooperative Work CSCW'92* (Toronto, Ontario), 107-114. New York: ACM.

Doyle, R., Chien, S., Fayyad, U., and Porta, H. (1992). Attention focusing and anomaly detection in real-time systems monitoring, *NASA/Air Force Space Operations, Applications, and Research (SOAR) Symposium*, Houston, TX, August 1992.

Dumas, J.S. and Redish, J.C. (1993). *A Practical Guide to Usability Testing.* Norwood, NJ: Ablex Publishing Co.

Ellis, L. and Gibbs, S. J. and Rein, G. L. (1991). Groupware: Some Issues and Experiences", *Communications of the ACM*, 34(1), 38-58,

Fox, J. A., Bane, R., Baker, P., Breed, J., and Baitinger, M. (1997). Human Factors Techniques for Designing the Virtual Mission Operations Center. *The 7th International Conference on Human-Computer Interaction*, San Francisco, CA.

Fox, J., Breed, J., Baitinger, M., Starr, C., Chu, C.D., Baker, P. (1999a). The Spacecraft Emergency Response System: A Web-Based System Enabling Lights-Out Automation. *AIAA Space Technology Conference*, Albuquerque, NM.

Fox, J. A., Breed, J., Baker, P., Chu, K., Starr, C. and Baitinger, M. A. (1998). Web-based Emergency Response Systems for Lights Out Operations. *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. (1999c). 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., Hoxie, M. S., Gillen, D., Parkinson, C., Breed, J., Nickens, S., and Baitinger, M. (2000). New Human-Computer Interface Concepts for Mission Operations. *Sixth International Symposium on Space Mission Operations and Ground Data Systems: 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.

Goldstein, I.L. (1992). *Training in Organizations: Needs Assessment, Development, and Evaluation*. Pacific Grove, CA: Brooks/Cole Pub Co.

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

Joint National Test Facility. (1999). *JNTF Fact Sheet 99-023*. http://www.jntf.osd.mil/Fact_Sheets/99-023.pdf.

Jones, P. M. and Mitchell, C. M. (1991). A Mechanism for Knowledge-Based Reminding and Advice-Giving in the Supervisory Control of a Complex Dynamic System. *1991 IEEE International Conference on Systems, Man, and Cybernetics*, Vol. 2, 1295-1300.

Kirwan, B. and Ainsworth, L.K. (1992). *A Guide to Task Analysis*. Washington, DC: Taylor and Francis.

Mejdal, S., McCauley, M., and Remington, R. (1999). *Advanced Interfaces for Space Operator Consoles*.

Moore, M. and Fox, J. A. (1993). The Virtual Missions Operations Center. *7th Annual Space Operations, Applications, and Research Symposium*. Houston, TX: NASA and USAF.

Price, H. E. (1985). The allocation of functions in systems. *Human Factors,* 27 (1), 33-45.

Sheridan, T. B. (1980). Computer Control and Human Alienation. *Technology Review*. 61-73.

Skvarla, C and Dooley, B. (2001). Wireless Services: United States. *Gartner DPRO-93504*. p. 15.

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

Wickens, C. D., Mavor, A. S., Parasuraman, R., and McGee, J. P. (1998). The Future of Air Traffic Control: *Human Operators and Automations*. National Academy Press. Washington, D.C.

Zhao, W. and Duffee, D. (2000). *Providing Survivable Real-Time Communication Service for Distributed Mission Critical Systems*. DARPA ITO Sponsored Research 2000 Project Summary. http://www.darpa.mil/ito/psum2000/J034-0.html.

Appendix A: Response Summaries from Contextual Inquiry

About the Users

1. *What Knowledge, Skills, and Abilities are required?*

   Operators have to learn to use the controlling tools and how to diagnose problems. They also have to work with other controllers and with the engineers to identify and resolve problems. It requires technical and analytical skills.

2. *Where do you get your training?*

   In the SOPS, the mission controllers are enlisted personnel selected based on test results. They attend several weeks of technical school run by the Air Force. Then they are assigned a squadron where they get approximately five months of on-the-job training.

   At CERES, contractors are hired for the job of mission controller. Most of these contractors are retired Air Force personnel. In general, most training is given on the job.

3. *How long do you stay at this job (how many years?)?*

   No average length, but, based on observations, most operators at CERES were fairly young (approximately 35 or younger).

4. *Do you have the authority to make decisions during a normal pass? During an emergency situation?*

   At CERES, mission controllers have the authority to make some decisions, but it depends on the level of the problem. The mission controllers are certified to respond to certain levels of problem. As they get more experience, they are certified to respond to more difficult problems. For problems they are not certified to address themselves, the mission controllers contact the engineer. In the SOPS, mission controllers have less authority, and contact specialists when there is a problem. <u>These specialists can be located anywhere on base and sometimes cannot be found during anomalous conditions.</u>

About the Environment

5. *What is the work environment like?*

   The work environment is similar to other office work environments. The actual operations center is a large room, with workstations circling the room (typical of most mission operations and command and control centers). Because there may be several people working at once in the one room, occasionally the operations center can get loud.

6. *What is the culture like?*

   In the SOPS, the responsibilities and activities are very structured and assigned to specific personnel. At CERES, operators have more responsibility and authority, and less structure.

They work on more aspects of operations, rather than focusing on a small niche, and they seem to appreciate the variety in their work.

7. *Are people working 24/7? On rotating shifts?*

   At CERES, people work in one of three shifts: 6:30 am - 2:30 pm; 2:30 pm - 10:30 pm; or 10:30 pm - 6:30 am. They work five days on, two days off, five days on, two days off, then rotate to the next shift. Basically they switch shifts in every two weeks. In the SOPS, the operators change shifts much more frequently. Although this would seem difficult, the operators we spoke with do not mind the variety in their schedule, and actually seemed to appreciate having free time during the day. Engineers work normal business hours and are on call the rest of the time.

8. *Do you work with anyone else?*

   a. *How are your duties divided?*

   At CERES, passes can be controlled by one operator, because the software tools they use are mostly point-and-click. At the SOPS, most systems require command line input, so there must be two operators for each pass - one to type in the commands and one to review commands to prevent typos.

   b. *Do you need the same or different information?*

   In the SOPS, both operators look primarily at the same information.

Preparing for a Pass

9. *How do you prepare for a pass? When? How long does it take?*

   Mission controllers review pass information provided by mission planning about one day in advance. They start setting up the system about 30 minutes prior to the pass. Aside from that, there is generally little preparation required for most passes.

During a Pass

10. *How often do you monitor passes?*

    There are about 7-8 passes in one shift at CERES.

11. *How automated are they?*

    The level of automation depends on the system being used. At CERES, the COBRA system is a collection of tools tied together via sockets. The command management portion (G2 IMT) is graphical and requires no typing, thus reducing the likelihood of data entry errors. In the SOPS, the system is command based, so every command must be entered by hand. There is almost no automation. However, the older deployed systems are due to be replaced over the next several years.

12. What is a typical task flow for a pass?

- The mission controller reviews the pass plan as much as a day before the pass.
- Approximately 30 minutes before the pass, the mission controller contacts the ground control network, the organization that receives the telemetry, to open the communication connection.
- During the pass, the mission controller uploads and downloads the data and commands.
- At the end of the pass, the mission controller contacts the ground control network to shut down the communication connection.
- At CERES, mission controller manually enters anomalies into a database called "The tool". The tool is in no way tied into the operational strings. Also, the tool provides little functionality beyond storing the anomaly data (as opposed to an anomaly management system).

a. Are pass activities fairly consistent?

They usually follow the same structure.

What can go wrong?

13. What types of things go wrong?

Sometimes ground equipment fails. Since there is no automated cataloging of ground and satellite events, we were unable to determine the frequency of ground-based events. As a point of comparison, at NASA over 50% of the events occur on the ground (from a datamining exercise using SERS for the Small Explorer (SMEX) missions at NASA). Mission controllers can often fix problems that reside in the control center themselves, but they often need job experience to know what the problem is. Sometimes they cannot fix the problem, but develop "work-arounds" using other pieces of equipment.

At CERES, when a mission controller encounters a problem, he/she is certified to results specific levels of problems themselves. If the problem is more significant, they must contact an engineer.

Today, at CERES and in the SOPS, anomaly and event notification does not go much beyond color coding of out-of-limit mnemonics or event messages on the operator's monitor. The color coding follows the typical usage of white – nominal, yellow – warning, and red -- severe. For many "red" conditions, the operators must contact the support engineers. If they must call the engineer on the telephone, the mission controller leaves a vague message to avoid breaching security.

a. What do you have to do?

See above.

14. Which events are the most difficult?

Difficult to specify. It depends on the mission.

15. Which events are the most Critical?

Difficult to specify. It depends on the mission.

16. What tasks are tedious and could be automated?

Although operators view a large number of mnemonics, the CERES COBRA system does little beyond providing color coding and scrolling event lists. The mission controllers would like for the system to provide more guidance as to the source of the problem.

After the pass

17. What do you have to do after the pass?

- Shut down the connection with the ground control network.
- For tracked anomalies, enter a report into the tool.
- Make printouts requested by the engineer.

Appendix B: Summary of Mission Controllers' Backgrounds

The following table summarizes our findings on the backgrounds for mission controllers for NASA, CERES, and the SOPS.

Topic	NASA	CERES	SOPS
Mission Controller (MC) Background	• Chose the field of spacecraft operations • Attended university programs in engineering (generally aerospace) • Much on the job training.	• Usually former SOPS operators • AF Contractors (General Dynamics)	• Chosen from aptitude test • Enlisted Air Force
MC Training	• University • On the job training	• On the job • Previous SOPS experience	• A 5-6 month training program. • On the job training
MC Responsibilities	• Fairly broad. Depends on the complexity of the spacecraft	• Fairly broad	• More limited • More specific
Missions	• NASA space operations (research satellites)	• Mostly testing of new ground equipment using old satellites	• AF Space operations (communications, weather, surveillance, etc.)
Work environment	• Typical work environment during daytime shifts • For lights-out missions, control centers are empty off hours • One facility may be shared by multiple spacecraft in a given family	• Typical work environment • Can get loud with multiple MCs.	• Unknown
Work Culture	• Informal	• Informal	• Formal • Well-Structured
MC Work Schedule	• Business Hours for lights-out missions • More complex spacecraft (like Hubble) are still staffed 7x24	• Rotating Schedule (change every 2 weeks) • Employees like schedule.	• Rotating Schedule • Employees like schedule.
Engineer Work Schedule	• For lights-out missions – only business hours	• Business hours • On call remaining hours	• Unknown