DRAFT

SGT Morgan, Jonathan H. and SPC Schroeder, Jeffrey N.

WO1 Matthew Roman

Stryker Brigade Combat Team, UAV Platoon

7 June 2003

Current and Future Development and Application of C4I Technology within the Shadow 200 TUAV System

C4I, or Command, Control, Communications, Computers, and Intelligence, technology is revolutionary in its ability to allow for digital cueing, information transfer, and dissemination; however, current doctrine, instruction, and application have severely limited this technology's feasibility to UAV operations. The purpose of this project is not only to highlight new approaches within the Shadow System's current configuration but also to illustrate an affordable expansion to C4I technology. The expansion package explored in this project would have two major benefits. First, it would employ the Muse Rack during flight operations and empower the Mission Commander (MC) with the full compliment of Mission Planning software. Second, it would restore the Mission Commander as the primary point of communications between UAV crews and integrate the Launch and Recovery Site (LRS) and other Intelligence assets into digital operations, thus allowing the flight crew to place their full efforts towards methodical intelligence collection. As among the first to actively employ this technology in the field, it is our intention only to offer our insights and ease the digital unification of UAV technology with the rest of the Intelligence Community.

Topic I: C4I Hardware and Emplacement

Often overlooked in operations, the Shadow Community neither fully understands nor has documented C4I hardware and emplacement. When UAV operators employ C4I technology, "The Operator's Command, Control, Communication, Computers and Intelligence Operations Checklist" is an invaluable resource and clearly defines day to day operations. For troubleshooting, the operator must first comprehend and determine the means of data exchange, whether fiber optic or coaxial. Utilizing coaxial cable, the operator has a durable, reliable, expandable resource, however, is subject to slow throughput rates and excessive cables that clutter the Tactical Operations Center (TOC). Implementing coaxial allows for expansion, is convenient, and limited only by its dependence upon a repeater.

Note To connect three or more cables, the operator must have a repeater that lengthens the range of the signal.

When the operator has access to a fiber optic network, he has the advantages of higher throughput rates, expedient emplacement, and more bandwidth. In TOC operations, the Shadow 200's Tactical Fiber Optic Cable's length limits the versatility that is critical to survival, however options exist. What to do?

Connecting TFOCA cable to TFOCA cable, Tactical Fiber Optic Cable Assembly, is an option and proven. In a TOC, the UAV operator can tap into several systems. TFOCA spools from the Trojan Spirit and ASAS systems are another option to extend range. Since Trojan Spirit rarely uses TFOCA cables, the operator can easily acquire a spool and obtain a length of cable otherwise impossible within the confines of the system. Because C4I connectivity depends upon cable length, an UAV representative must be present for TOC planning, an operator familiar with both GDT and C4I limitations.

Connectivity with the All Source Analysis System (ASAS) truck is essential and demands a preliminary knowledge of communication's equipment previously unknown to the UAV Community. Through time, the Army has hired many contractors to develop its software, the differing approaches and methods, mainly the use of either FX or TX signal, has created the need for signal converters such as the Multi-Media and Viper Kit. However, the Shadow 200 System's dependence upon the Multi-Media Kit affords independence from the ASAS's switch and frees UAV Operations from hardware inconsistencies. Receiving all intelligence reports in the network makes ASAS critical because it handles all queuing, digital traffic, and access to the web. If the UAV operator communicates with the ASAS operator and plugs his TFOCA cable to the corresponding pigtail, he should have no difficulty establishing connectivity.

Most missions demand the following; the AVO selects all the annotated video fields, the MPO chooses the printer and 9-in monitor as annotated, and the three user fields as closed captioning in the Video Crossbar. Reason being, the system's current configuration connects the video encoder to the MPO workstation that is critical for closed captioning. By connecting client systems to either AVO or MPO ports located on the side of the shelter, the operator distinguishes between general and specialized users and determines whether the client system has access to closed captioning or annotated video. Considering Client access is a procedure dictated by client system capabilities, subject to unit SOP, but generally follows these guidelines: ASAS and the TOC's main LCD display are general users; JSTARS and Trojan Spirit are specialized.

When JSTARS directly ties into UAV operations, a Viper Kit is essential for compatibility and directly connects to the designated MPO Port; the Kit acts as another media connector. The Viper Kit is JSTARS specific hardware that is the responsibility of the JSTARS operator to employ. As with coaxial LAN cables, the use of coaxial extenders (Barrel Adapters) can increase cable length and are subject to the same three-cable limit. A final note, every TOC differs in layout and design and requires a separate scheme that demands cable adapters fulfilling functions unique to situation and location. Anticipating these demands, the UAV operator is prudent to bring the full set of adapters provided by AAI and have them readily available.

Note Notorious for their dependence upon adapters to access video, Tactical LSDs and laptop displays will pose special challenges.

Topic II: LAN Connectivity

If you know what questions and whom to ask, connectivity is simple. Linking the various intelligence systems, ASAS acts as the central hub, provides access to the battle-net, and is invariably the single point of failure for the network. Creating the initial list of addresses or responding to IP address and hostname changes entails verification of all information in the C4I address window. The operator establishes digital communications by connecting a TFOCA cable to a pigtail on the left side of the ASAS shelter and confirms signal by observing a green light on the switch that indicates low-level network connectivity. If no green light is present, the operator must confirm the condition of the TFOCA cable by flashing a light into one end. While the other end remains connected to a TFOCA port, the operator observes the cable for two points of light and determines its condition, failure to illuminate indicates a fault.

Note All commands typed into a terminal window are in *italics*. Access the terminal window by right clicking on the desktop, selecting Tools, and selecting the Terminal icon.

After verifying the condition and proper placement of cables and connections, the user confirms digital communication by performing basic network software troubleshooting. Are the computers talking? The *ping* command tests network connectivity and informs the operator whether he can send data to and from a given host.

A successful ping is as follows:

```
# ping 148.87.123.87
tuav-23 is alive
```

When an unsuccessful ping occurs, the computer replies with a timeout error message that entails troubleshooting the problem. Are you using the proper IP address or hostname? To verify an IP address, the user has two options and must determine the optimal solution, whether to confirm his or the other operator's IP address. Validating your workstation's IP address requires only right-clicking the desktop, selecting Application Manager, clicking DII_APPS, and then the TACLAN icon. If the other operator's IP address is critical, the user opens the Text Editor. Once within the Text Editor, the user can access the /etc/hosts file and determine the appropriate IP address.

Note The Text Editor is found under the "Applications" menu after right clicking the desktop. Further details on the use of the Text Editor are on page 0050-3 of the "LRIP II C4I Task Map for ABCS".

Failing to identify the IP address, the operator can verbally confirm the correct address.

If despite working hardware and correct IP addresses, problems with digital connectivity persists. A higher-level problem is evident, one that will require you to contact the Network Administrator of your TOC. Frequent updates to the LDIF, the master list of IP addresses and hostnames that govern your Brigade's digital world, may cause incompatibilities with other systems. When the rest of Squadron/Battalion uses a different version of the LDIF, connectivity is improbable.

If all other possibilities are exhausted, responsibility for broken digital communication may lie in misconfigured network security measures. In short, these problems require the attention of the Network Administrator.

Once connectivity is established, the operator can use well-documented C4I startup procedures; however, there are a few considerations not explicitly highlighted in the C4I checklist. Contrary to the current checklist, the AUX circuit breaker must remain off until the MPO's VME has completely booted. When the user flips the AUX circuit breaker before the MPO's VME has completely booted, the system fails to recognize the AutoFill server and prohibits C4I operations. As with MPO messaging, AVO functionality requires the AutoFill server, though the system's configuration negates the AVO workstation's ability to auto-fill date and coordinate fields in the role of AVO. Despite the AVO workstation's inability to auto-fill message fields, it remains the primary tool for the SBCT (Stryker Brigade Combat Team) and affords operators the ability to better manage flight demands. Envisioned to add ease to the messaging process, MPO messaging is labored intensive and poorly engineered, inefficiently distributes operator workload, and fails miserably.

C4I Troubleshooting Steps

- Verify the condition of cables and connections.
- Ping the other systems.
- After the operator successfully pings, send a test C4I messages.
- In the case of an unsuccessful ping, verify connections to the Multi-Media Kit and IP addresses.
- Completing all other checks, consult with the following in this order:
  - I. ASAS Operator
  - II. TOC Administrator
  - III. UAV Tech

Topic III: 220A Connectivity

220A is to many Shadow units a mystery; its role in operations is often disputed or nonexistent. The name 220A simply refers to the protocol implemented for FM digital communications. In common, use for years with the AFTADS system, 220A offers many unique abilities to the UAV operator and allows him to transfer script files, mission plans, overlays, and C4I messaging over FM. The Operator's Command, Control, Communications, Computers, and Intelligence Operations Checklist clearly defines routine operation of 220A. However, a few aspects of the initial setup warrant some intention.

For 220A to work, you must create a separate and independent hostname and address, one that in no way conflicts with the Tactical Local Area Network (TACLAN) configurations. Otherwise, the system will be confused and fail to operate correctly. Creating an IP address requires familiarity with Unix and is the role of a Tech or specially trained operator. To create such an address: the Tech must enter the Terminal Window; type *su root*, and enter the Super User password. Becoming the Super User (su) and possessing all system privileges, the tech then types, "vi /etc/hosts." The user proceeds with utmost caution, so to avoid altering in anyway the current files. Entering /220A, the tech can read all the 220A address strings and add a new one. The Shadow 200 Ground Control Station (GCS) LRIP II C4I Task Map for ABCS 6.X describes in detail the numeric considerations essential for IP address creation. Please refer to this guide and a CLS representative if this is your initial experience with creating 220A addresses. Once finished with the vi editor, the tech types, ":wq!" to save the files or, ":q!" to quit without saving.

Topic IV: NITF and NIMA

Note These scripts were written as simple proof of concept and have been superceded by the newest C4I upgrade.

Added 22 October 2003

NITF and NIMA are both dependent upon and optimally used in conjunction with a CD Burner. When Brian Decker devised a script for loading maps, he freed users from the hassle experienced by the first Shadow Operators. However, NITF and NIMA both are limited by the failure of initial designers to create a user-friendly means of switching the CD Burner from "read only" to "write." Unable to burn CDs, since in most instances the Burner is set to "read only, the user is restricted to hardcopies or electronic means to exchange information, create or manipulate graphics, or communicate intelligence to both other Intelligence Assets and upper echelons. Installing the script below allows operators to utilize all the resources available for the Intelligence process.

Save this script as burncd:

```
#!/bin/sh
####################################
#                burncd 1.0                    #
####################################
#           By: Jeffrey Schroeder 06/21/03          #
#     This script must be run before burning a cd     #
####################################
cd /etc/init.d
if [ -x /etc/init.d/volmgt ]; then
echo "Stopping Volume Manager: /c"
/etc/init.d/volmgt stop
sleep 2
echo "done"
sleep 2
else
clear
echo "Volume Manager error. Please contact a local CLS representative"
exit 1
fi
exit
```

Save this script as readcd:

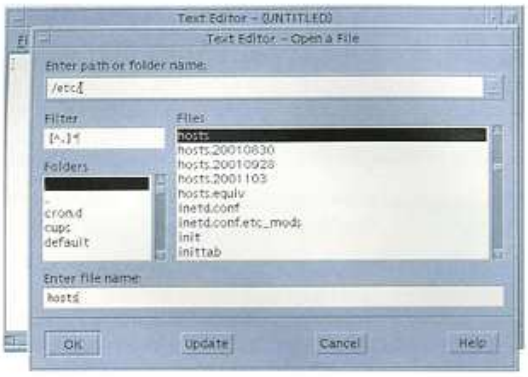
```
#!/bin/sh
#################################
#                readcd 1.0                              #
#################################
#       By: Jeffrey Schroeder 06/21/03                 #
#      This script must be run after burning a cd       #
#################################
cd /etc/init.d
if [ -x /etc/init.d/volmgt ]; then
echo "Restarting Volume Manager: /c"
/etc/init.d/volmgt stop > /dev/null
cp vold.conf.org vold.conf
/etc/init.d/volmgt start
echo done
else
clear
echo "Volume Manager error. Please contact a local CLS representative"
exit 1
fi
exit
```

Topic V: Netscape, C4I, and XFTP Integration

Another facet to C4I Messaging that remains under utilized in the Shadow Community is the integration of C4I message fields and XFTP with Netscape. The application of simple software along with cut and paste facilities allows the operator to digitally transmit weather, scripts, mission plans, and overlays via 220A, thus remotely incorporating the LRS.

If your connection to ASAS is sound and the NITR Server is functioning, the operator can easily access the Brigade web page and other sites through Netscape. To access the Battle Net, Netscape requires either the hostname or IP address of the site you wish to contact.

Since operations can range over large geographical areas and inhibit one on one communications with the various system users, the operator must have a working knowledge of the Text Editor to reference desired IP addresses. Once in the Text Editor, delete all of the text in the top drop-down menu. From there, type "/etc" and press enter. In the bottom text box, type in the word "hosts" and press enter. A listing of all the Brigade's IP addresses and hostnames should become available.



Note The operator must adhere to the following format to access the web, "http://127.30.74.48."

Through the Brigade Web page, the UAV Platoon of the first SBCT has accessed weather, the ACO, and the ATO. Accessing many web sites presents a significant problem because the majority of Army webmasters design for an audience running windows.

Unless converted into a UNIX format, the AVO and MPO workstations fail to read many pertinent web sites. On the other hand, web pages for weather in the SBCT are in a Unix friendly format. Once the web page is open, the user can copy and paste the contents into a standard C4I Free Text messaging window.

Note Control C enables the operator to copy text and Control V to paste. Free Text Messaging has none of the standard right-click functions.

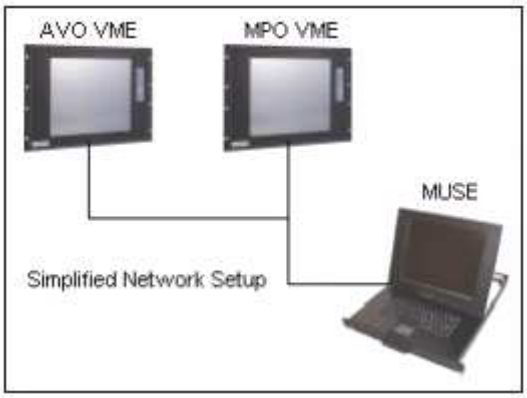
Once transferred into the Free Text window, the user can send weather via 220A to the LRS, provided you have line of sight for FM communication.

As with C4I message fields, the operator can send XFTP files via 220A. Using 220A requires no separate operations and differs only in that the user enters a 220A address in place of a flight-LAN address. Where LAN XFTP file transfers require a flight-LAN address, 220A transfers require the corresponding shelter's 220A address, found under Addresses in the C4I main menu. The User field remains, "Shadow," for 220A XFTP transfers. Using 220A XFTP messaging in close ranges, the operator has a reliable means of delivery and is free from the aggravations of setting up a LAN between the shelters. In addition, 220A XFTP transfers free operators from prolonged voice transmissions, reduce errors in communication, and make available to both sites the most current overlays and mission plans.

Though the current configuration allows for file transfers and C4I messaging via 220A, no means exists to send files from the MUSE Rack. Written for Microsoft Internet Explorer, the operator accesses the ACO and ATO through the MUSE Rack and faces an implicit question. What role does the MUSE Rack play in daily operations? In exploring this question, a larger question is evident. Is a better means of messaging and planning possible?

Topic VI: MUSE Future Capabilities

An important issue, the shadow community under utilizes the MUSE Rack as a tool for the Mission Commander (MC). According to doctrine, MPO's duties are to perform all C4I configuration, initialization, and messaging. Because the nature of payload operations and data exploitation is demanding, C4I messaging acts as a hindrance to effective intelligence gathering. Our current solution involves assigning C4I messaging to the AVO; this proves less than optimal. The MC is the focal point of all communications between higher echelons and develops the intelligence picture in conjunction with the crew.



Operators familiar with the Hunter system and its original ideology will remember the Mission Planning Station (MPS). The MPS was an entire shelter configured and dedicated to just the Mission Commander's planning considerations. Although an extra shelter dedicated to mission planning is highly impractical, the MUSE, with modifications, is capable of MPS functionality. Running on the MUSE and VME, the different operating systems are incompatible, however a solution exists. To bridge the two operating systems, I will introduce a free, open source program originally written by AT&T Laboratories to provide an eloquent solution to the current decentralization of both planning and communications.

Enter Virtual Network Computing. VNC)

VNC consists of two components, a Server and a Viewer. The Server runs on the computer you want to remotely access and sends a virtual desktop to the viewing workstation that then allows for full remote control, when provided with the proper login credentials.

There are two important features of VNC:

- Running on separate machines and different operating systems, the VNC protocol connects the Server and the Viewer while being simple and efficient while being transparent to the operator.

- Due to the stateless nature of the VNC protocol, no data loss will result from breaking the Viewer's connection to the Server and then reconnecting.

Providing access to the Mission Planner, Overlay Editor, and C4I Messaging on the MUSE requires a few changes to the current system configuration. The technician (tech) must install VNC Server on the MPO console and the VNC Viewer on the MUSE. Currently, the ACO and ATO are accessed from the MUSE; however, current software limitations prevent file transfers from the MUSE to the MPO console preventing transfer to the Launch and Recovery Site (LRS) via 220A.

Topic VII: LRIP II Accessibility Upgrades

Powering up the Remote Video Terminal (RVT) requires the operator to type several commands into an x-terminal (xterm) window; currently, the operator must type the following:

```
su – root
cd /home/rvt/kfir/src
make insmod
```

Error prone and unsophisticated, the novice operator is granted "Super User" privileges, and thus capable of damaging mission critical file-systems. Scripting is an embedded feature of all UNIX systems that allows flexibility and greater ease of use. To employ scripting capabilities, the tech should write and save the following script to the /home/rvt/rvt directory using the vi editor.

```
#!/bin/bash
su – root
cd /home/rvt/kfir/src
echo "Please wait… "
make insmod > /dev/null
echo –n Done
sleep 2
exit
```

After writing and saving, the script requires executable permissions to run.

```
chmod 755 /home/rvt/rvt
```

The Change Mode (chmod) command performs the required altercations to make the "rvt" executable. The operator opens the xterm window and types rvt; presses enter and receives a prompt for the root password, enters the correct password and completes script execution.

Note Unlike previous solutions giving the operator root privileges and then allowing continued input, this solution requires the root password and no user intervention.

Though proven as a working solution by the First SBCT, coordination between the original contractor and PM office is necessary for mass distribution.

Another potential solution exists that frees the operator from needing the all-powerful "super user" password and prevents accidental system corruption. Untested, this solution would work with a slight tweak of the above script and minimal testing.

Currently every time a user inserts a map cd or other relevant data cd into the shelter CDROM drive, the operator must open terminal window and type superfluous commands to mount the cd. The shelter's operating system (Solaris 7) natively includes facilities for auto-mounting removable media. With proper time and testing, I can implement these features; however, unit OPTEMPO prevents the necessary research to write the auto-mount configuration files.

The vast scope of this subject precludes in any depth exploring, discussing, or researching every avenue in a single paper. In conducting the research for this project, the authors found many new approaches, capabilities, and weaknesses that tantalized and challenged, many warrant review in subsequent papers. However, emplacement; LAN connectivity; 220A connectivity; NITF and NIMA accessibility; XFTP, C4I, and 220A integration; MUSE modifications, and other improvements were most relevant for not only the SBCT but also the community at this time. It is our hope to unify digital communications within the traditional role of the MC and create redundant systems for C4I operations. Written by operators expressly for the betterment of the UAV community, we hope subsequent units find use in this project. And for our comrades who are going or are in harms way, God bless you.