Bolt Beranek and Newman Inc.

1

Report No. 3582

Advanced Fleet Command Control Testbed Planning

May 1977

Submitted to:
Advanced Research Projects Agency

BBN Report No. 3582

MAY ~~June~~ 1977

Advanced Fleet Command Control Testbed Planning

Final Report
February 1976 to May 1977

Contract No. MDA 903-76-C-0211
ARPA Order No. 3181

Principal Investigator:
Dr. Robert H. Thomas

Submitted to:

Advanced Research Projects Agency
Information Processing Techniques
1400 Wilson Boulevard
Arlington, Virginia 22209

Attn: Cdr. Floyd Hollister, USN/IPT

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER
BBN Report No. 3582

2. GOVT ACCESSION NO.
AD-A122698

3. RECIPIENT'S CATALOG NUMBER

4. TITLE (and Subtitle)
Advanced Fleet Command Control Testbed Planning

5. TYPE OF REPORT & PERIOD COVERED
Technical

6. PERFORMING ORG. REPORT NUMBER

7. AUTHOR(s)
R. Thomas

8. CONTRACT OR GRANT NUMBER(s)
MDA-903-76-C-0211

9. PERFORMING ORGANIZATION NAME AND ADDRESS
Bolt Beranek and Newman Inc.
50 Moulton Street
Cambridge, Massachusetts 02138

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS

11. CONTROLLING OFFICE NAME AND ADDRESS
Defense Advanced Research Projects Agency, Information Processing Techniques
1400 Wilson Blvd., Arlington, VA 22209

12. REPORT DATE
MAY ~~June~~ 1977

13. NUMBER OF PAGES
14

14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)

15. SECURITY CLASS. (of this report)
Unclassified

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)
Distribution of this document is unlimited. It may be released to the Clearinghouse, Department of Commerce for sale to the general public.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES
This research was supported by the Defense Advanced Research Projects Agency under ARPA Order No. 3181.

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Command and Control	Secure ARPANET
ACCAT facility	Private Line Interface (PLI)

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This report is the final report for a project to assist NAVELEX with the facility planning for the joint ARPA/NAVELEX Advanced Command Control Architectural Testbed (ACCAT) program. In particular, BBN assisted with the planning for the computer systems which are to comprise the ACCAT central site which is to be installed at NELC. This work included designing the layouts for the computer equipment to be installed at NELC as well as insuring that the software executes effectively in the ACCAT environment.

CONTENTS

Summary

The Advanced Command Control Architectural Testbed (ACCAT) is a facility designed to support evaluation of the applicability of various new computer-communication and information processing techinques to military command and control problems. The ACCAT program is sponsored jointly by ARPA and the Navy.

The core of the ACCAT facility is located at the Naval Ocean Systems Center (NOSC) in San Diego. It is scheduled to begin operation in mid-1977. The testbed is built on a number of existing capabilities including: the ARPANET; the ability to provide secure communication for subnetworks within the ARPANET; the standard interfaces and protocols of the network which enable interoperability of heterogeneous equipment; and a large base of existing software and experience in computer networking, time-sharing nd interactive computing.

The objective of this contract was to assist with facility planning for the ACCAT program. In particular, BBN assisted with the planning for the computer systems that comprise the ACCAT core facility located at NOSC. This work included designing layouts for the placement of ACCAT computer equipment at NOSC, scheduling the delivery and installation of the equipment, procurement of interactive display terminals for the testbed, and insuring that the system level software executed effectively in

the secure ACCAT environment. The following sections describe these activities in more detail.

1. Planning for the ACCAT Core Site.

The central ACCAT site is located at NOSC in San Diego. The major components of the core facility are a DEC KA10 TENEX system, a DEC KL20 TOPS-20 system, and a DEC PDP-11/70 Unix system. These three systems are connected to the ARPANET and thus to each other through an on-site ARPANET TIP. The ACCAT concept includes support for remote site operations via so-called "remote site modules". When they are operational, these remote site modules will communicate with the core ACCAT facility using the ARPANET.

Because it deals with classified information, the ACCAT facility must operate in a secure environment. Secure inter-computer communication over the public, unsecured ARPANET is accomplished by connecting the ACCAT computers to the network through Private Line Interfaces (PLIs) rather than directly to IMPs (or TIPs). The PLI is a small computer, based on the Pluribus architecture, which controls a cryptographic device (KG-34) through which all data exchanged between the host and the network must pass. An additional level of security and privacy is accomplished by using a capability of the ARPANET which allows the ACCAT hosts to operate as a "logical subnet". This capability, which is implemented within the ARPANET IMPs, ensures that ACCAT hosts may communicate only with other ACCAT hosts.

As part of our facility planning activities, we prepared plans for the layout and installtion of the major components of the core ACCAT facility. This included the ARPANET TIP, a pair of PLIs, and the three host computer systems along with their associated peripheral equipment.

This planning activity involved several visits to NOSC to inspect the building that was to house the ACCAT equipment (the EDATL building) and to confer with on-site NOSC personnel and personnel from the University of Southern California Information Sciences Institute (ISI) who were to assume operational responsibility for the core facility computer equipment. As a result of these visits and meetings, we drafted a plan for the layout of the equipment. The plan was distributed to ARPA, NAVELEX, NOSC, and ISI personnel for review. After some minor modifications the plan was accepted and used for the equipment installation.

2. Host System Operation in the Secure ACCAT Subnetwork.

The TENEX and TOPS-20 operating systems(1) do not generally run in a secure network environment. These hosts normally are connected directly to an IMP rather than to an intermediary PLI. In addition, they normally operate within the context of the entire ARPANET and have the ability to communicate with the full range of ARPANET hosts rather than operate within a "logical subnet" with limited communication ability.

Both the PLI and the logical subnet capability were designed to be transparent to hosts. However, there were known to be several areas where the goal of transparency was not possible to achieve. As examples: the maximum allowable length for a host/PLI message is shorter than the maximum allowable host/IMP message; hosts connected to PLIs can not use both normal and priority messages. Because these security mechanisms are not totally transparent it was important to assess the impact they might have on the hosts. This was necessary in order to determine what, if any, changes would be required to the host operating systems and application software to insure their proper operation in the ACCAT environment.

(1) The TOPS-20 operating system is the standard operating system for the DEC KL20 processor, a new processor which was designed to replace and be upward compatible with the older KA10 processor which houses TENEX. TOPS-20 evolved from an early version of TENEX (approximately 1972). Hence, the two systems are quite similar and software developed for TENEX should run with only minor, if any modificaton, under TOPS-20.

A series of expriments were performed in which two TENEX hosts were configured into a logical subnet of the ARPANET in order to simulate the ACCAT secure environment. The network control programs (NCPs) on the hosts were thoroughly exercised in this simulated environment by running standard network-oriented subsystems, such as TELNET, FTP, and RSEXEC.

These experiments indicated that the impact on host software due to the lack of transparency of the PLI and of the logical subnet capability was minimal and could be handled in fairly simple ways. As examples:

- The TENEX and TOPS-20 NCPs can be made to operate with the shorter maximum message size limitation of the PLI by changing the contents of a single NCP memory cell.

- Although the TENEX and TOPS-20 NCPs uses both normal and priority messages for host-host protocol control functions, it operates correctly (and with no modification) if only normal messages are used (i.e., if the PLI converts priority messages to normal messages for transmission through the network).

- The reduced effective host address space that results from operating within a logical subnet causes no problems for the TENEX and TOPS-20 NCPs and only minor problems for most application programs. The problems for application programs occur when programs attempt to interact with hosts not included in the logical subnet, in which case the attempts fail. Application programs not prepared to recover from such failures malfunction and need to be modified somewhat to run in the ACCAT environment. Fortunately, most existing nework-oriented programs do not need to be modified in this way.

A list documenting known differences between normal ARPANET operation and operation within a secure subnet and means for handling the differences was compiled and circulated to ACCAT personnel responsible for the operation of host software.

3. Installation of PLIs.

A number of factors present during the early planning and development stages of the ACCAT facility contributed to complicate the task of configuring the three initial ACCAT hosts into a secure subnetwork. These factors included: changes in the configurations for the two PLIs being procurred for the testbed and the resulting uncertainty in PLI delivery dates; uncertainty in the schedule for securing the building that houses the ACCAT core facility; uncertainty in the delivery schedules for the three host computers; the desire to make maximum utilization of the ACCAT host resources (in an unclassified mode if necessary) during the period when the testbed equipment was being delivered, installed, and checked out to insure that important ACCAT program milestones would be met.

These and other factors required a flexible plan for connecting the ACCAT hosts to the ARPANET and securing their operation. A plan was developed for this system interconnection and integration which involved a sequence of steps spanning several months. The plan was followed and the configuration of the principal ACCAT hosts into a secure subnet was successfully accomplished with minimal disruption to operation of the hosts and the activities of their users.

4. Procurement of Display Terminals for ACCAT.

Six Hewlett-Packard HP2640A display terminals were procured for use in the ACCAT core facility. After the terminals were ordered, two of them were temporarily allocated for use in the joint ARPA/Navy Military Message Experiment program. This reallocation was the source of some confusion to the vendor and as a result, two of the six terminals were delivered without some of the options ordered. This situation was eventually corrected by field installation of the missing options for the two terminals. The two terminals allocated to the Military Message Experiment program have been returned to the ACCAT program. At present, all six terminals are fully configured and operational in the core testbed facility at NOSC.

5. Evaluation of the National Software Works System.

The National Software Works (NSW) system is a network operating system being developed under ARPA and Air Force funds. It is designed specifically to provide an effective environment for software production. Prototype versions of the NSW system have been successfully demonstrated and the first release of an operational version is expected in mid-1977.

One of our activities has been to investigate the possibility of integrating the NSW system into the ACCAT facility. There are two somewhat different motivations for considering this integration:

1. ACCAT is a distributed, heterogeneous, multi-computer facility. At present there is no uniform operating system for the ACCAT facility as a whole; rather, users must deal with each of the constituent host operating systems individually. An operating system which allowed users to deal with the facility as an integrated entity rather than as a collection of autonomous hosts would permit much more effective use of the ACCAT resources.

2. The NSW system acts to manage a collection of distributed, heterogeneous resources in a way that provides a uniform, reliable service in the presence of communication network and host computer outages. As such, NSW and its underlying

technologies are appropriate technologies for demonstration and evaluation within the testbed.

Our recommendations with respect to the use of the NSW within ACCAT are:

1. The NSW system is not yet (i.e. in calendar 1977) ready to be integrated into ACCAT as a testbed operating system. The NSW system at present is neither sufficiently reliable nor adequately responsive to be used in an operational way within ACCAT.

2. During the course of calendar 1977 NSW reliability and performance can be expected to improve. The question of integrating it into ACCAT as a testbed operating system should be re-evaluated at the end of calendar 1977.

3. The MSG facility used to support inter-host communication between NSW system components is fully operational and should be made available in the testbed immediately for use in applications which require inter-host communication.

4. The version of the NSW system scheduled for release in mid-1977 should be installed in the testbed as a resource to be used in demonstrations and in order to allow testbed users to gain familiarity with NSW concepts. This hands on experience with NSW should be useful as input in re-evaluating the use of NSW as a testbed operating system (see 2 above).

5. The status of the NSW project should continue to be closely tracked to ensure that developments beneficial to ACCAT can be transferred into the testbed as early as possible.

6. Miscellaneous

As part of this contract we have been available to consult with personnel from the Computer Corporation of America (CCA) on the problem of modifying the Datacomputer software so that it will run on the ACCAT TENEX and TOPS-2Ø hosts. The Datacomputer software has been in operation for a number of years on a specially modified version of TENEX at CCA. However, because the ACCAT hosts will use standard versions of TENEX and TOPS-2Ø, some amount of software conversion is required. This consulting activity has been a relatively small one. From time to time we have been called upon to assist when conversion problems have been encountered.

In order to meet important ACCAT program milestones, it was important to begin classified operation of the ACCAT TENEX host early in April 1977. Because of the uncertainty in the delivery dates for the PLIs (see Section 3), there was a possibility that TENEX would not be able to operate as a host on the secure ACCAT subnet by that date. However, because of the structure of the application software to be used, it was important that the TENEX host appear to be on the network to processes executing on it. In particular, a classified data base was to be loaded from tapes into the Datacomputer (which executes on the TENEX). The Datacomputer software is constructed such that the only access path to it is through the network. That is, processes interacting with it do so using the ARPANET even if they are executing on the same host as the Datacomputer. The advantage of this approach is that there is a single, uniform access path to the Datacomputer regardless of the host locations of the accessing process relative to the Datacomputer. The principal disadvantage is that if the network is down (as would be required for security reasons if the PLIs were not installed), local processes cannot access the Datacomputer.

In order to provide a contingency for the possibility that the PLIs could not be installed in time, we developed a modification to the TENEX Network Control Program (NCP) to enable local processes to communicate with each other via the NCP even though TENEX itself was physically disconnected from the network. This would allow the programs loading the data from the tapes to interact with the Datacomputer software as if through the network even though the TENEX was rot physically connected to the network. As we understand it, this NCP "short circuit" was used at the ACCAT facility for a short time.