

NERTS
JMPS Combat/Force Level Network Architecture Meeting
April 4, 2000 - SPAWAR Philadelphia

Minutes & Action Items

Purpose

This was a continuance of previous meetings to aide in determining the system architecture for JMPS Combat and Force Level. The purpose of the NERTS Tiger Team is to identify issues, operational architecture, technical alternatives, program interfaces, etc. to assist in the development of acquisition documents and government direction for a future JMPS acquisition contract.

This meeting was aimed at getting a better understanding of current programs including a brief on TAMPS, GCCS-M, and ADMACS programs. Current top-level technical alternatives were presented and discussed.

Introduction / Overview (Capt Sel Mike Hecker, PMA233)

A list of JMPS Combat/force level requirements were presented to focus the group:

- TAMPS “off-the-boat” (Required)
- Secure Computing (Required)
- Real-time / responsive planning
- Hosting the Strike Planning Folder (SPF)
- Non-carrier locations
- Low bandwidth / no connectivity

Products that this group will be working on are:

- 1) An operational architecture via Use Cases and CONOPS.
- 2) Products to feed into JMPS acquisition documents (SOO, SSS, SOIs, etc.)
 - Technical alternatives “trade space”
Pluses and minuses
 - Network interfaces:
 - ADMACS, GCCS, TBMCS, JSIPS, TOPSCENE, GPS Almanac via SIPRNET, GPS Almanac via NAVSSI, Weather server like NITES
 - Options for interfacing
 - ROM Costs
 - Business case
- 3) A strategic plan for coordination with other progrms:
 - ADMACS, GCCS, NSWPC, TBMCS, JSIPS, (REDS)

Our current goal is to have a product by the end of May when Capt Sel Hecker departs PMA-233.

NERTS Minutes - 4 April 2000

TAMPS 6.2.1 (Joe Mountain, SPAWAR/Gnostech)

PowerPoint briefing available

An overview of the current TAMPS 6.2.1 architecture was presented along with current NT and UNIX integration. Some discussion points included IT-21 LAN integration, Carrier LAN integration, and classification issues.

IT-21 LAN: There are currently 3 Carriers that are not IT-21: USS Roosevelt, Kennedy, and Constellation. All drops on the carriers currently utilize an Asynchronous Transfer Method (ATM) LAN not Ethernet. For TAMPS 6.2.1, the PCs located in CVIC are connected directly to the ATM backbone or via an Ethernet switch. For shipboard LAN installations TAMPS runs on one of the 4 Secret Tactical Computer (STC) LANs (STC3 ELAN/VLAN). Each carrier has a unique network manager. It was noted that every carrier CVIC and ready room is configured slightly different.

PCs in CVIC: The goal of the 3 PCs in CVIC is to be TAMPS x-terminals. They do not have the full compliment of IT-21 software due to the need for extra licenses. With 6.2.1 they could be moved to IT-21 PCs. The x-term software (Hummingbird Exceed) is the same as is used by IT-21. **** Do we need to field these PCs in the future? ****

LAN Issues: JMPS will need to network to similar systems as TAMPS including weather, a mission rehearsal program, GPS Almanac data, JSIPS, etc.

Some differences between Sun PC NetLink and Samba were discussed. TAMPS 6.2.1 chose PC NetLink for a variety of reasons including the ability for one copy of data to be sharing between PFPS seats on common RAID array space. GCCS is currently using the Samba software for use on their HP Servers.

The use of a Windows NT Environment allows for centralized network management including domain passwords.

JMPS v.1 will be making unclassified to classified transfer of data similar to PFPS. Currently only desktop NavMPS PCs can be connected to the ATM LAN (no ATM cards are available for laptops).

Q: Certified computers are currently separate for IT 21 and GCCS. The plan is for them to be moved to a common platform. With the current horizontal integration initiatives at SPAWAR, the SPAWAR 05 makes the Server decisions.

Enterprise Networking: E4000 is OS independent. Need to maintain Ethernet for PCs; no ATM cards for laptops. 6.2.1 uses three approaches for networking.

1) Standalone PC

Sharing of data is internally controlled. Data share by snekernet.

2) Groupware

Hooked on local network. Different domains (UNIX vs. NT) require different logins. Data can be shared via shared resources.

3) Enterprise Server (CVIC)

Single server with one login for any domain. Mapping of user name from NT SID to UNIX user login. Dat loaders hooked to TAMPS machine, but can be accessed via x-term on PC.

NERTS Minutes - 4 April 2000

Technical Trades (Dan Wright, PMA-233)

PowerPoint briefing available

Dan Wright presented a discussion of back-end server options for JMPS Combat/Force Level. This was not a decision brief, but a break down of possible technical options. It was noted that political issues would need to be addressed when making decisions regarding system interfaces and network design.

GCCS and other systems such as TAMPS that have a Core system with modules tend to not like to allow module-to-module communication.

A discussion took place regarding the transfer of information from GCCS and TBMCS. JMPS may be utilizing a Data Access Layer (DAL) to access GCCS information. The Air Force is currently TBMCS Core focused and are not looking at accessing GCCS information directly. It was noted that there are some same core segments between GCCS and TBMCS. They do share some components. There is a basic difference in mentality between the Air Force when it comes to accessing information. The Air Force looks to push in formation vs. the Navy pulling information. Mary Collins (NAWCWD/BAI) is a good person to tap in regards to database issues.

Dan Wright highlighted 5 basic options for servers. A 6th option was identified following some follow-on discussions. Reachback and JMPS as a GCCS segment were not included.

Options:

1. No Server (Direct GCCS client)
2. 3 Tier Architecture (Server in between JMPS PC and data systems)
Subset – Storage array only
3. GCCS proxy (Agent inside GCCS segment)
4. Sun Serengeti/Wildcat server architecture
5. Bitty Server (For special case implementation)
6. Peer Model (Some talking between JMPS workstations)

Discussions were made regarding a “JMPS lite” system that would not be hooked to a network and could be taken home. Numerous issues were raised as to the ability of the system to remain unclassified. JMPS is planned to be scaleable and portable. There is a desire to have the basic JMPS version unclassified similar to PFPS. A process needs to be developed to declassify hardware.

BJ Ramsay has been working CONOPS issues for JMPS v.1 and 2. Emphasis needs to be placed on identifying and meeting Fleet requirements.

DII COE compliance (plus, minus?)

Option 1: No JMPS Server

Where does a file server, or common data space reside.

Don't need server and client release at same time

Data access would be via SQL, DAL or equivalent API.

Pluses:

- No hardware costs
- Flexible configuration
- Easy expansion via fleet developed software (RIP) by adding functionality to client

NERTS Minutes - 4 April 2000

Minuses:

- Totally reactive to outside programs
- Ad hoc connectivity
- Need for common storage
- Need to negotiate with other programs or pay for resource requirements
- Fat client

Option 2: 3 Tier Architecture

Middle ware

Manages information, supplies to Client

Similar to TAMPS 6.2.1 E4000.

Does not imply replication

Could be data storage only

Pluses:

- Stable environment for client, isolated from GCCS
- Benefits to Trusted
- Can act as data storage
- CORBA based computational resource option
- Option could involve pass-through data storage only

Minuses:

- Server hardware cost and space in CVIC
- Development of server software
- Possible duplicate database management
Replication on JMPS server for GCCS or other databases
- SA/DBA required
- Security of CORBA

Option 3: GCCS Proxy

GCCS Segment built to support JMPS PCs. Proxy collects data and supplies it to clients; "MPS agent inside GCCS". This is similar to IMF web with NSWPC. Possible publish subscribe like interfaces.

Data Storage is TBD.

GCCS is running in a Solaris Enterprise environment. Their desire is for us to go directly to GCCS with no replication.

Pluses:

- JMPS PCs do not need to speak GCCS
- Limited or no HW costs for server, save space in CVIC
- Stable GCCS interface for clients

Minuses:

- May not meet all server needs
- GCCS politics, they do not want to have data agents interacting with segments
- Inter segment APIs
- Locked into GCCS UNIX software development schedule
- Data storage

NERTS Minutes - 4 April 2000

- Poor fit for Windows environment. DII COE UNIX mentality/processes transferred to PC?

Option 4: Serengeti

Pluses:

- H/W flexibility.
- Sun leading edge architecture.
- GCCS may be going to this.

Minuses:

- Unproven technology. Certification issues.
- Unknown interface between domains.
- GCCS politics.

Option 5: Bitty Server (Unique to other side)

Addresses unique needs of Trusted. Looks like server to clients. Will have to support local storage. Can be combined with firewall/guard, etc.

Pluses:

- Does not impose extra requirements on other clients.
Location transparent to client.
- Could be combined with other trusted components.

Minuses:

- Connectivity issues.
- Certification issues. NT vs. Trusted Solaris
- Potential for additional variants, hardware configurations.

Option 6: Peer Model

PCs talk among them selves with a possible "Chief PC". This is a variant of the 3 Tier option. Data storage can be on any (or multiple) computers.

JMPS is looking at making a PC like a server. Even in version 1 PCs may be able to talk among themselves. Doing prototypes now under current contract.

Pluses:

- No Server.
- Flexible configuration.
- Shared peer storage.
- More generic

Minuses:

- Development of Peer software
- Client reactive to outside tasking

Summary:

We need some form of server. All options are viable (variations, hybrids). GCCS is evolving; they are a moving target. We need to target where a user will want to be in 2003.

Operational Thresholds: How do we handle Reliability, Maintainability, and Availability if we do not own servers/environment?

NERTS Minutes - 4 April 2000

NERTS Minutes - 4 April 2000

GCCS-M Jack Sommer PRC, PMW-157

PowerPoint briefing available

Developers are INTR (imagery) and PRC (intelligence). GCCS transitioning from 3.x to 4.x to 5.x.

Horizontal Integration, Data Access Layer (DAL), Intel Channel, Document Management

Current Architecture with 3.1.2.1

3.1.2.1 OT tentatively scheduled for 4-10 August 2000.

Data Servers:

TDBM is master track database. Machine is called universal comms processor (UCP). Feeds Organic, TDDS, SIPRNET, TADILS.

ISDS (Intelligence Shared Data Server), old JOTS-19. Data sources are MIDB 2.0, national records, local records, reference databases, and local updates.

ITS (Image Transformation Services), JOTS014. Image push and pull system. Data sent to IPL and PTW. Can automatically associate imagery to target in ISDS if header data is filled out (e.g. BE associated with image). Relationship exists between ITS and IPL/PTW.

Information via router: MIDB (at the JIC), SIPRNET, and remote GCCS sites.

COP (Common Operational Picture) is derived from various stored data (tracks, maps, overlays, weather, and ATO).

Issues: Where is reality? Need to look at what the tools are being used.

Dan Wright stated "We do not want to go down the "Geeky" path that may not provide significant user capability".

Future integration will utilize the DAL. The GCCS Party line is to use JMTK with 4.x.

GCCS-I3, Integrated Imagery and Intelligence (I3)

Minimize redundant development and maximize commonality and interoperability.

Working with cross service programs: GCCS (DISA), GCCS-M (USN), TBMCS (USAF), IAS (USMC), and ASAS (Army).

GCCS 4.x

More energy into being spent on getting early Fleet inputs, and training sites.

Utilities/applications are on Windows NT.

4.X has slid from Lincoln to Roosevelt (OTRR May/June 01, SOVAT Nov 01, deploy CY 02) deploy FY03.

DII COE Horizontal Integration

Moving from stovepipe to integrated information. Reducing the UNIX footprint and required system administration. Utilizing common layers of software. Common HW/SW, development, Battle Group install, test, etc.

NEED most recent schedule to coordinate efforts. 5.X fielding 07/2003

NERTS Minutes - 4 April 2000

Data Access Layer (DAL)

Provides isolation between segment developers and external systems from changes (applications and data schema). Provides an extensible set of distributed C4I objects. Easier to access database entities such as MIDB

Intel Channel

Distribute timely intelligence data to Fleet. User subscribe to intelligence data, pertinent data is pushed to user.

NSWPC efforts

IMF Web Architecture. SPF/GCCS-Interface (point man is Tom Millman). Data mining inside GCCS-M to support SPF

Document Management System

Using interleaf product called Bladerunner (Interleaf (UNIX centric) vice Adobe PDF). Requires segment developers to come to table with segment build AND documentation.

NERTS Minutes - 4 April 2000

JMPS I3 Dave Pearson

PowerPoint briefing available

JMPS v.1 SSS Requirements are relevant to GCCS.

Technical Approach

Need to provide a threat intelligence data feed from AF and Navy. The preferred technical approach is through the DAL (Preliminary). Using DAL as an API vice SQL or something else.

Another option not preferred is to go directly to ISDS databases via SQL.

Q: Is an interface to GCCS-I3 via the DAL the joint answer for JMPS? This has been validated by Mary Collins. The Navy has bought in, but the Air Force is still studying and proposing alternatives.

Could use GCCS segments or build our own. (VIDAR and ORDINCL segments utilize JMTK tools for viewing.)

Initial work from Logicon is focused on XML files. Populate XML file, rewrite to update.

Intelligence community will be making frequent event-by-event updates. You can access any GCCS server via SIPRNET (Connection and band-width). Q: What functionality can we do with minimal bandwidth?

PROBLEM: JMPS v.1 is working in isolation of v.2 and 3. There is no server architecture for JMPS v.1. A server will be a JMPS v.1 to 2 change. Decisions being made now will affect the system architecture.

NERTS Minutes - 4 April 2000

ADMACS John Kovacs

PowerPoint briefing available

A general overview presentation was given on the Aviation Data Management and Control System (ADMACS) system. This is a tactical real time system being incorporated on carriers. It has an open architecture with multiple redundancies.

ADMACS is currently running under their own separate (confidential high) LAN.

Installations have been made on the CVN-71 and 73. The next carrier will be the CVN-74. First installation of the Information Management System (ISIS) on the CVN-73 was in 1995. ADMACS is now a Milestone III system. ADMACS interfaces with other systems including GCCS-M, CC TV, NAVSSI, and NSWPC. ISIS is one component system under the ADMACS architecture.

General ADMACS hardware consists of x-terminals throughout the ship and 4 dispersed servers. Grease boards have been replaced with projectors and a plan to move to flat panel displays.

Process exists to translate functions into data requirements.

ADMACS systems are involved in numerous operations from planning to flight operations, and reports information.

NavMPS could utilize a lot of the information maintained within ADMACS. Some of this will be used in the SPF. Do to a difference in classification, there would need to be a push, not pull of the data.

ADMACS is IT-21 level 1 compliant. It resides on a separate LAN, hardware and software ISNS backbone. They are looking for an IT-21 Level 3 compliance by 4Q FY03. Future LAN could be integrated or remain separate.

NERTS ACTION ITEMS

7 Apr 00

1. **Mike Hecker:** JMPS plan for SOO. Coordinate with Dave Gay and Liz Eagle.
2. **Mike Hecker:** Can ADMACS non-critical data be moved to JMPS (NT solution) or REDS?
3. **Mike Hecker:** Identify REDS functions that may migrate to JMPS.
4. **Mike Hecker:** Determine what product is needed prior to departure (end of May).
5. **Mike Hecker and Dave Pearson:** When and who to talk to at Logicon. Possibly Frank O'Brian. Probably after pre-ASP. get ADMACS brief and REDS brief
6. **Mike Hecker and John Kovacs:** Coordinate ADMAC ISIS Demo on 21 April.
7. **Carl Tankersley:** Work CONOPS and Operational Architecture issues with AIR-4.10
8. **Rick Grabenstein:** Develop near term security issues for JMPS (vice log-term CONOPS).
9. **Mary Collins and Nate Schutz:** Access to METAL functionality.
10. **Mary Collins and Logicon:** Options on using I3 Microsoft Office front end for JMPS vice building functions in JMPS.
11. **Jack Sommer:** Does the PIF have GCCS-M version 3.1.2.1?
12. **Jack Sommer:** Is IMF Web Architecture for NSWPC implemented?
13. **Dan Wright:** Provide a more detailed TAMPS HW overview to John Kovacs-ADMACS.
14. **Dan Wright:** Get VF-101 (ATMIOS) POC to John Kovacs. Similar system as ADMACS for shore based.
15. **Dan Wright:** Provide ROM hardware costs for each option. Look at Total Ownership Costs (TOC). (API maintenance, redundant capability, etc.).
16. **Dan Wright:** Coordinate Sun Serengeti brief for members of Team that have not seen it.
17. **Ken MacDonald:** Provide hardware plan. Server phasing plan, etc.
18. **Ken MacDonald:** Post briefs and minutes on NavMPS website.
19. **Mike Stine:** Get with Nate Schultz regarding XML standards (CRD).

[Possible brief for Mugu, Logicon]

Capt Moebius, Mike Hecker, BJ Ramsay, Dan Wright going to Lakehurst on Fri 21 Apr.