11th International
Command and Control Research and Technology Symposium
26-28 September 2006
De Vere University Arms, Cambridge, UK

TOPIC: Coalition Command and Control in the Networked Era

TITLE: Enabling Interoperability in C2 Aircraft

AUTHORS:

(1) Charles P. Satterthwaite (**point of contact**)
Air Force Research Laboratory
Information Directorate, Advanced Computing Division
Embedded Information Systems Branch (AFRL/IFTA)
2241 Avionics Circle, Bldg. 620
Wright-Patterson AFB, OH 45433-7334
Phone: 937-255-6548 x3584
Fax: 937-656-4277
Email: charles.satterthwaite@wpafb.af.mil

(2) David E. Corman
The Boeing Company
P.O. Box 516 MC S111-1335
St. Louis, MO 63166-0516
Phone: 314-234-3725
Fax: 314-233-8323
Email: david.e.corman@boeing.com

11th International
Command and Control Research and Technology Symposium
26-28 September 2006
De Vere University arms, Cambridge, UK

TOPIC: Coalition Command and Control in the Networked Era

TITLE: Enabling Interoperability in C2 Aircraft

Charles P. Satterthwaite
Air Force Research Laboratory
Information Directorate, Advanced Computing Division
Embedded Information Systems Branch (AFRL/IFTA)
2241 Avionics Circle, Bldg. 620
Wright-Patterson AFB, OH 45433-7334
Phone: 937-255-6548 x3584
Fax: 937-656-4277
Email: charles.satterthwaite@wpafb.af.mil

Dr. David E. Corman
The Boeing Company
P.O. Box 516 MC S270-4265
St. Louis, MO 63166-0516
Phone: 314-234-3725
Fax: 314-233-8323
Email: david.e.corman@boeing.com

Abstract

The warfighter of today is increasingly dependent upon information that gives him or her precise understanding of their role in hostile (or peace keeping) activities. The information must be timely, concise, and secure in order for the warfighter to be successful in their endeavors, which includes surviving the activity. Though the advent of network technologies is providing huge improvements in useful information, both the access and usability of this information is limited by the warfighter's legacy systems.

The Air Force Research Laboratory (AFRL), with support of The Boeing Company, is executing several research initiatives targeted at these limitations. AFRL is developing the Joint Battlespace Infosphere (JBI) as a means to realize information dominance. In effect, the JBI can be viewed as a tactical internet that provides unprecedented access to data sources. Through this wide-area network connectivity, the JBI can be accessed, searched, and manipulated to create new products.

While the ability to access large quantities of data is vital, the essential capability of the JBI is to support the translation of data into actionable information. This capability directly satisfies the principal need of Command and Control (2) The AFRL/Boeing Insertion of Embedded Infosphere Support Technologies (IEIST) initiative has already demonstrated dramatic improvements in the exchange of information between deployed tactical elements including airborne C2 and information nodes worldwide. IEIST focuses on the integration and requirements for off-board software agents, designed to augment embedded tactical systems and interface with the evolving JBI, while still providing interoperability with legacy systems and communication links.

Introduction

Weapon and surveillance systems and the supporting command and control system elements can be considered nodes or internet protocol (IP) addresses on a wide-area network. Each node becomes both: 1) a server of raw data, collected by its on-board sensors and transmitted, to the JBI; and 2) a client of other servers. Unfortunately, much of this process must be performed using legacy systems. The important next step is to identify a path for providing the benefits of the information technology (IT) revolution to the particular legacy systems without requiring their complete re-development.

IEIST research is being conducted by AFRL/IFTA with support from Boeing in coordination with development of the JBI and other Global Information Grid (GIG) implementations. IEIST is dedicated to extending legacy systems to meet evolving GIG information exchange challenges by applying technologies that enable, automate and expedite this information exchange process. IEIST promises to deliver dramatic improvements in the exchange of information between deployed tactical elements including airborne C2 and information nodes worldwide. IEIST focuses on the integration and requirements for off-board software agents, designed to augment embedded tactical systems and interface with the evolving GIG, while still providing interoperability with legacy systems and communication links. We have appropriately

named the off-board agent responsible for a specific platform - the Guardian Agent (GA). The essence of IEIST is to understand the information needs and collection capabilities of the platform, as described by the platform-specific Force Template (FT), and to match these against information sources and destinations throughout the GIG. In addition, IEIST has a technology focus on application of Quality of Service (QoS) management techniques for efficiently allocating scarce system resources to best meet its own information needs and those of its information subscribers. Furthermore, IEIST is dedicated to demonstrating the tactical utility of the evolving GIG while developing and prototyping requirements for GIG services which will benefit tactical consumers of GIG products and will enable tactical systems to become suppliers of information which is useful to other GIG nodes.

Relevance to C2

The essential capability of the JBI and IEIST is to support the translation of data into actionable information. This capability directly satisfies the principal need of Command and Control. The AFRL/Boeing IEIST initiative has already demonstrated dramatic improvements in the exchange of information between deployed tactical elements including airborne C2 and information nodes worldwide.

IEIST focuses on the integration and requirements for off-board software agents, designed to augment embedded tactical systems and plug into the evolving JBI, while still providing interoperability with legacy systems and communication links. The essence of IEIST is to understand the information needs and collection capabilities of the platform, and match these against information sources and destinations in the JBI. Key elements of the IEIST Architecture include the Guardian Agent (GA), the Host Agent (HA) and the Force Template (FT). The GA identifies and accesses information of interest across the JBI, evaluates the tactical utility of the accessed information, and transmits the information to the tactical element (aircraft) using available communications. The HA is a thin layer, which resides on the tactical node and operates in conjunction with the Operational Flight Software (OFP) The Host Agent provides an interface between extant tactical systems and Guardian Agents, using legacy tactical data links for communications. The FT is an information object that defines the information generation capabilities and information needs of the tactical platform. IEIST has already demonstrated integration of GAs and HAs for multiple tactical assets and C2 nodes communicating with JBI protocols and services over a simulated Link 16 interface. Other agents within the IEIST demonstration scenario have automatically generated time critical target (TCT) Evidence Files, which were transmitted to and exhibited on the cockpit displays of assigned prosecution assets.

IEIST

The GA, Figure 1, is the key concept developed under IEIST. It is an off-board agent that represents the guarded platform in all interactions with the GIG and with other elements of the force structure through their GAs. It is able to take advantage of its location on a powerful, local server/PC that has broadband connectivity to requisite information sources. Through the FT, the GA "knows" the platform mission, characteristics, as well as the status of the platforms information needs and information generation capabilities. It solves the problem of aircrew/operator information over-load by filtering information into that which is relevant to the platform. It monitors for new threats and evaluates their importance using a high fidelity threat analysis module provided by the platform. The GA is designed to work with future de-confliction services and with modern weapon/target pairing decision aids. It supports real-time collaboration including match-making service for real-time sensor re-allocation. It gives Platforms Subscription/Publication/Query capability. Finally the GA can connect with other GAs through either a GIG or another network.

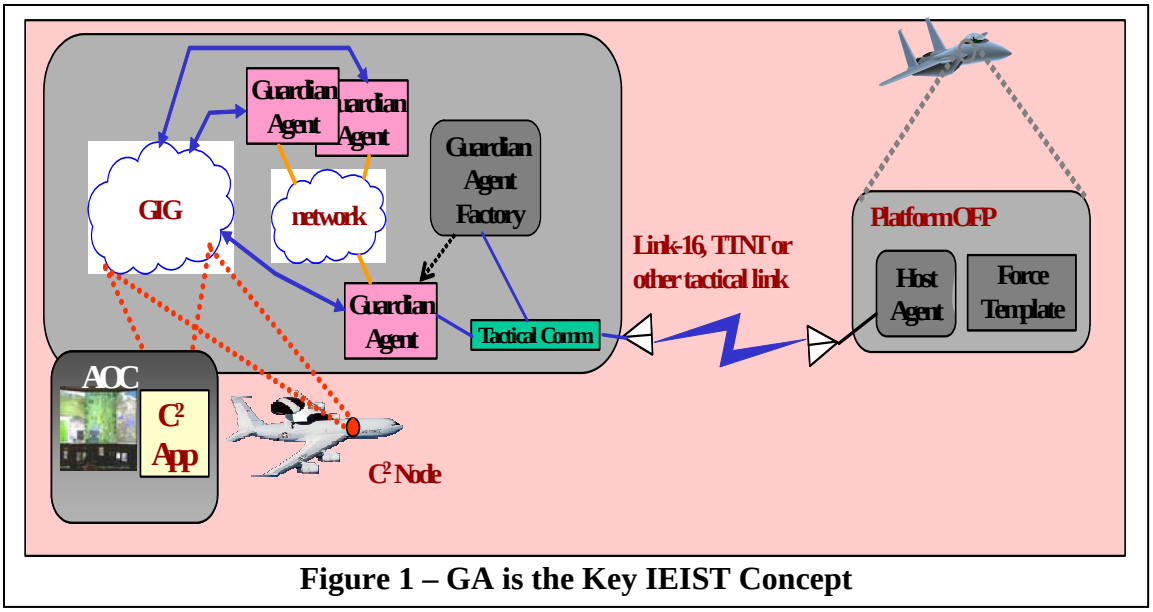


Figure 1 – GA is the Key IEIST Concept

The GA has a modular design, as shown in Figure 2. Within this architecture, the Guardian Agent core is generic in that it behaves the same independent of platform type, infosphere, or other module implementations. The GA also provides the non-core modules shown in the figure. These include: 1) GIG Module, 2) Time Service Module, 3) Platform Module, 4) Threat Analysis Module, 5) Router Module and 6) Threat Filter Module. Each of these non-core modules can be replaced by platform-supplied modules. Platform-supplied-module writers use abstract interfaces provided by the core. Module writers must have their module interact with the GA core in a specified manner. The capability for platform-supplied modules is particularly valuable for the Platform Module, Threat Analysis Module, Router Module and Threat Filter Module that enable the platform to tailor the IEIST capabilities to their platforms specific needs and capabilities.

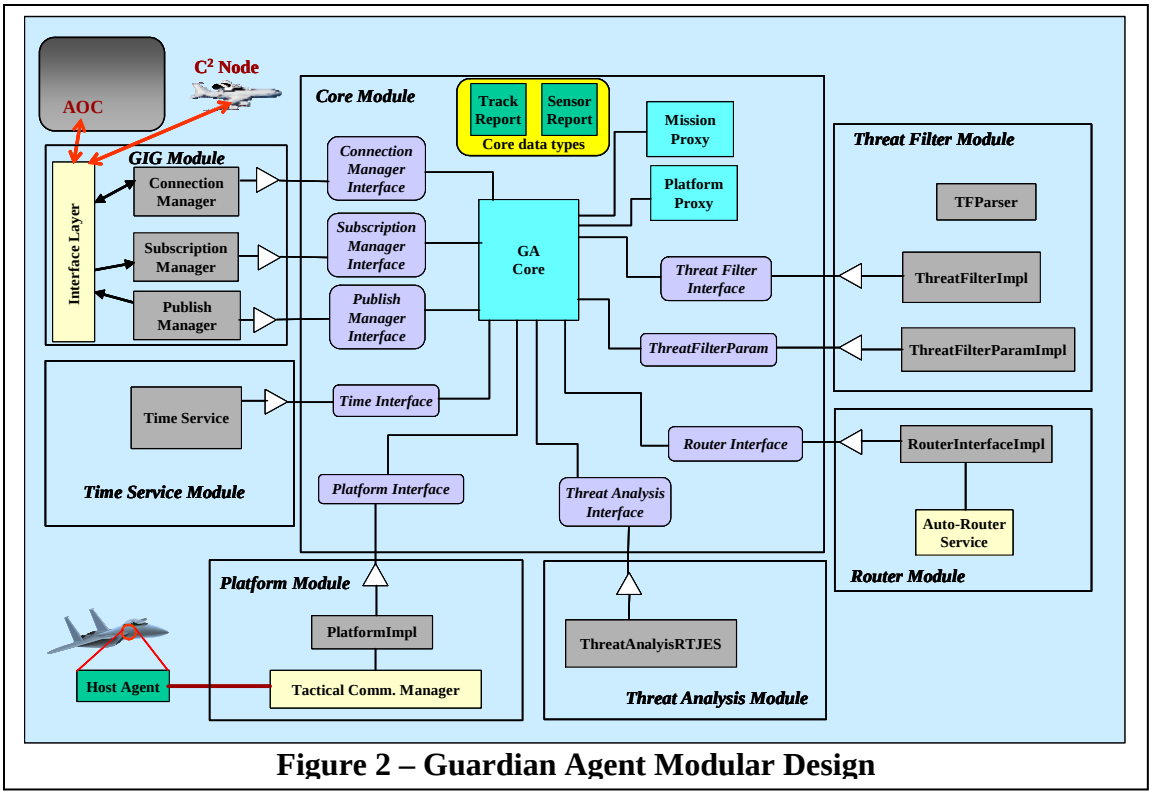


Figure 2 – Guardian Agent Modular Design

The Host Agent, Figure 3, is a "thin client" located on the platform. In consideration of normal platform limitations, it has a small memory and central processing unit (CPU) footprint. The HA is designed to impose minimal impact on platform operational flight program (OFP). The HA performs only those functions needed to support the interfacing of the platform with the Guardian Agent. The HA is connected to GA via standard tactical data link such as Link-16. The HA implementation is platform specific.

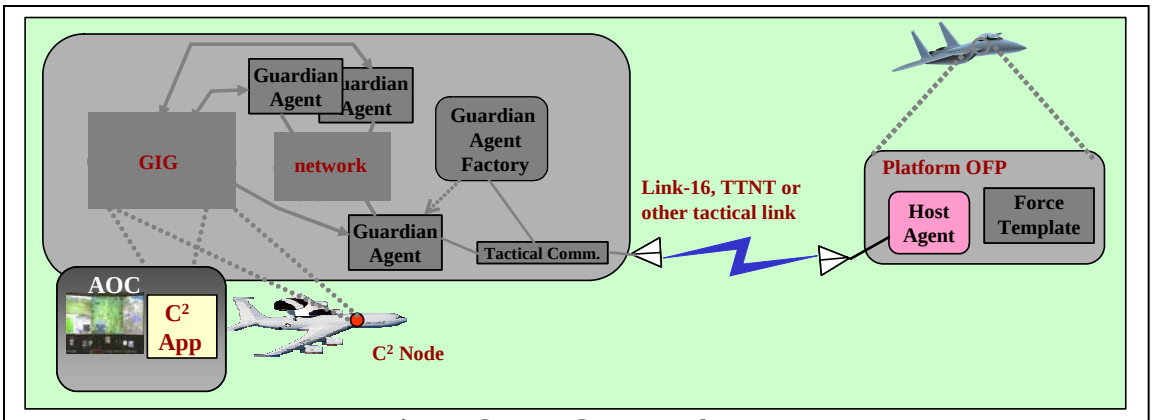


Figure 3 – IEIST Host Agent

Host Agent provides a gateway for aircrew interaction with GA and C2 Applications. The HA can be designed to use existing on-board displays, or HA functions can be

provided in an on-board laptop or personal digital assistant (PDA). The HA can gather state and status information for transmission to GA. Integration of the HA into the platform avionics is a platform decision. Tighter integration enables additional functionality in terms of integrated displays, OFP access to off-board data and off-board access to platform data. This tighter integration comes at the cost of more extensive OFP modification. Figure 4 depicts multiple HA integration approaches.

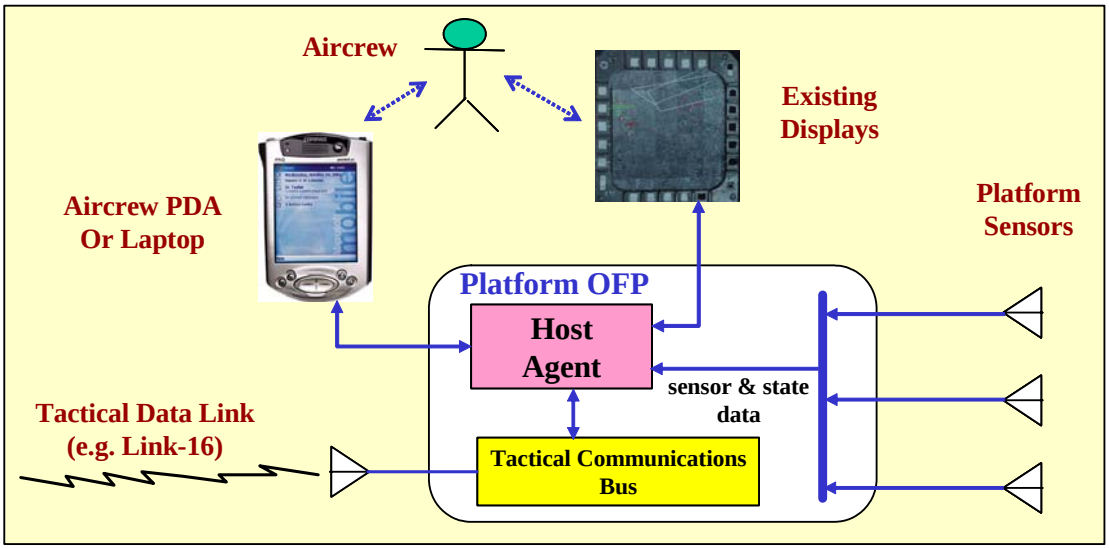


Figure 4 – Host Agent Platform Integration

The Force Template defines the relationship between a client (like the Guardian Agent) and a GIG. The FT is used to connect to the GIG. In the IEIST concept, the FT resides on the platform with the Host Agent and is downloaded to the GIG at the start of the mission. This is further discussed along with the Guardian Agent Factory below. Alternatively, the FT could be stored at other locations within the GIG. In IEIST the FT is the mechanism that defines the GA for a particular platform and mission. The FT consists of two files contained in a zip archive file: 1) An extensible mark-up language (XML) file (platform data, GIG publish/subscribe information, security, listing of GA modules provided by FT), and 2) a Java Jar file (platform-provided GA functionality in the form of GA modules). This zip file can be transmitted via common object request broker architecture (CORBA) octets sequence data transfer that was successfully demonstrated for the Weapon System Open Architecture (WSOA) program image transfer. Figure 5 depicts the IEIST FT implementation.

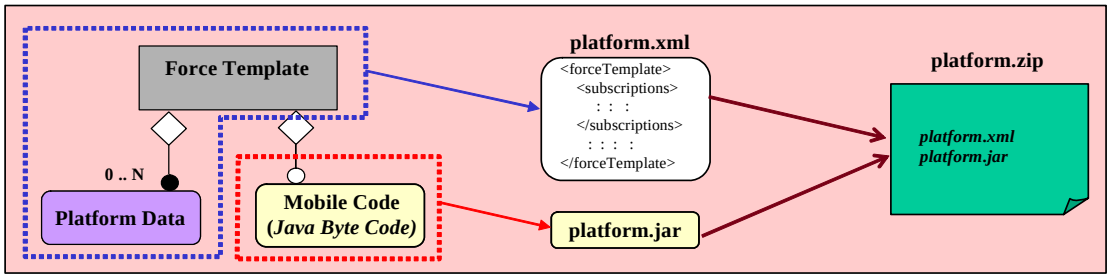


Figure 5 – Force Template Implementation

The Guardian Agent Factory enables operational creation and configuration of Guardian Agents. The GA Factory implements the "mobile code" capability of the Guardian Agent. As discussed above, the mobile code is contained in FT that is initially part of the HA on the platform. When a platform desires to be an IEIST participant it sends a request to the GA Factory along with its FT. The GA Factory has an operator interface for accepting or rejecting platform "join" requests. If the platform is accepted, the GA Factory instantiates a GA for the platform and includes any platform provided mobile code. Security issues with regard to a platform joining a GIG would be addressed by the Guardian Agent Factory. Figure 6 shows the GA Factory within the IEIST architecture.

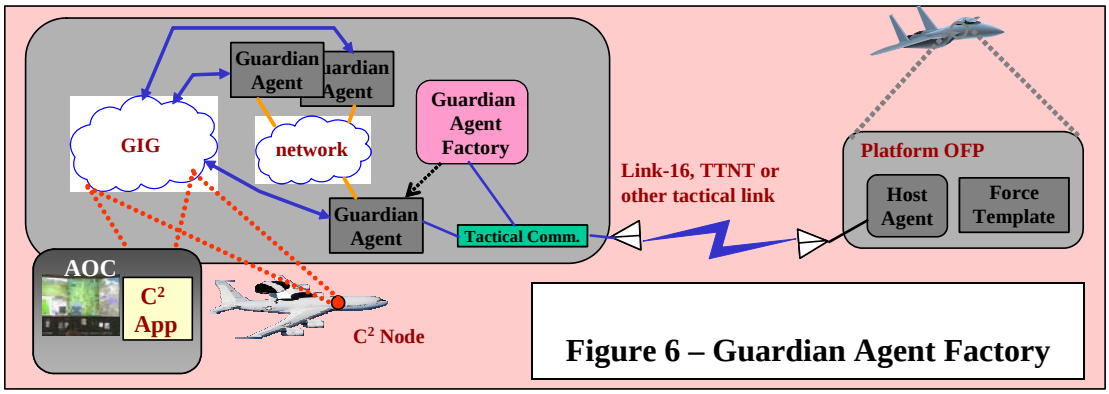


Figure 6 – Guardian Agent Factory

The C2 Platform as the Center of Network Centric Warfighting Activity

IEIST utility is further demonstrated by plugging a C2 system into the emerging Global Information Grid, and developing a set of GA functions that enable the C2 platform to have a Web Portal Demonstration which accesses simulated air operation center (AOC) information for weather and air tasking order (ATO) updates. Regarding weather updates the following subscription capabilities were demonstrated: 1) User can specify subscription to a weather object (Meteorological Aerodrome Report [METAR} data or XML format), 2) Subscription includes specification of a filter for the stations of interest, 3) When an update from the infosphere is received, the update is forward to the C2 on-board portal (updates are only for those stations that are part of the current subscription filtering), 4) The C2 operator can dynamically change the filtered stations, 5) (Initialization) When the GA is on-line, the latest METAR data for the stations specified as part of the subscription list is sent to C2 portal, and 6) (Station Status) The station update sent to the Portal will include a color-coded status (Red, Yellow, Green.) The station status is calculated based on a C2 specified criteria for the values within a METAR report. For example, visual flight rules (VFR) would correspond to "Green status" while instrument flight rules (IFR) could correspond to "Red Status." Criteria would be part of the weather module initialization part of the GA Force Template. Query capabilities include: 1) The operator at any time can query for METAR data from any station that has data published to the infosphere, and 2) The query station may or may not be part of the list of stations that have updates as part of the Weather subscription. For the ATO update, subscription capabilities include: 1) User can subscribe for ATO

updates, 2) Subscription can include meta-data filtering of the ATO update, 3) When the GA receives a ATO update (that meets the subscription filtering criteria,) it will send the update to the C2 portal, and 4) The subscription will be static (dynamic updates to filtering is not required). No ATO update Query capability is required. Figure 7 shows the CORBA based Web Portal integration approach used to accomplish these objectives in the demonstration.

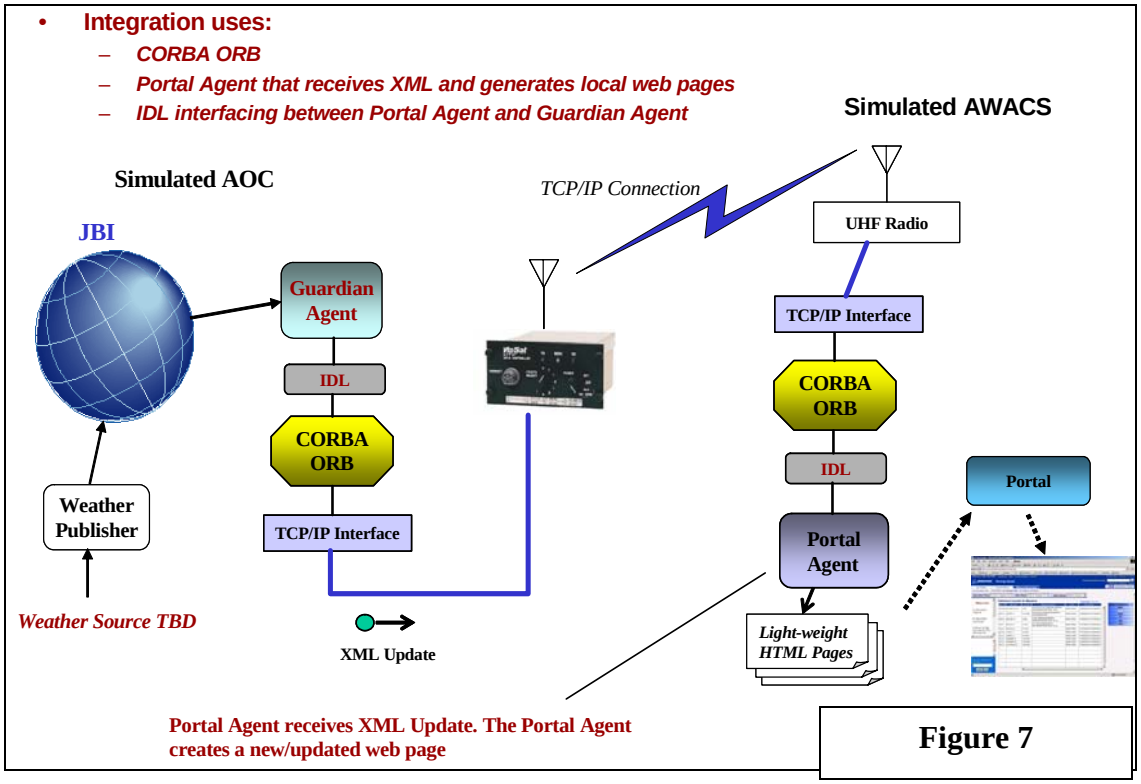
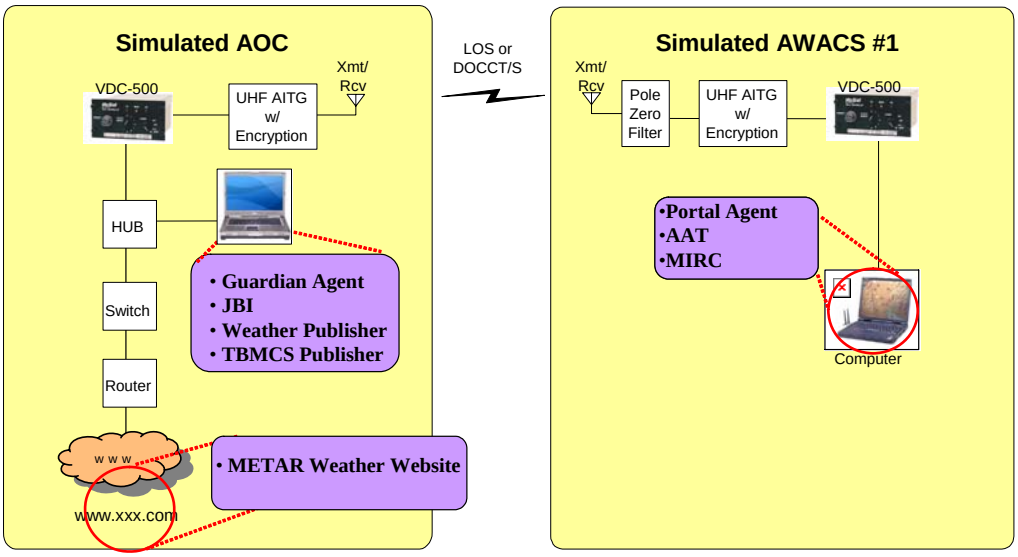


Figure 7

Figure 8 shows the physical configuration for the demonstration. The IEIST components execute in a separate computer that acts as a simulated AOC. IEIST personnel developed a weather service and ATO update utility to support the demonstration. The connectivity between the simulated AOC and the AWACS is UHF radio. The VDC 500 acts as a modem extending IP protocols over low bandwidth, half-duplex, full-duplex and simplex radios.

Physical Block Diagram



Aircraft Integration Lab

Figure 8 Physical Block Diagram for IEIST AWACS Demonstration

Benefits to the C2ISR

The benefits of Network Centric Warfare and the JBI (GIG) to the C2ISR community are well documented, and beginning to be understood. Commanders are better able to coordinate their war fighting resources with their latest intelligence. In theory, the flow of information from the commander to and from his/her war-fighters is greatly improved with this new infrastructure. But the connectivity to the war-fighter still needs considerable improvements which allow him/her to publish and subscribe to the C2 resources.

Guardian Agents and Force Templates are technologies that greatly improve this war-fighter connectivity. The Guardian Agent reviews, filters, and formats information that is pertinent to the war-fighter. It also is able to publish time critical information that the warfighter discovers to the C2 platform. The Force Template provides a way for legacy war-fighting systems to be understood and enhanced so that they can play in the Network Centric engagement.

Summary/Conclusions

The issue of the modern warfighter is his/her dependence upon information that gives them a precise understanding of their role in hostile (or peace keeping) activities. The information must be timely, concise, and secure in order for the warfighter to be successful in his/her endeavor. Huge opportunities await warfighters who can tune their legacy systems to play in this information centric world.

The Air Force Research Laboratory, in partnership with Boeing, has developed key technologies that address the issue of connectivity of legacy systems to global information grid (GIG) enabled information capabilities as well as the transportation of these capabilities into decision quality information. The Joint Battlespace Infosphere (JBI) offer vastly improved information management services. These services facilitate the assimilation of JBI clients and their processes into an infosphere by defining their information needs and products and their roles, capabilities and organizational affiliations. Another key technology, which refines the JBI services down to the warfighter platform level, is the Insertion of Embedded Infosphere Support Technology (IEIST) program. IEIST has developed a tactical node architecture made up of Guardian Agents, Host Agents, Force Templates, and Guardian Agent Factories. These components enable a legacy system to have extended "off-board" information centric capabilities through the GIG and honed to its specific mission requirements.

This offers extraordinary advantages to coalition C2 platforms. They now have a way to be actively connected to the diverse campaign warfighters. Mission planning, and re-planning, can now be made dynamic activities. Situation awareness and responsiveness are now realities.

References

1. For AFRL/IFTA by Boeing Phantom Works, *Incremental Upgrade of Legacy Systems for Common Battle Management System Battle-Management Elements (IULS-CBE) Study Program Final Report*, 25 January 2002.

2. [USAF, 1999] *United States Air Force Scientific Advisory Board Report on "Building the Joint Battlespace Infosphere"*, Volume 1: Summary, SAB-TR-99-02, December 17, 1999.

3. [USAF, 1999] *United States Air Force Aerospace Command Control Intelligence, Reconnaissance (C^2ISR) Campaign Plan 2000*, December 23, 1999.

4. [USAF, 1997] *Chairman of the Joint Chiefs of Staff, "Joint Vision 2010"*, May, 1997.

5. [USAF, 2000] *Chairman of the Joint Chiefs of Staff, "Joint Vision 2020"*, June, 2000.

6. Satterthwaite, C. P., Corman, D. E., and Herm, *T. S., Transforming Legacy Systems To Obtain Information Superiority,* 6th International Command and Control Research and Technology Symposium, U. S. Naval Academy, Annapolis, MD., June 2001.

7. *The Unified Modeling Language User Guide*, Grady Booch, James Rumbaugh, and Ivar Jacobson, Addison-Wesley, 1999.

8. UML Use Case Tutorial Document.
http://www.objectmentor.com/resources/articles/usecases.pdf

9. *OMB Unified Modeling Language Specification*, v1.4, Object Management Group, September 2001. Reference located at http://www.uml.org

10. Corman, D. E., Gossett, J., "*WSOA – Using Emerging OSA Standards to Enable Innovative Techniques for TCT Prosecution*", 20th DASC, IEEE/AIAA, October 2001.

11. *Power to the Edge, Command Control in the Information Age,* Alberts, D. S., Hayes, R. E., Center for Advanced Concepts and Technology, June 2003.

12. *Network Centric Warfare, Developing and Leveraging Information Superiority*, Alberts, D. S., Garstka, J. J., Stein, F. P., R. E., Center for Advanced Concepts and Technology, August 1999.

13. AFRL/IF Joint Battlespace Infosphere Office, Force Templates: Standardized Client Information Interface Descriptions for the Joint Battlespace Infosphere, JBI Concept Definition Document, Version 4.0, July 2003.

14. For AFRL/IFSE by ISX Corporation, *Force Templates: Standardized Client Information Interface Descriptions for the Joint Battlespace Infosphere,* 28 July 2003.

15. Levin, Lawrence J., Critical Architectures, LLC, *Force Templates for Assimilating Unit Infospheres: Phase I Final Report*, AFRL/IF Technical Report.

16. For AFRL/IFTA by Boeing Phantom Works, *Insertion of Embedded Infosphere Support Technologies (IEIST), Final Report,* AFRL/IFTA Technical report, 31 August 2005.