7th International
Command and Control Research and Technology Symposium
June 11-13, 2002
Naval Post Graduate School
Monterey, CA

TITLE: Real-time Information Extraction for Homeland Defense

TRACK: Network-Centric Applications /Homeland Defense

AUTHORS:

(1) Charles P. Satterthwaite (**point of contact**)
Air Force Research Laboratory
Information Directorate, Information Technology Division
Embedded Information Systems Engineering 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) 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

(3) Thomas S. Herm
The Boeing Company
P.O. Box 516 MC S270-4265
St. Louis, MO 63166-0516
Phone: 314-233-7277
Fax: 314-233-8323
Email: thomas.s.herm@boeing.com

Real-time Information Extraction for Homeland Defense

Charles P. Satterthwaite
Air Force Research Laboratory
Information Directorate, Information Technology Division
Embedded Information Systems Engineering 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

Thomas S. Herm
The Boeing Company
P.O. Box 516 MC S270-4265
St. Louis, MO 63166-0516
Phone: 314-233-7277
Fax: 314-233-8323
Email: thomas.s.herm@boeing.com

Abstract

The National interest in Homeland Defense was the farthest thing from most American's minds prior to the horrific attacks of the Pentagon and the World Trade Center. The worst nightmares of many Department of Defense leaders and technologists had been realized. Our Country was hit, and hit hard. No longer could we take for granted our borders, our way of life, or our freedom. For a short while, no cost was to high to re-secure these basic privileges of American life. But the practicality of manning and equipping airports, seaports, power plants, water supply, borders, and many other American Infrastructure entities demanded a more comprehensive and cost effective way of defending our homeland. One practical investment is in the Nation's network of airborne warning ground based radar systems that are deployed throughout the United States and Canada to monitor any air traffic entering either of these countries. This system of networked radars was designed with the philosophy that threats would originate outside the borders of the United States and Canada. The system worked so well, that when thoughts of expanded capability presented themselves, they were abandoned in favor of more (apparent) pressing issues. This paper addresses this system of systems, and how with some insertion of technology, it can absorb its share of the National Homeland Defense.

Problem Or Issue

The events of September 11 have given a new emphasis to real-time monitoring of domestic air traffic and development of decision aids, which support the safe but immediate intercept and possible interdiction of suspicious aircraft. In response to these challenges, National Command Authority has delegated release authorization, for the use of air interdiction weapons against private and commercial aircraft, to subordinate levels of command. The real-time, decision-making requirement inherent in this delegation of authority necessitates great improvements in the timeliness, completeness and automation of supporting systems. When examining the infrastructure of the resources required to obtain a timely response to these challenges, it becomes apparent that existing legacy systems will need to continue to contribute both on the ground and in the air. Current scenarios for domestic surveillance systems focus on a small number of tracks originating outside CONUS and provide limited intelligence above that obtained from radars, flight plans and through execution of aircraft intercept. This situation is no longer acceptable. In some cases, plans have been initiated to replace elements of these legacy systems with off-the-shelf solutions, which offer more current hardware and software architectures. However, these potential replacement systems are years away from full operational capability and will apply military surveillance techniques against a domestic environment, i.e. they were also created with the paradigm that the threat is relatively easy to identify and will originate outside the defended area. Unless further developed, they will not include the types of real-time decision aids required to rapidly discern hostile intent and to access additional information pertinent to effective disposition of the situation.

In the current environment the capability is needed to monitor all tracks, regardless of their point of origin, and to quickly and automatically identify those, which represent a substantial risk. Because of the extreme number of domestic air tracks, automated means must be provided to aid in this task. Subsequent to identification as high risk, additional scrutiny and intelligence must be brought to bear such that within a very limited timeline, sound decisions can be made regarding the application of requisite force. In response domestic surveillance systems need to move towards a short lead-time response and adaptive capabilities. These systems require augmented information access integrated into their embedded software architectures and conveyed over established communication links. Information filtering and automated decision aiding are critical. Importantly, these new capabilities must provide two-way information exchange with other elements of the Defense Information Infrastructure as well as civilian agencies including the FAA and Custom Service. This information exchange must also encompass those tactical assets assigned to intercept and potentially engage suspect aircraft.

Relevance To C2

The USAF has evolved the concept of the Joint Battlespace Infosphere (JBI) as a means to realize information dominance. In effect, the JBI (Figure 1) can be viewed as a tactical Internet that provides unprecedented access to data sources. Following up on this analogy, weapon and surveillance systems and the supporting command and control system elements can be considered nodes or 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. Through this wide-area network connectivity, the JBI can be accessed, searched, and manipulated to create new products.

Whilst the ability to access 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 principle need of Command and Control. For example, the recent events of September 11 have pointed out that large and diverse quantities of data were available but had not been pieced together into a coherent story that could be used as the basis for real-time command and control. This process includes separating the small number of potentially hostile tracks from the vast domestic air surveillance picture, rapidly accessing additional information to confirm suspicions, and coordinating a timely and safe intercept while further expanding the actionable information reservoir. From a command and control perspective then, we see that the trends in information technology strongly support the rapid exchange of data between higher orders of command and the rapid extraction of information from this data. 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 IT revolution to the involved legacy systems without requiring their complete re-development. This paper describes an approach to extending legacy systems to meet current challenges by applying agent technologies that automate and expedite the C2 decision process fundamental to responsive Homeland Defense.

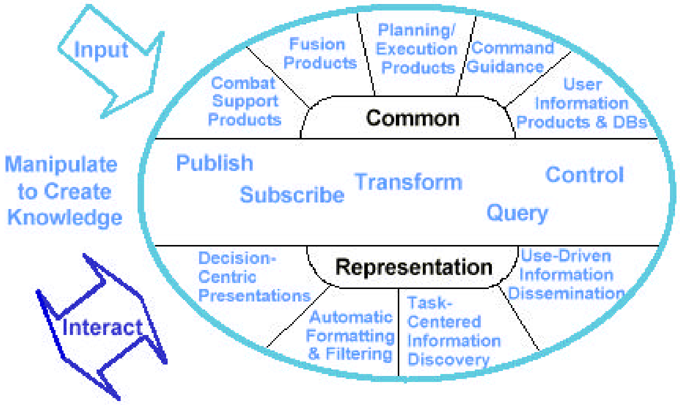

Input
Fusion Products
Planning/ Execution Products
Command Guidance
Combat Support Products
User Information Products & DBs
Common
Manipulate to Create Knowledge
Publish
Subscribe
Transform
Control
Query
Decision-Centric Presentations
Representation
Use-Driven Information Dissemination
Interact
Automatic Formatting & Filtering
Task-Centered Information Discovery

Figure 1. The Joint Battlespace Infosphere

North American Air Defense (NORAD) is the key organizational element in the C2 chain bridging military C3I systems and civilian air surveillance. The NORAD Atmospheric Early Warning System (AEWS) is located at each Regional Air Operations Control Center (ROCC), performs the function of real-time surveillance of air tracks and supports critical C2 decision regarding intercept and interdiction. The critical element of the AEWS is the AN/FYQ-93 (Q-93), which performs real-time surveillance, identification, and weapons control missions of the ROCCs. The Q-93 has connectivity to numerous domestic radar sights, receives flight plans from the FAA, and has bi-directional communications with NORAD Headquarters and a real-time link to AWACS. The Q-93 hardware platform is based on 20+-year-old equipment including a Hughes H-5118VE Central Computer (CC), and four Hughes HVP-1116 Peripheral computers. The legacy software is written in an obsolete dialect of JOVIAL J3 officially known as JSS JOVIAL. Initiatives have begun to replace the Q-93 with an off-the-shelf military surveillance system. However, it will be several years before this solution may become operational and even then it will not provide many of the capabilities required for effective Homeland Defense. The Q-93 must remain operational until the replacement system IOC. Furthermore, it is essential that additional capability, including real-time access to the information capabilities of the JBI, be infused into the Q-93 and-or its replacement in order to satisfy its greatly increased post-September 11 role.

Authors' Approach To The Topic

This paper discusses the adaptation of three technology initiatives – IEIST, IULS and Soft Walls to the specific needs of Homeland Defense and their integration into a systems-of-systems solution for the problem of timely identification and interdiction of domestic aircraft, which are exhibiting hostile intent. The adaptation of these technologies to Homeland Defense is low risk and offers huge potential benefit in our efforts to combat terrorism and keep our nation safe.

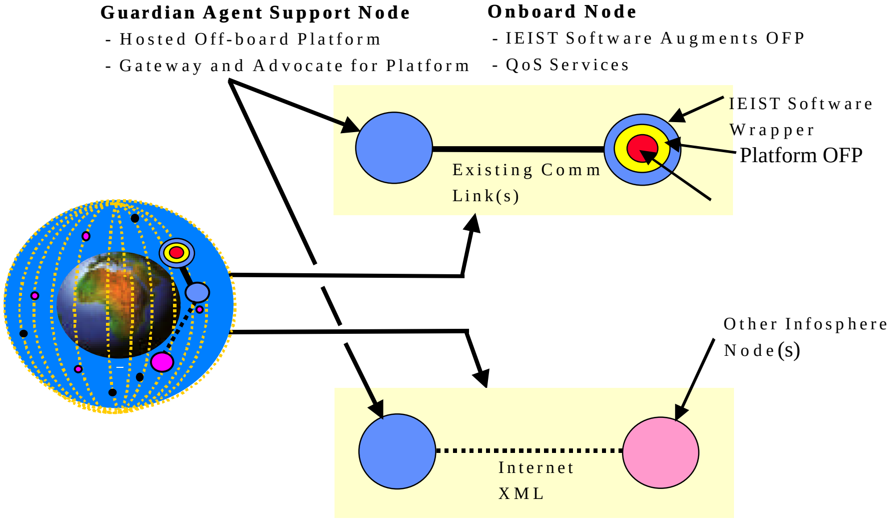
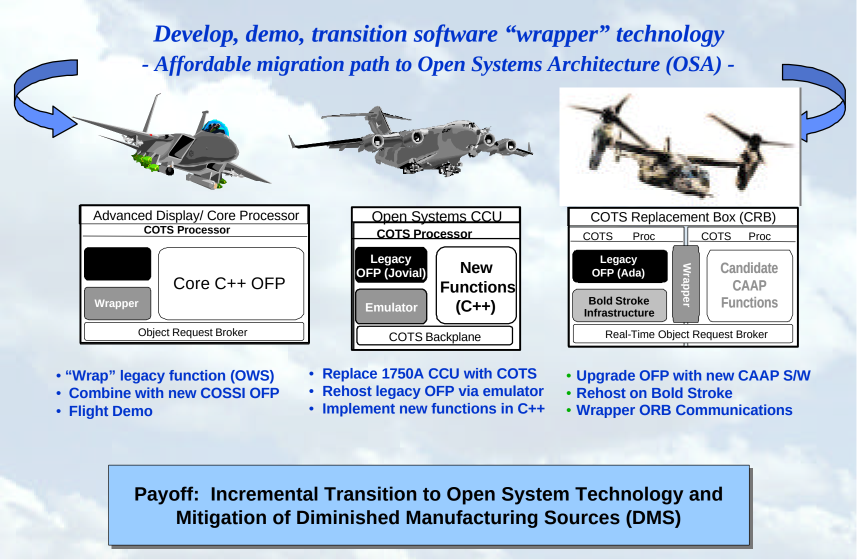

Guardian Agent Support Node
- Hosted Off-board Platform
- Gateway and Advocate for Platform
Onboard Node
- IEIST Software Augments OFP
- QoS Services
IEIST Software Wrapper
Platform OFP
Existing Comm Link(s)
Other Infosphere Node(s)
Internet XML

Figure 2. IEIST Guardian Agent Concept

The Insertion of Embedded Infosphere Support Technologies (IEIST) is an Air Force Research Laboratory initiative, being conducted with support from The Boeing Company. 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 plug into the evolving JBI, while still providing interoperability with legacy systems and communication links, Figure 2. We have appropriately named the off-board agent responsible for a specific platform - the Guardian Agent. The essence of IEIST is to understand the information needs and collection capabilities of the platform and to match these against information sources and destinations in the JBI. 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 it's own information needs and those of its information subscribers.

The Incremental Upgrade to Legacy Systems (IULS) program is another AFRL/Boeing initiative. Under IULS AFRL and Boeing have developed and demonstrated tools and processes designed to enable cost effective, incremental improvements to fielded weapon system software. The products of IULS are: 1) Methodology for analyzing software upgrade approach; 2) Wrapper technology; 3) Toolset for constructing wrappers for software upgrade. IULS technologies have been successfully applied to three significant challenge problems - F-15E, C-17 and MV-22 avionics, Figure 3. These embedded system “wrapper” technologies have direct benefit to Homeland Defense where they can be used to integrate requisite agents into both interdiction and commercial aircraft. Furthermore AFRL/Boeing have recently completed an analysis of the feasibility of applying IULS tools and processes to mitigate the Q-93 hardware/software obsolescence problems and to open the system to new capabilities. The findings are very promising and confirmed IULS viability as a tool for introducing additional hardware and software capabilities – Guardian Agents - into domestic surveillance system architectures.



Develop, demo, transition software “wrapper” technology

- Affordable migration path to Open Systems Architecture (OSA) -

- “Wrap” legacy function (OWS)
- Combine with new COSSI OFP
- Flight Demo

- Replace 1750A CCU with COTS
- Rehost legacy OFP via emulator
- Implement new functions in C++

- Upgrade OFP with new CAAP S/W
- Rehost on Bold Stroke
- Wrapper ORB Communications

Payoff: Incremental Transition to Open System Technology and Mitigation of Diminished Manufacturing Sources (DMS)

Figure 3. IULS Demonstrations

The Soft Walls approach, Figure 4, under development by Boeing and the University of California, Berkeley, proposes to enforce a no-fly zone around critical Government and civilian infrastructure by integration with the aircraft flight control system. As an aircraft approaches the boundary of such a zone, the flight control system responds by creating a force that pushes the aircraft away. The boundaries of these zones are called “Soft Walls” because the aircraft is gently diverted by its own control system when it attempts to enter these zones. Pilot feedback would be provided by a display that is active when the walls are nearby. On-board cautions and warnings could also be generated as a result of an encounter with the Soft Wall. Furthermore, attempts to penetrate the barrier could be tied into off-board systems to generate alerts and provide advance warning to civil and military authorities.

The combination of IEIST technologies is referred to as an IEIST Tactical Node. This terminology corresponds to the original intent of IEIST, which is to extend the capability of tactical elements (aircraft, UAVs, etc.) by augmenting their embedded capabilities with off-board processing and communications. The Tactical Node represents the full Weapons System capabilities including both dedicated on-board and off-board capabilities. Figure 5 shows the elements of the IEIST Tactical Node, which include: the Guardian Agent (GA), the Tactical Communications Manager (including links), the Force Template (FT) and the Host Agent (HA). The GA and HA are of particular interest in the Homeland Defense application.

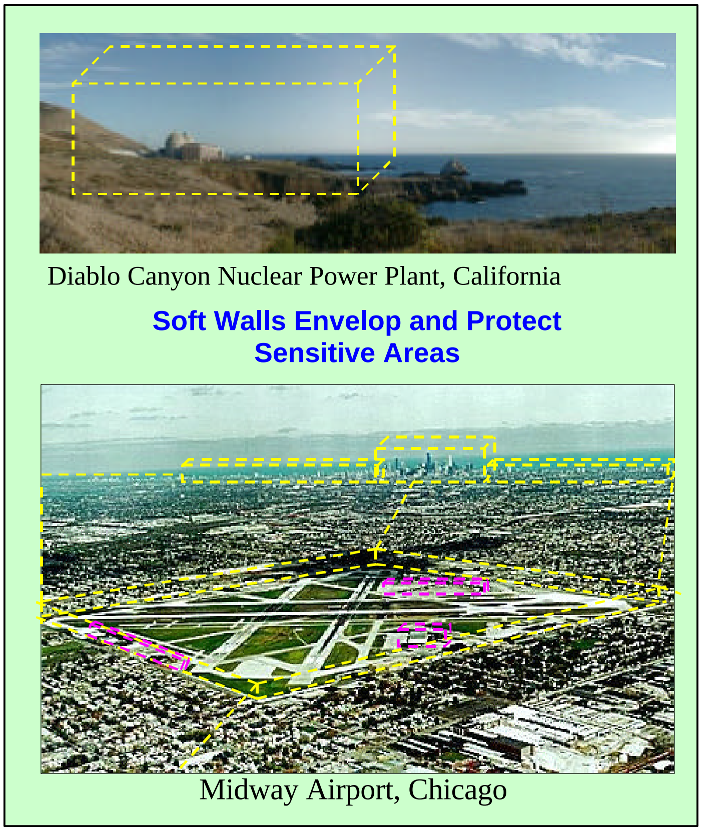
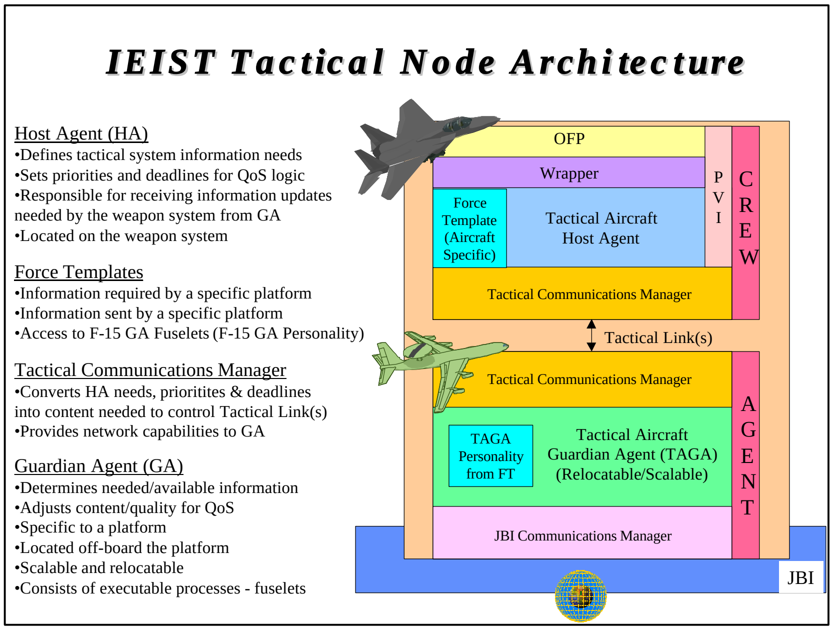

Diablo Canyon Nuclear Power Plant, California
Soft Walls Envelop and Protect Sensitive Areas
Midway Airport, Chicago

Figure 4. Soft Walls Approach

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 GA is scaleable to the tactical need and relocatable anywhere within the JBI. It will be automated, requiring human intervention only in the most stressing tactical situations such as those in which an aircraft has been identified as an imminent threat. The GA design is generic in nature allowing reuse over a wide range of systems.

The Host Agent is a relatively small software entity, which resides on the tactical node and operates in conjunction with the Operational Flight Software. The Host Agent will provide an interface between extant tactical systems and Guardian Agents, using legacy tactical data links for communications. It will include QoS logic similar to the Guardian Agent and will also satisfy any operator interface requirement associated with the additional IEIST functions.

A natural extension of IEIST is the integration of the JBI exploitation capabilities into domestic surveillance systems in order to provide the additional capabilities demanded in the current environment, as shown in Figure 6. In this concept, a Guardian Agent process will be created for each flight plan and track generated in the surveillance system. There are also two sets of Host Agents. The interdicting aircraft, an F-15 in the example, has an HA which allows it to hare information and a common operating picture with controllers on the surveillance system. A second HA might exist on the suspect aircraft, although this second agent is not required. This HA is associated with the Soft Walls logic and provides a strong indication of malicious intent in situations where the pilot attempts to penetrate the "Soft Walls".


IEIST Tactical Node Architecture

Host Agent (HA)
- •Defines tactical system information needs
- •Sets priorities and deadlines for QoS logic
- •Responsible for receiving information updates needed by the weapon system from GA
- •Located on the weapon system

Force Templates
- •Information required by a specific platform
- •Information sent by a specific platform
- •Access to F-15 GA Fuselets (F-15 GA Personality)

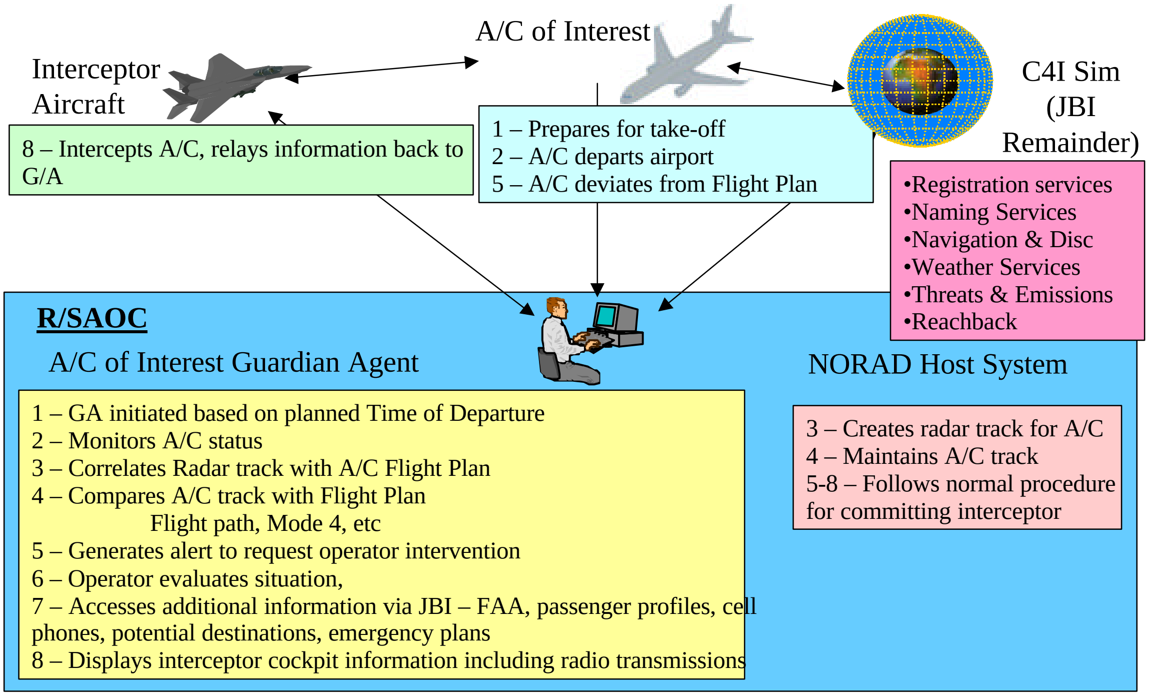
Tactical Communications Manager
- •Converts HA needs, prioritites & deadlines into content needed to control Tactical Link(s)
- •Provides network capabilities to GA

Guardian Agent (GA)
- •Determines needed/available information
- •Adjusts content/quality for QoS
- •Specific to a platform
- •Located off-board the platform
- •Scalable and relocatable
- •Consists of executable processes - fuselets

OFP
Wrapper
P V I
C R E W
Force Template (Aircraft Specific)
Tactical Aircraft Host Agent
Tactical Communications Manager
Tactical Link(s)
Tactical Communications Manager
A G E N T
TAGA Personality from FT
Tactical Aircraft Guardian Agent (TAGA) (Relocatable/Scalable)
JBI Communications Manager
JBI

Figure 5. IEIST Program Elements

Figure 6 presents a typical scenario in which the IEIST Homeland Defense capability might be exercised. After a track is initially detected and a GA process is created, the first activity is to associate tracks with flight plans, if available. In executing this association, and other decisions, the Guardian Agent will execute the "Commander Guidance ".



8 – Intercepts A/C, relays information back to G/A

1 – Prepares for take-off
2 – A/C departs airport
5 – A/C deviates from Flight Plan

•Registration services
•Naming Services
•Navigation & Disc
•Weather Services
•Threats & Emissions
•Reachback

1 – GA initiated based on planned Time of Departure
2 – Monitors A/C status
3 – Correlates Radar track with A/C Flight Plan
4 – Compares A/C track with Flight Plan
Flight path, Mode 4, etc
5 – Generates alert to request operator intervention
6 – Operator evaluates situation,
7 – Accesses additional information via JBI – FAA, passenger profiles, cell phones, potential destinations, emergency plans
8 – Displays interceptor cockpit information including radio transmissions

3 – Creates radar track for A/C
4 – Maintains A/C track
5-8 – Follows normal procedure for committing interceptor

Fig. 6. Homeland Defense Scenario

Boeing has implemented similar rule-based "Commander's Guidance" in their Y-JBI prototype, Figure 7, where agents automatically generate "Intruder Evidence" files, which are passed on to tactical assets for prosecution. Execution of “Commander’s Guidance” entails the application of a set of rules, which determine whether an event has occurred such as a track corresponds to a flight plan. Because “Commander’s Guidance’ is adjustable, criteria may be tailored to the National Threat Alert Status in effect at the time of execution. The first element of “Commander’s Guidance” might say that tracks for which there is no flight plan should be elevated to the next higher level of scrutiny, i.e. they would be monitored for proximity to a no-fly zone. If a track satisfied this additional criterion it might be deemed as meeting “deviant” criteria. Reaction to satisfying “deviant” criteria is discussed in the paragraph below. Tracks with flight plans would be automatically monitored for compliance to the flight plan. The “Commander’s Guidance” would include tolerances for executing this monitoring process. If a track deviated from its flight plan, the appropriate FAA controller would be queried to ascertain if permission to deviate had been given. If permission had been given, the track might be added to the list of those being monitored for proximity to no-fly zones. If permission had not been given, the track might immediately be deemed as meeting “deviant’ criteria. For situations in which a “Soft Walls” HA is available, any attempt to penetrate a no-fly zone would immediately place the track on the “deviant” list.

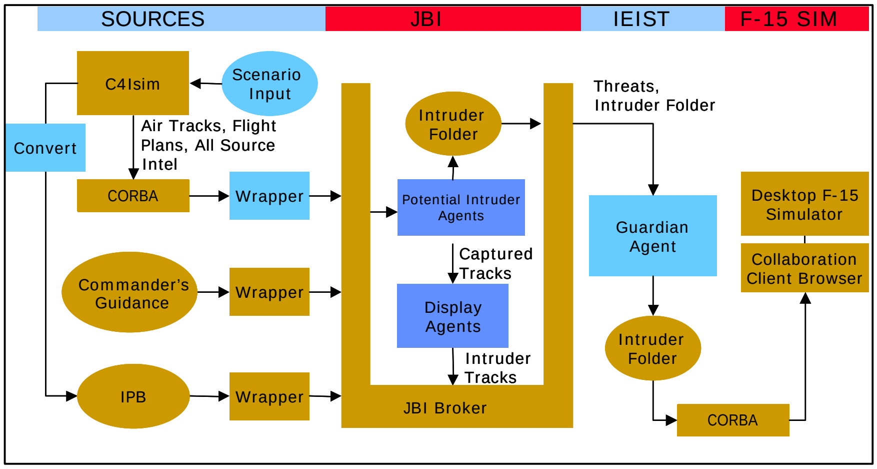


Figure 7. IEIST/Y-JBI Prototype

When a track meets “deviant” criteria, it is to be deemed high risk and brought to an operator’s attention, i.e. “deviant” categorization is an indication of immediate threat. The operator might command intercept based on this information alone or may choose to obtain additional information before committing to intercept. In executing this search for additional information, the operator is given access to the entire JBI in order to access items including aircraft type and capabilities, passenger list, passenger history, cell phone numbers and connectivity, potential high value “targets” along the route and within range of the suspect aircraft. The operator will be assisted in these activities through a set of menus designed to guide him to the proper decisions. When the operator chooses to initiate an intercept with a suspect aircraft, the IEIST capabilities will enable real-time Internet-like communications between the intercept aircraft, the surveillance operator and any other affected JBI nodes. These communication capabilities have already been demonstrated in IEIST using F-15 flight program with the Desktop Test Environment, and will be flight demonstrated during CY02 under the WSOA Program. This real-time connectivity will further assist in accurate and safe employment of weapons, when required.

In the Figure 6 example, the subject aircraft has filed a flight plan. The GA is initiated in response to the flight plan, step 1, and in step 3 the GA correlate a surveillance track with the flight plan. In steps 4 and 5, the subject aircraft requests and receives FAA permission to deviate from the flight plan. Also in step 5, the GA queries the FAA regarding the deviation from flight plan and is assured that it is approved. However, the GA continues to monitor the track for proximity to No-fly zones. In step 6, the GA determines that the A/C track is “deviant” because of proximity to a No-fly zone. An operator is apprised of the situation. Intercept is commanded and the operator accesses amplifying information retrieved from the JBI. The ‘deviant’ status is confirmed in step 7 when the “Soft Walls” HA reports attempts to penetrate a No-fly zone. In step 8, the interceptor contacts the “deviant” A/C and subsequently escorts it to a safe landing in an unpopulated area.

Summary and Conclusions

The need for real-time domestic surveillance and decision making has dramatically increased since September 11. Tools are required to support commanders, who have been authorized to employ live ordinance against suspect commercial aircraft. These tools must be compatible with, and in many cases built upon legacy architectures, which are severely limited both in performance and ability to assimilate change. Fortunately, several technology initiatives, which are well underway or have been successfully demonstrated, offer potential to alleviate this critical need. In particular, agents and JBI exploitation technologies, being developed under the IEIST program can be easily modified and applied to this domain. Furthermore, IULS has demonstrated tools and processes, which readily integrate these agents into legacy embedded and workstation hardware and software architectures. This solution can be further enhanced by utilizing additional agents, resident on commercial aircraft, to sense attempts to guide the aircraft into high value Government and civilian resources. Given this development and integration approach, it is feasible to deploy a prototype system, which responds to the current need, in the 2004 timeframe.

References

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.

[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.

[USAF, 1999] *United States Air Force Aerospace Command Control Intelligence, Reconnaissance (C2ISR) Campaign Plan 2000,* December 23, 1999.

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

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

Satterthwaite, C. P., *Space Surveillance And Early Warning Radars: Buried Treasure For The Information Grid*, 5th International Command and Control Research and Technology Symposium, Naval Post Graduate School, Monterey, CA., June 2000.

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.