Defining A Security Architecture for Real-time Embedded Systems

June 15-17, 2004

Tod Reinhart 937/255-6548 X3582
Tod.Reinhart@wpafb.af.mil
Air Force Research Laboratory
Information Directorate

Carolyn Boettcher 310/607-3585
cbboettcher@raytheon.com
Andy Gandara 310/334-7126
andrewgandara@raytheon.com
Mark Hama 310/334-7660
mhama@raytheon.com
Raytheon Space and Airborne Systems

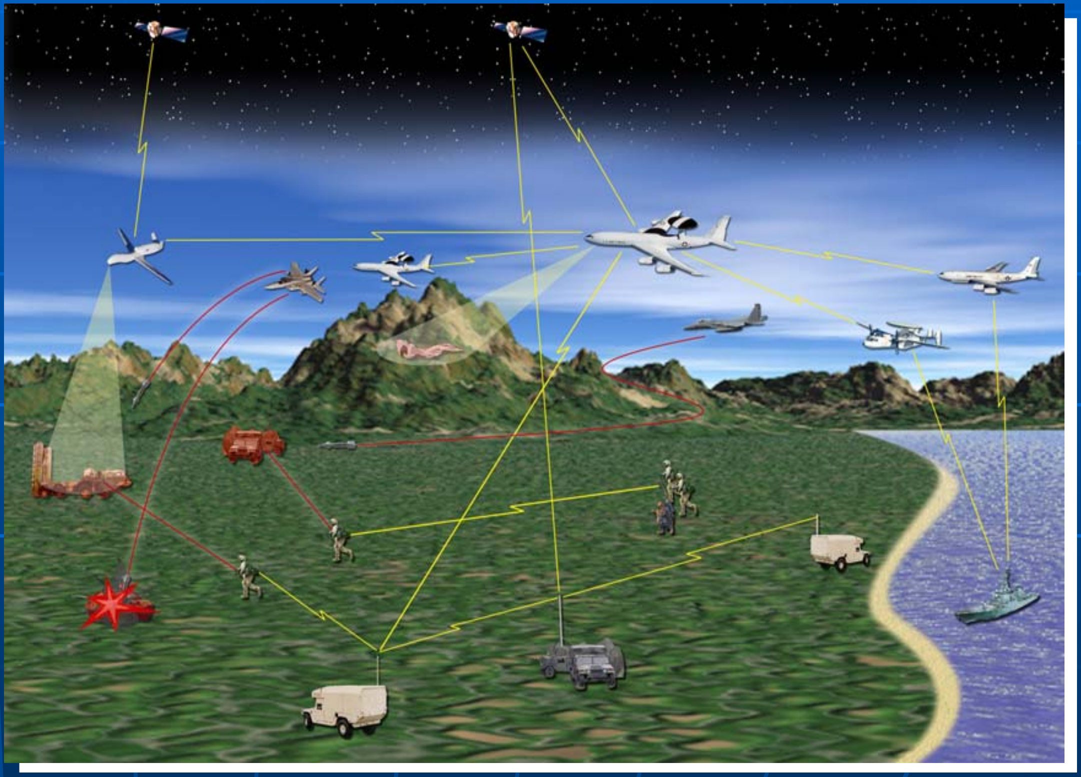
Raytheon

Problem Description

- Current aerospace platforms have limited connectivity with other platforms
  - Limited bandwidth
  - Limited data/information content
  - Limited dynamic connectivity capability
- The DoD is moving from a platform-centric to a network-centric battlespace
  - Increased use of commercial technologies, standards, and mechanisms
    - Eventual transition from Tactical Datalinks (e.g., TADIL-J) to IP-based protocols
    - Middleware, web services, J2EE, publish/subscribe
  - Increased richness of data/information content
    - XML-formatted messages (STANAGS)
  - Increased dynamic connectivity capability
    - Domain-independent infrastructures (e.g., Global Information Grid (GIG) Enterprise Services) that will enable higher levels of interoperability
    - ability to locate and communicate with any platform in the battlespace
- However, the use of commercial standards/technologies and increased platform connectivity introduces the need for higher levels of information assurance

Information Assurance is a System-of-Systems Issue

- Many different types of platforms will be interoperating in the network-centric battlespace.
- Some examples are
  - Navy DD(x), Army FCS, Air Force MC2C, Global Hawk, …
- Interoperable IA approaches are needed to achieve end-to-end information assurance
- Individual platforms must be able to guarantee their own security, even if other platforms are compromised.
- End-to-end quality of service must also be maintained



Technology Trends

- **Trends in the Battlespace**
  - **Increasing dependence on timely and accurate information that needs to be shared between the warfighter, planner, and command centers**
  - **Information that is delayed, corrupted, exposed, or that *originated from an unknown source* threatens mission success**
- **Trends in Military Communications**
  - **Tactical Datalinks are evolving toward IP-based protocols**
  - **COTS middleware products are starting to be used in embedded systems (e.g., CORBA™, J2EE)**
  - **Interoperability enablers such as Java ™ and XML may be used in embedded applications**
- **Trends in Information Assurance**
  - **Information assurance and security at a single layer (e.g., physical network layer) is not considered sufficient**
  - **A layered defense-in-depth is needed to protect each platform**

Raytheon

Program Overviews

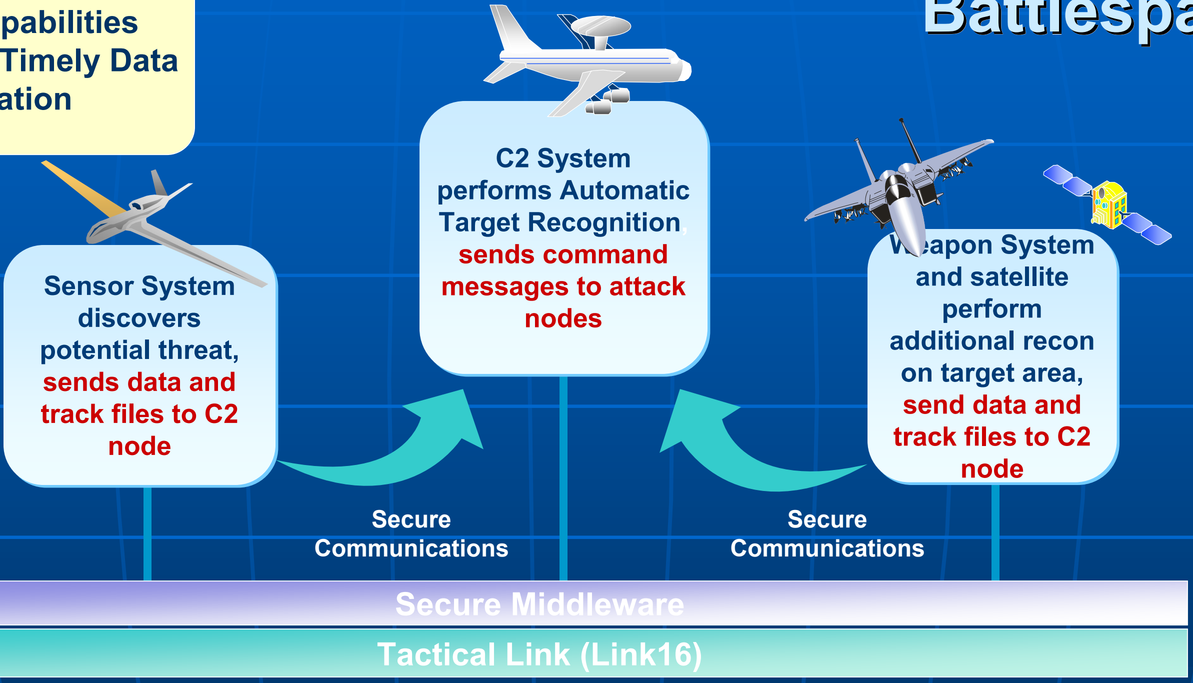
- Embedded Information System Assurance (EISA) Program
  - Completed four year Air Force Research Laboratory (AFRL) technology research and demonstration program
  - Focus on network-based and middleware technologies that provide secure communications for real-time embedded systems
  - Demonstrated secure, inter-platform communications using TCP/IP and CORBA™
- Secure Interoperability for Real-time Embedded Systems (SIRES) Program
  - Initial phase of four year AFRL technology research and demonstration program
  - Will extend EISA results to secure communications for applications using advanced software middleware and application technologies that enable interoperability and network-centric operations
  - Focus on security issues in post-2010 timeframe for DoD Global Information Grid, and especially the AF Joint Battlespace Infosphere

EISA Demonstration Scenario

Raytheon

Network-Centric Battlespace

Investigating Information Assurance Capabilities While Providing Timely Data Dissemination



Sensor System discovers potential threat, sends data and track files to C2 node

C2 System performs Automatic Target Recognition, sends command messages to attack nodes

Weapon System and satellite perform additional recon on target area, send data and track files to C2 node

Secure Communications

Secure Communications

Secure Middleware

Tactical Link (Link16)

- Assess security overhead
- Investigate security between diverse platforms
- Benchmark IPSec, RT CORBA security and Multi Level Secure OS

- Authenticate Sender and Receiver
- Verify data integrity and confidentiality
- Preserve asset availability

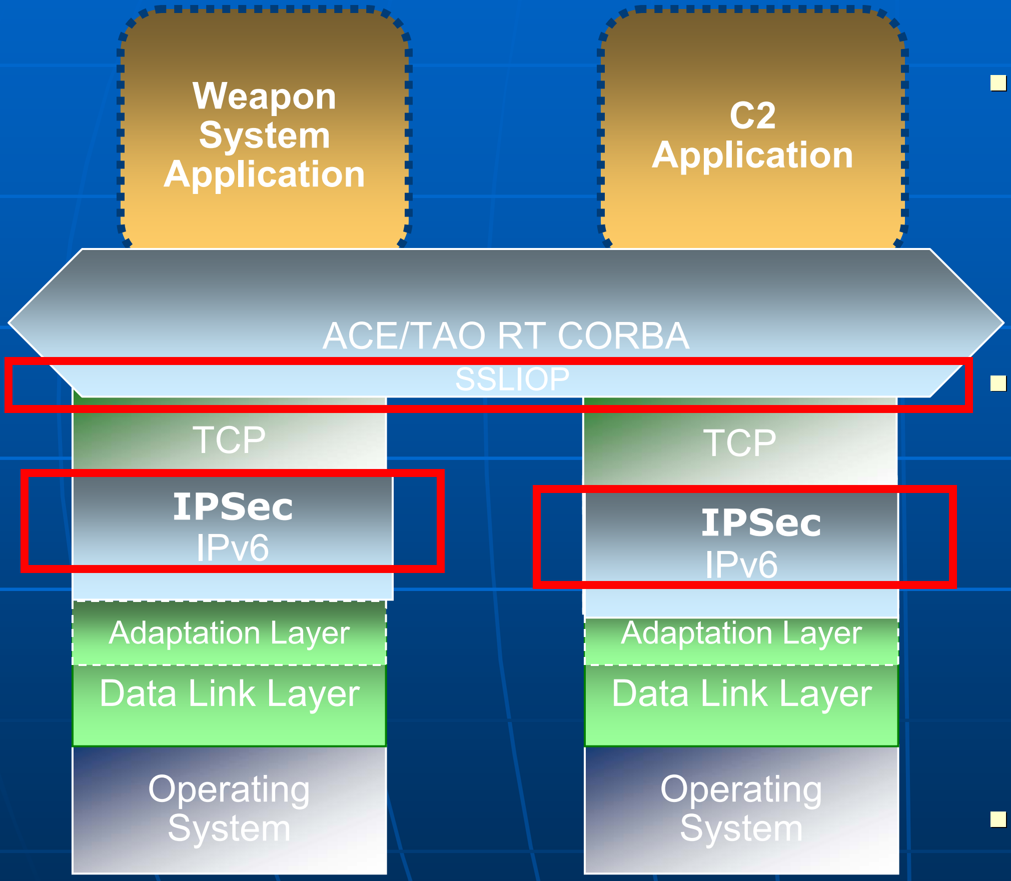
What Are the Threats?

Raytheon

- Spoofing
  - The messages are not coming from or being received by the authorized C2 officer or application
  - The messages are not being received by or coming from the authorized tactical platform, application, or officer
- Sniffing/Traffic Analysis
  - Some unauthorized platform, object, or individual is reading the transmissions or analyzing the message traffic
- Denial of Service
  - Flooding - Extra messages are sent to the tactical platform, overloading its processors
  - Hijacking - A required communication service is hijacked and taken down, preventing its availability
- Replay
  - Messages are captured and resent to delay systems or provide them with invalid/outdated information
- Redirection/Tampering
  - Messages are captured and sent to an unauthorized destination, while dummy messages are sent to satisfy the source and destination

IPSec and CORBA/SSLIOP Demonstration Results

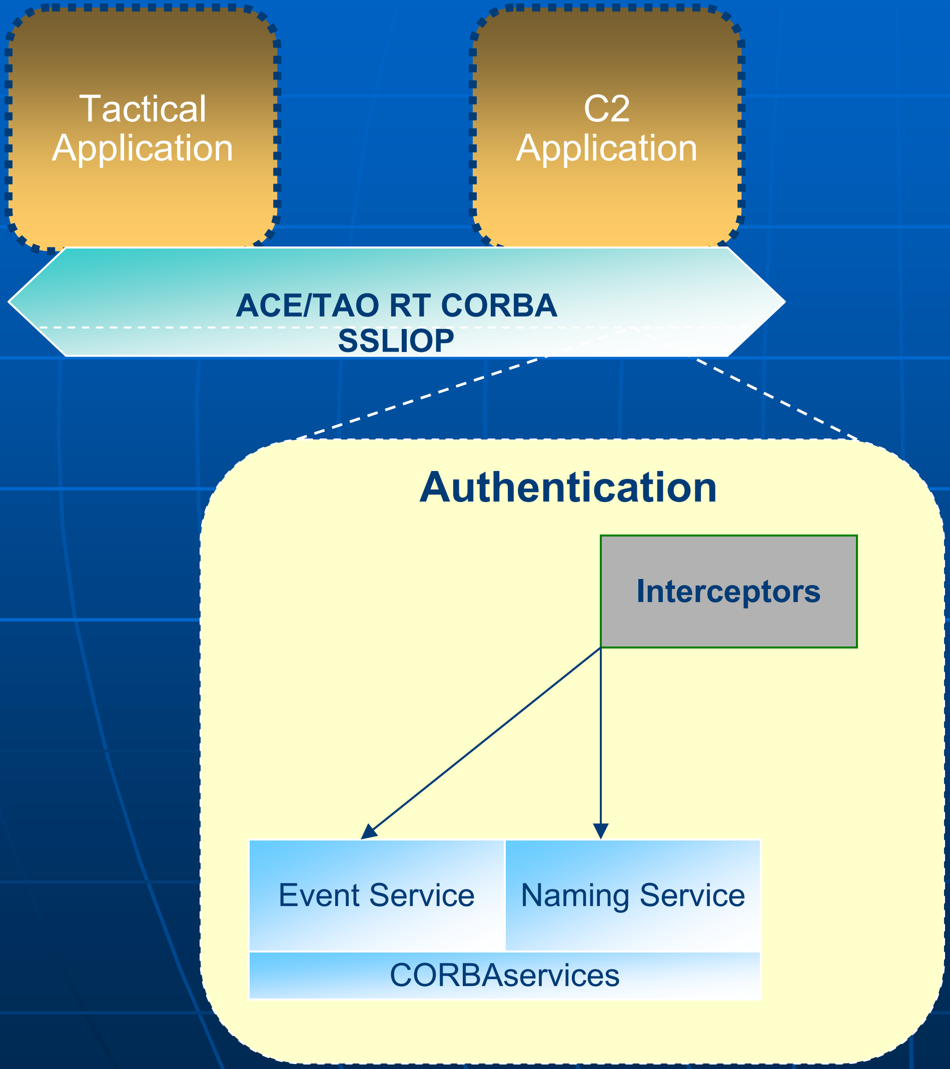
Raytheon



- **IPSec suite with IPv6 provides protection against**
  - **Sniffing/Traffic Analysis**
  - **Spoofing, redirect, replay**
  - **DOS by Flooding**
    - ***Not 100% successful***
- **Secure Socket Layer (SSL) over CORBA's Internet Interoperable Protocol (IIOP) protects against middleware "Over-the-Wire" vulnerabilities**
  - Added ***confidentiality***
  - Limited ***authentication***
  - Transmission ***integrity***
- **SSLIOP does not protect against some CORBA-specific platform-level attacks**
  - E.G., DOS resulting from the hijacking of CORBA services

Raytheon

Portable Interceptors Protect CORBA Services



- SSLIOP cannot be used to secure the Event and Naming Services
- Portable Interceptors can be used as part of a non-bypassable authentication and authorization mechanism
- Interceptors are activated when the Naming Service is invoked for registration or object name linking
- Interceptors activate CORBA security services (CSIv2) to check validity of request
- The approach is being coordinated with ongoing security enhancements to the open source ACE/TAO RT/CORBA ORB
- Initial demonstrations were successful
- Further work is needed to integrate Interceptor approach with CSIv2.

Threats Countered with EISA Security Architecture

Threat		CORBA	CORBA w/ SSLIOP	CORBA w/ Interceptors Architecture	CORBA w/ SSLIOP & Interceptors Arch.	IPv6	IPSec w/ IPv6	CORBA w/ IPSec, IPv6, SSLIOP & Interceptors
Sniffing								
	Sniffing message payload		X		X		X	X
	Traffic Analysis		X		X		X	X
Spoofing								
	Spoofing packets		X		X		X	X
	Spoofing CORBA object ID			X	X	N/A	N/A	X
Denial of Service								
	Flooding						X	X
	Naming Service hijack/takedown			X	X	N/A	N/A	X
Replay								
	Replay messages						X	X
Redirect								
	Redirect network traffic						X	X
	Naming Service Hijack/Redirect			X	X	N/A	N/A	X

AF Joint Battlespace Infosphere

Raytheon

- Repository of all electronic data
  - Historic data
  - Real-time data feeds from intelligence and surveillance systems
    - Theater and national assets
- C2 and tactical systems are considered nodes (IP addresses) in a Wide Area Network
  - Can be a server of raw data (from onboard sensors)
  - Can be client of other information servers
- Data can be accessed, searched, and manipulated to create new information

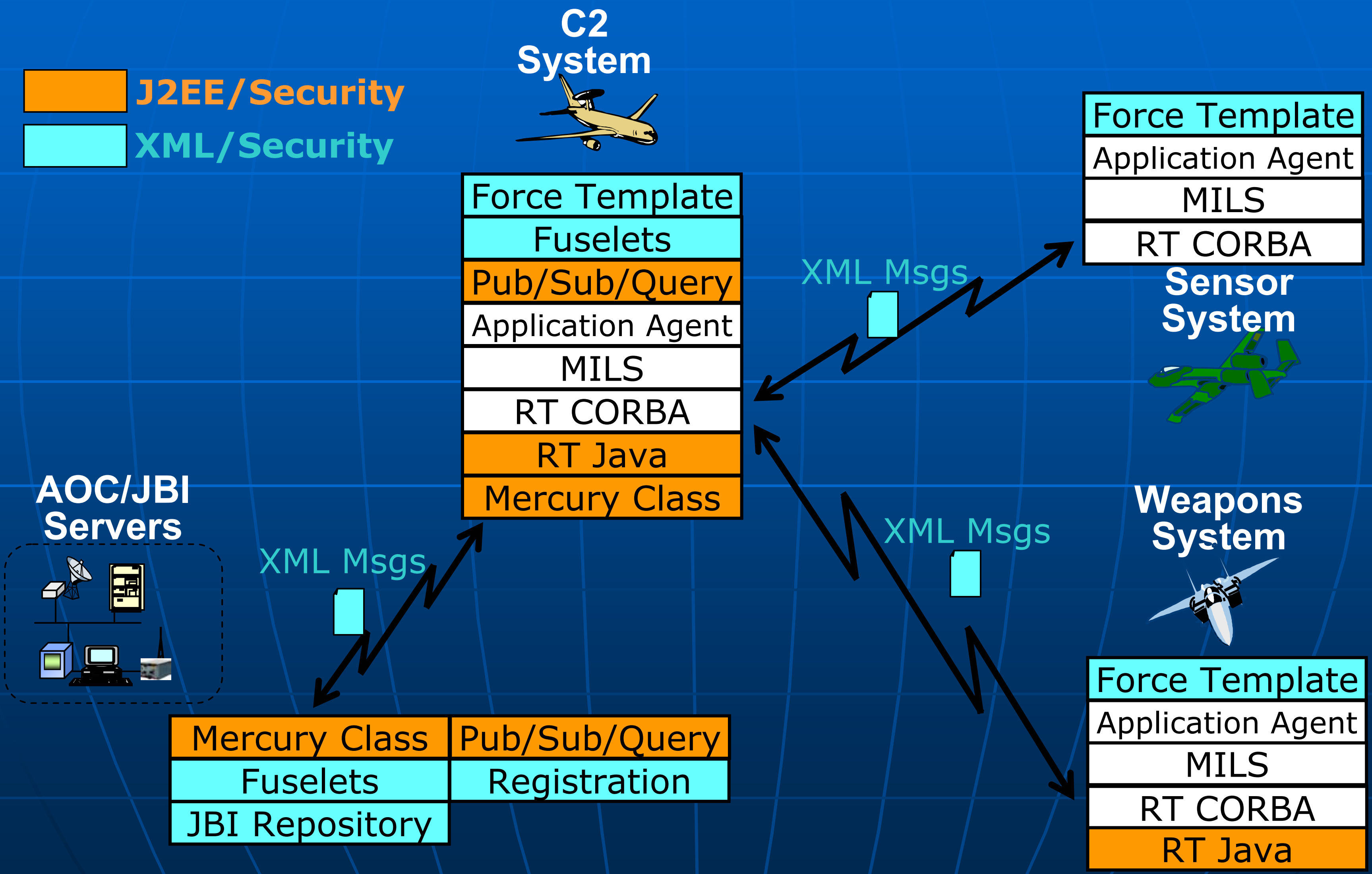
JBI delivers the right information to the right user at the right time *in a secure manner*

Joint Battlespace Infosphere Concepts

Raytheon

- **A JBI is a *System of Systems* that integrates, aggregates, & distributes information**
  - **In the appropriate form**
  - **At the appropriate level of detail**
  - **To users at all echelons**
- **Based on four key concepts**:
  - **Publish, Subscribe, Query**
    - **Publish** information in the JBI
    - **Subscribe** to and receive newly published information from the JBI
    - **Query** and receive previously published information from the JBI
  - **Fuselets**
    - Small, scripted Java programs that transform (filter, refine, fuse) data into knowledge
  - **Force Templates**
    - Use of automated templates to reduce C2 workload
    - Information handshake between the JBI and a combat unit
  - **Distributed Collaboration**
    - Distributed collaboration through shared, updateable knowledge objects

Conceptual "JBI" Deployment Architecture



🟧 J2EE/Security

🟦 XML/Security

C2 System

Force Template
Fuselets
Pub/Sub/Query
Application Agent
MILS
RT CORBA
RT Java
Mercury Class

Sensor System

Force Template
Application Agent
MILS
RT CORBA

Weapons System

Force Template
Application Agent
MILS
RT CORBA
RT Java

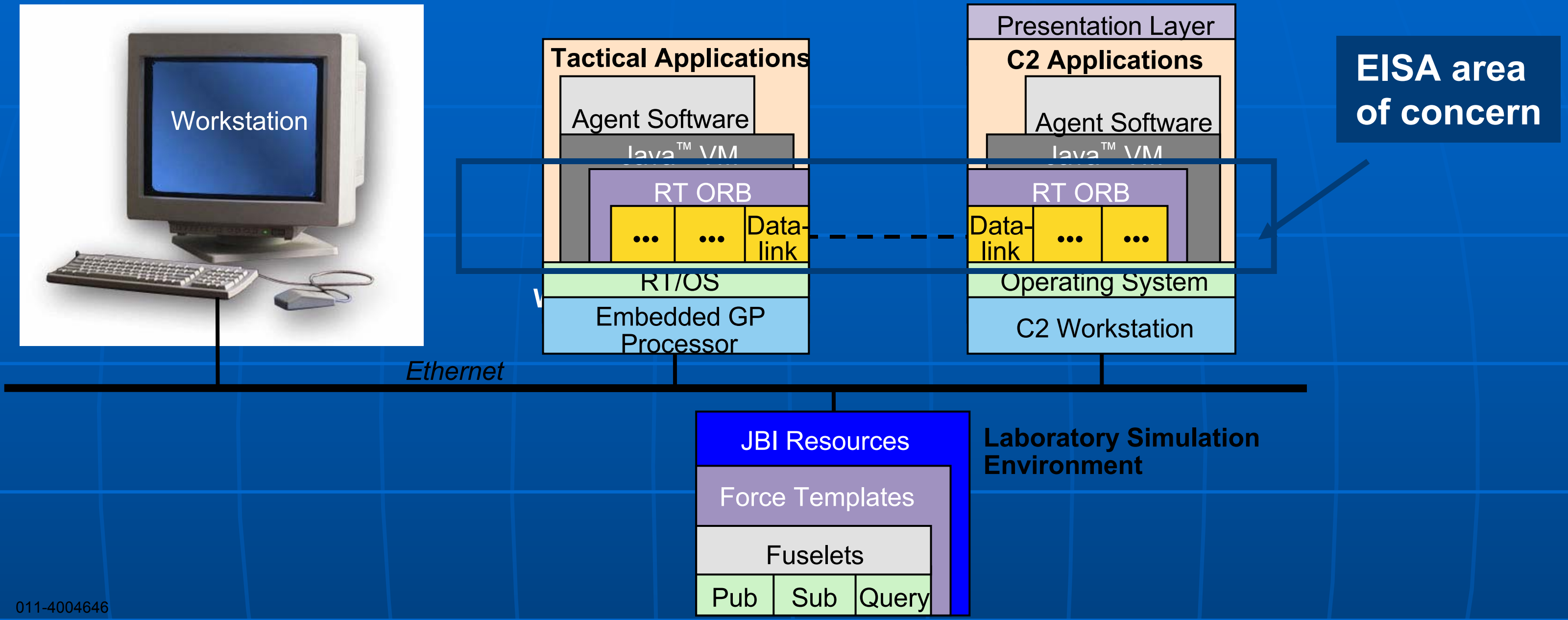
AOC/JBI Servers

Mercury Class	Pub/Sub/Query
Fuselets	Registration
JBI Repository	

Information Assurance Issues in a Deployed JBI

- Java Middleware Security
  - Security implications of Java-based distributed computing mechanisms
    - Authentication of publishers and subscribers
    - Authorization of publishers/subscribers to disseminate/receive information
  - Secure interoperability between Java and CORBA
- Application Agent and Fuselet Security
  - Authentication and authorization
  - MLS Impact
  - Mechanisms for protecting JBI Fuselet engines
- Force Template Security
  - Authentication
- Web Services (XML) Security Standards
  - Evaluate XML-based security standards within the JBI

SIRES Testbed Will Leverage EISA Results and JBI



- EISA considered security at the network stack level and the RT ORB level
- SIRES will consider security for other types of middleware (e.g., J2EE) and for other technologies that are being inserted into platforms to enable interoperability
- Examples of technologies for interoperability that have security impacts include the Java VM, JBI services, and Agent applications.
- IA technologies will be inserted into each layer of the test bed architecture to measure their effectiveness and performance impact.

Summary and Conclusions

- The EISA program demonstrated critical security features of network-level and middleware technologies for real-time embedded systems
  - IPv6, IPSec, CORBA SSLIOP, CORBA Portable Interceptors
- The EISA demonstrations have shown that secure communications can be achieved for real-time embedded systems using commercially available technologies
- The SIRES program is extending the EISA security architecture to advanced research needed to secure the DoD vision of the Global Information Grid and the AF Joint Battlespace Infosphere
- SIRES is investigating the emerging Multiple Independent Layers of Security (MILS) technology
  - Demonstrate its applicability to more affordably meet MLS requirements of C2 and tactical platforms with COTS products
  - Advance both intra-platform and inter-platform data separation at EAL 7 level