12th International Command and Control Research and Technology Symposium

"Adapting C2 to the 21st Century"

The U.S. Air Force Technical Implementation Architecture (TIA)

Point of Contact: Scott Foote

Scott Foote
The MITRE Corporation
202 Burlington Road MS 1624R
Bedford, MA 01730-1420
781-377-6856
scottfoote@mitre.org

Jay Scarano
The MITRE Corporation
202 Burlington Road MS 1624R
Bedford, MA 01730-1420
781-377-7240
jgs@mitre.org

Steve Foote
The MITRE Corporation
202 Burlington Road MS 1624R
Bedford, MA 01730-1420
781-377-4566
sfoote@mitre.org

Ray Modeen
The MITRE Corporation
202 Burlington Road MS 1614
Bedford, MA 01730-1420
781-266-9730
modeen@mitre.org

Abstract

This paper provides an introduction to the Air Force's Technical Implementation Architecture (TIA) effort. The TIA is an initiative to promote the convergence of computing infrastructure for Air Force (AF) Command and Control (C2) information systems.

The TIA is a collaborative effort across several Air Force organizations: the Air Force Electronic Systems Center (ESC); Air Force CIO (SAF/XC); Air Force Command, Control, Intelligence, Surveillance, Reconnaissance Center (AFC2ISRC), Air Mobility Command (AMC), Air Force Space Command (AFSPACE), Air Force Research Labs (AFRL) and other stakeholders.

Genesis

The Department of Defense is a very large, complex, adaptive system. The Air Force (AF) is attempting to integrate its Command and control (C2) Systems into this evolving environment. To varying extents, each AF C2 system is implementing contemporary information system architecture.

There was a perception that C2 systems were diverging in their respective evolution due to different architectural artwork and competing computing infrastructures. In response to this situation, the C2 General Officer Steering Group (GOSG) issued a task to establish a common architecture and governance construct to address the perceived divergence.

An Air Force-wide, cross functional focus team was established to develop a solution.

Evolving the AF Enterprise

The Air Force is attempting to integrate its many individual programs and systems into a comprehensive enterprise.

More and more frequently, the concept of the "*system*" refers to a "*system of systems*" or more accurately a "*community of applications*" that are increasingly more "integrated" through shared infrastructure. This begs an ability to leverage the industry-wide trend toward separation of infrastructure and application.

TIA continues to promote the separation of applications and infrastructure – started by the C2 Enterprise Technical Reference Architecture (C2ERA) and continued by the Net-Centric Enterprise Solutions for Interoperability (NESI.)

The TIA initiative is focused on promoting convergence around infrastructure decisions made by Air Force programs; specifically those programs building C2 Systems or procuring infrastructure components.

The Technical Implementation Architecture ("TIA")

Overview

The TIA was endorsed by the Air Force C2 GOSG on 7 November 2006.

The TIA objectives are to:

- Ensure consistency across C2 program acquisitions;
- Provide pre-qualified software infrastructure products for the Air Force enterprise;
- Provide a framework for identifying enterprise-driven specific solutions, when standards are insufficient or immature, but the enterprise needs a capability; and
- Provide a governance and management construct to efficiently and effectively evolve critical enterprise infrastructure.

The Four Pillars of TIA

I. Interoperability Specifications and Constraints

The Air Force needs to ensure consistency across C2 program acquisitions. The TIA proposes a multi-faceted approach to accomplish this. First, we developed an abstract reference model (or "blueprint") to be used by all C2 systems to articulate a modular, layered architecture and the fundamental enterprise constraints required to manage and secure their components as they evolve independently. Second, using that model we laid out the functionality we expect to be provided by infrastructure software vendors allowing them to map their product offerings to the enterprise needs. Third, we are developing enterprise level contract language in the form of a templated technical requirements document (TRD) to be used by Air Force acquisition programs to establish consistency across the infrastructure they procure and build upon.

Figure 1 illustrates the TIA general blueprint, or model of a modern information system. This model has two intended purposes. First, it is intended for use by program engineers to define the boundaries between application-specific objects that should be built/developed and supporting infrastructure that should be bought or provided by an integrator (or the enterprise.) Second, it is a reference used to bin functionality, standards, and solutions for all TIA-related activity.

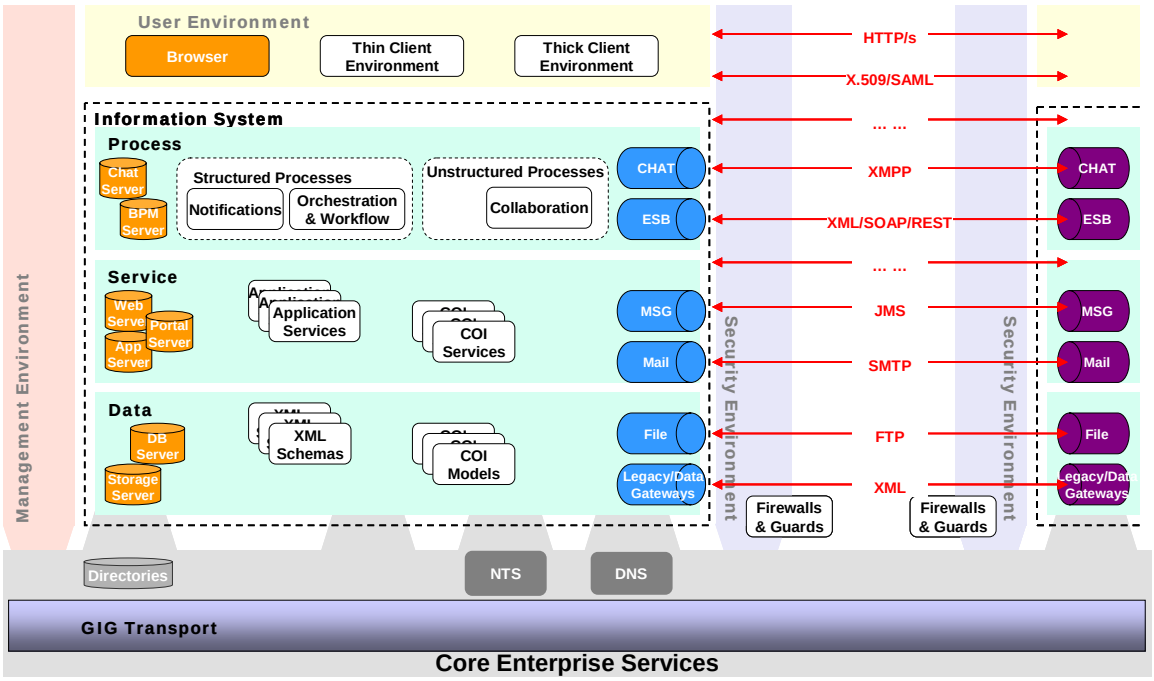

Figure 1: The TIA "Blueprint"

Application-Specific Objects: Data, Service, Process, Thin and Thick Clients

Applications provide specific functionality desired by a community of interest or customer for which an information system is being acquired. The application-specific parts of TIA are described below. The intent is that information system builders are to produce these objects and rely on infrastructure bought or provided by others. In the TIA model, application-specific functionality is color-coded white.

Data Objects: Information describing business entities is organized into data objects. These data objects are typically stored persistently by infrastructure; for example, as files on a file server, or as more complex data objects within a database. These data objects are described by XML schemas and Community of Interest (COI) information models, also stored by the infrastructure.

Service (or Software) Objects: Most software written today is highly modular in nature, allowing greater flexibility in how software objects can be used together, increasingly accessed as web services. These software objects are typically stored persistently, and executed dynamically, by infrastructure; for example, as "pages" of script in a browser or on a web server, or as more complex software objects within an application server or servlet engine.

Process Objects: All information systems enable businesses by arranging software and data objects into workflow patterns that support actual business processes. Increasingly, these workflow patterns are no longer being statically defined within compiled application code; but instead are being dynamically configured, and persistently stored, using workflow or

orchestration infrastructure components that generally perform business process management (BPM).

Thin and Thick Client Objects: Thin clients are application components that execute completely within a web browser (e.g., HTML pages, JavaScript, JSP, etc). Thick clients are software components that are fully resident on an end-user's desktop machines, and do not require a web browser.

Infrastructure Components: "Containers", "Pipes", "Guardrails" and Transport

Fundamentally, the TIA initiative describes two general types of infrastructure components using the simplistic terms "*containers*" and "*pipes.*" Constraints are described using the term "*guardrails*." "*Transport*" is the term used to describe physical communications medium and protocols.

Transport Component: Information is ultimately shared via some means of physical communication. TIA assumes transport to be implemented via a TCP/IP backbone. In the TIA model, transport is labeled GIG Transport and color-coded blue.

Guardrail Components: Guardrails define enterprise constraints or provide risk mitigators. They apply to security, system performance and consistency of presentation. These controls are placed upon all information system components. In the TIA model, the guardrails are labeled Management Environment, Security Environment and User Environment, and are color-coded pink, blue and yellow, respectively.

The guardrails may be implemented two ways. First, guardrails may be rules (or standards) governing software development and deployment. Second, guardrails may be enforced by containers and services that must be accessed by the information system – providing consistent behavior across an enterprise.

Pipe Components: The term pipe refers to all aspects of a communications channel established between infrastructure containers, or more specifically between the objects within these containers. The primary function of a communication pipe is to define how to move data. Examples of pipes include: legacy gateways for moving data between applications, SMTP connections for moving email messages, message-oriented-middleware (MOM) for moving messages between systems, HTTP connections for moving web pages or XML objects, etc.

Container Components: Infrastructure containers are components whose function is to provide storage, management and execution of data and software. Examples of containers include: file servers, database servers, metadata registries, application servers, web servers, service registries, business process management servers, and directories of user identities.

Containers may be local or global in nature. The scope of ownership is determined by the nature of the data in the container. The criteria for global ownership are discussed in the Global Containers section.

In the TIA model, the containers are labeled as various servers and are color-coded orange. The exceptions to the labeling and color-coding are the enterprise (or global) containers ("directories", Network Time Service (NTS) and Domain Name System (DNS)) – colored various shades of gray.

Global Containers: These are enterprise services that are shared by all systems and are the building blocks upon which other services are based. The following criteria should be used to identify Global Containers or services[1]:

- Is this a common utility ("service") essential for enabling operational capability across the Enterprise?
- Is Enterprise control of the service required to ensure successful implementation?
- Does the service scale to support the Enterprise?
- Is Enterprise content, consistency, or connection required? That is, must the service content be complete, does the service behavior need to be the same every time it's accessed, or will the service be required to accept connections from across the enterprise?
- Is a single service specification possible (or practical)?

The set of attributes that we believe should be common to all enterprise services is:

- Usable by all systems and nodes (with development tool support);
- Available across the enterprise (millions of users in diverse locations);
- Accessible via a single service specification (A least common denominator interface available to all users);
- Well defined quality of service measures (e.g., reliability, performance);
- Well managed (24x365 support, worldwide); and
- Potential for multiple service/business models. (Few, if any, enterprise services are provided by a single organization.)

The implications of these attributes are that Global Containers are constrained to those services which provide capabilities to most, if not all, systems participating in the enterprise. Accordingly, the services must be ubiquitous and will utilize a variety of deployment, operations and management models. As enterprise services will be used by a wide variety of applications – most unknown to the provider – the service must be highly available with published service levels and around-the-clock support.

---

[1] *Leveraging the Air Force Enterprise Approach to Time Synchronization: A Proposal* – Glenn Bell, Jay Scarano, The MITRE Corporation

II. "Short List" of Infrastructure Products on the "Shelf"

As part of the TIA, the Air Force must provide and manage a set of commercial vendor-integrated computing infrastructure products for the enterprise.

The intent is to provide acquisition Programs of Record (PORs) the ability to choose from a few pre-configured infrastructure software suites that have been pre-assessed for critical technical interoperability criteria. The Air Force must also have an environment enabling the successful support of our POR customers and technology evolution as the products are embraced and get updated over time.

This Air Force environment must include software test harnesses, enterprise technical interoperability criteria, configuration management processes, and relevant documentation.

The Air Force must ensure that each vendor suite is tested against a common set of interoperability criteria. The test harnesses must be designed to support the addition of suites from new vendors and enable regression testing as patches and modifications are made to the existing inventory. Ultimately, all permutations of the products, underlying operating systems and associated updates/patches could be tested. The near-term focus will be on the products and operating systems in use, and anticipated for use, by our AF C2 systems.

III. Enterprise-driven Specific Solutions

The TIA provides a framework for identifying when enterprise-driven specific requirements exist, and where relevant industry standards are insufficient or immature. The framework includes ongoing identification and demonstration of products and/or custom technologies that uniquely meet these specific demands. This may include documenting specific configurations, protocols, standards and solutions required for components within the enterprise to interoperate.

Complex environments present a number of issues. The TIA has selected the following high priority categories of issues to address:

- The use and integration of various types of Metadata across the enterprise;
- Integrated security (information assurance), focused initially on Identity Management/Authentication across the enterprise; and
- Enterprise-scale technical interoperability, focused on connectivity enabled through message-oriented middleware.

The cross-functional TIA Focus Team has established a number of sub-groups to investigate these areas:

- Integrated Metadata Environment
- Identity Management/Authentication
- ESB Federation

The Integrated Metadata Environment sub-group is focused on existing metadata and related program-specific technologies in an effort to bring them together into a single, comprehensive metadata environment for the enterprise.

The Identity Management/Authentication sub-group is investigating existing information security technologies and methodologies across C2 and Combat Support systems. The objective is to identify and propose an enterprise-wide strategy for Identity Management and Authentication that meets a broad spectrum of access management requirements.

The ESB sub-group is determining what communication mechanisms and software suites the programs of records are using today. Their goal is to identify a set of enterprise-relevant best practices based on specific patterns of communication employed and enterprise interoperability criteria applicable to vendor offerings.

IV. Governance & Management

The TIA also aims to provide a governance and management construct to efficiently and effectively guide the evolution of critical enterprise infrastructure and its adoption. The objective is to manage critical enterprise decisions and tradeoffs. These tradeoffs must address a balance between innovation flexibility leading to complexity and the strict manageability required to maintain a robust, reliable enterprise often directed by rigid integration policies.

Summary – Enterprise Convergence

Enterprise systems (or “systems of systems”) require a balanced approach to design and implementation. The balance is between the flexibility and agile evolution that "open" architectures promise, and the management requirements introduced by the complexities that such an approach permits.

Enterprise engineering efforts such as the Air Force’s TIA are intended to define contractual language for acquisitions, provide products as a basis for development and integration, work through complex enterprise technical issues, and mature the overall approach to acquiring enterprise systems.