C4ISR Architectural Frameworks in Coalition Environments

Charles R. Myer, Lt. Gen. (rtd) U.S. Army
Unisys Corporation
8008 Westpark Drive
McLean, Virginia 22102
(703) 556-5007
cbobmyer@aol.com

Abstract

The break-up of the Soviet Union unleashed a flood of nationalism throughout Southeastern Europe (SEE). Freed from the yoke of suppression, the nations of the region sought economic stability and security in a dramatically changing global environment. These nations are anxious to display Western leanings and to ensure national security through multinational regional coalitions. These coalitions, in turn, are being supported by a variety of national, NATO, and U.S. sponsored initiatives with the common goal of regional stability. Within the regions of the Pacific Rim, similar coalitions may emerge with similar goals to which the principles set forth in this paper will equally apply.

The common thread through these SEE initiatives is the use of Information Technology (IT) to improve Command, Control, and Communications (C3) in a combined military/peace support domain. This paper proposes an IT-driven Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architectural Framework approach to the integration of combat and peace support forces in regional coalition initiatives. Although the framework is applicable across the total C4ISR domain, only Command, Control, and Communications are relevant to the subject addressed in this paper and will be the term used throughout. Computers are assumed as a logical part of C3.

This paper also proposes that this type of architectural approach is applicable to regional coalitions on a global basis.

The Coalition Environment

(Solomon, The NATO Enlargement Debate, 1990-1997, 1998, The Washington Papers1l 74, Praeger, London, England).

For nearly a decade following the break-up of the Soviet Union, the newly freed nations of SEE directed their energies internally. Military reform, political instability, economic upheaval, and severe budgetary constraints and re-directions were but a few of the crises that were ultimately abated through newly adopted democratic processes. Concurrently, the stirrings of "coalition" had begun as the need for regional stability grew stronger.

The origin of SEE coalitions date back to 1990 when NATO first extended "a hand of friendship'' to all ex-Warsaw Pact States. Within a year, NATO endorsed the establishment of the North Atlantic Cooperation Council (NACC). The NACC charter was "to commence planning with liaison countries on disaster relief and refugee programs and other security challenges in Europe." Two years later (in 1993), a U.S. Office of the Secretary of Defense (OSD) Policy Paper was approved by the NACC and endorsed by NATO. The term "Partnership for Peace (PFP)" emerged from that paper. Shortly thereafter, the U.S. Secretary of Defense—Les Aspin—publicly described the 5 "big advantages" of the PFP for both allies and partners:

1) The PFP does not re-divide Europe.

2) The PFP sets up the right incentives. In the new post-Cold War world, NATO can be an alliance based on shared values of democracy and the free market. The PFP rewards those that move in that direction.

3) The PFP requires that partners make a real contribution. Security consultations with NATO, for instance, are offered only to States that are serious about playing the game.

4) The PFP keeps NATO in the center of European security concerns and, thereby, keeps American involvement at the center of Europe.

5) The PFP puts the question of NATO partnership for partners where it belongs, at the end of the process rather than at the beginning. (Another way of saying partners must first pull their own load for partnerships to solidify.)

From this beginning, the PFP has become the foundation for nearly all coalition efforts that have evolved within the SEE nations.

The Coalition Initiatives

The key PFP coalition initiatives that emerged from this origin, and on which this paper is based, are discussed below:

The PFP Information Management System (PIMS): PIMS was initiated with U.S. funding, and it has received continued U.S. support. Also, PIMS provides a LAN-based host infrastructure and broadband satellite-based network access to each PFP nation that has elected to participate in the PIMS Program. A typical PIMS network is shown in Figure 1.

The various PIMS national hosts (e.g., Bulgaria) are linked with each other and with NATO/U.S. PIMS support Agencies via the Internet or E-mail. Connectivity is provided by 2-way VSAT or FDDI cable. PIMS support nodes are shown in Figure 1. As a part of the PIMS Program, each PFP host nation is partnered with a U.S. National Guard Unit located in 1 of the U.S. States. Each partnered Guard Unit also has a PIMS LAN. This linkage provides the coordination, exchange, and collaboration of information covering a variety of global peace support applications resident on PIMS host servers. PIMS unclassified information exchange includes collaborative operational and planning data that are relative to peace support actions.

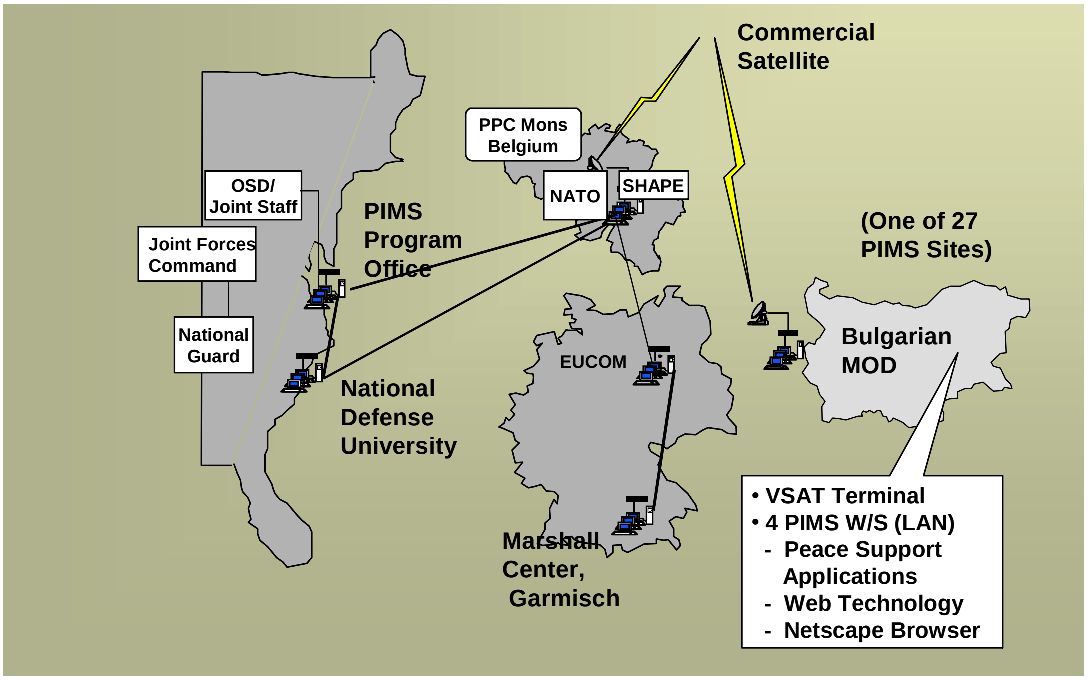

Figure 1. PIMS Hosts and Network Connectivity

The SEE Defense Ministers (SEDM): The Ministers of Defense of 9 nations (Albania, Bulgaria, The Former Yugoslavian Republic of Macedonia (FYROM), Greece, Italy, Romania, Slovenia, Turkey, and the United States) signed an agreement to establish the SEE Defense Ministers (SEDM). The SEDM engenders cooperation and dialog among the countries of SEE to foster regional security, stability, and good neighborly relations. The SEDM has generated numerous internal PFP-based regional initiatives through periodic Plenary Sessions. Through these sessions, the SEDM is rapidly extending PFP interest, enthusiasm, and regional cooperation throughout Southeastern Europe. The more significant of these initiatives are as follows:

- On September 26, 1998, 7 of the SEDM nations (Bulgaria, Romania, FYROM, Italy, Albania, Turkey, and Greece) agreed to participate in the activation, manning, and support of a Multinational Peace Force South-Eastern Europe. The initial force is a Brigade. The mission of the Brigade, named the SEE Brigade (SEEBRIG), is to contribute to regional security and stability in the Euro-Atlantic area and to foster cooperation among SEE countries. Slovenia and the United States are only SEDM observer nations, but they have expressed their full support and determination to contribute. The SEEBRIG domain is shown in Figure 2.

  The SEEBRIG has been activated in Plovdiv Bulgaria in a new military compound provided by the Bulgarian Government. Currently, military personnel from all 7 participating nations man the SEEBRIG. The first SEEBRIG commander, with a tenure of 1 year, is a Turkish Brigadier General.

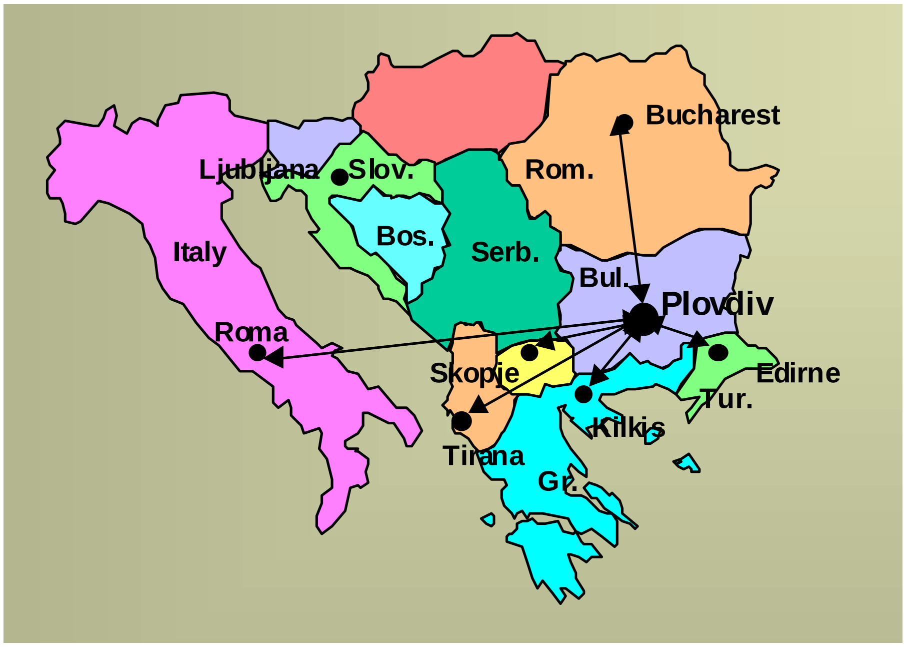

Figure 2. The SEEBRIG Domain

- In June 1999, the SEDM launched a construction engineering initiative to aid Kosovo post-conflict reconstruction. The initiative establishes an Engineer Task Force to respond to construction-oriented humanitarian and infrastructure challenges. The effort will, in the long-term, evolve into an SEE Construction Brigade (SEECONBRIG) to complement the SEEBRIG cited above.

- At the same SEDM Summit, an initiative was launched to create a Crisis Information Network (CIN) by expanding the reach of PIMS. This expansion would include enhanced W/S and server capability, satellite bandwidth, crisis management functionality, or other upgrades to meet new crisis management requirements. Video Teleconferencing, C2 systems (heretofore excluded from PIMS), digital libraries, and modeling and simulation commercial-off-the-shelf (COTS) products are candidates. To date, firm requirements for the CIN have not been defined. *(South East Europe Crisis Information Website, ASD Kramer Proposal, http:l!server.pims. org/Desktop/Topics/CivilEmerg/sedm/Kramer brief ht).*

The following U.S. sponsored coalition initiatives are also in the planning stage. Though currently outside the SEDM charter, they will impact SEDM goals and objectives.

- An initiative undertaken by the U.S. DoD to develop a Civil/Military Emergency Planning (CMEP) capability to be offered to all PFP nations, to include those in the SEDM.

- A Global Disaster Information Network (GDIN) as a means of exchanging information between CMEP sites. Currently, the security classification of the GDIN is undecided.

The Issues of IT/C2 and Common Enterprise Architectures

When addressing regional coalitions such as PFP/SEDM, Command and Control (C2) assumes a broader significance than its more traditional combat support role. Accelerating advances in IT provide the means of enhancing C2 in both the military and civil domains for peace support. Information Dominance, Information Operations, and Information Assurance are terms that confirm the pervasiveness of IT in this broader context. IT enhances National Security C2 through improved Information Dominance over hostile forces. IT enhances Peace Support through improved Information Operations to empower both law enforcement/disaster relief agencies and wartime military forces. IT enhances information assurance by denying unauthorized access to IT terminals and IT networks, as well as protecting the terminals and networks themselves. IT processes, in one form or another, provide C2 Command and Operations Nodes and Centers with a common operational picture, a complete awareness of the situation, and the ability to collaboratively plan and implement the military or civil response. The leader's staff, whatever the mission, can truly execute operations through the science of "control," and the leader can truly influence operations through the art of "Command."

Unity of effort among coalition partners, however, is not possible if the initiatives are discordant. A common architectural thread, woven through these diverse coalition efforts, offers the best means to bring accord, thus avoiding duplication of effort, fragmentation of resources, and development of diverse technical standards.

An Enterprise Architectural Approach Defined

The U.S. DoD, over the past decade, has developed costly C3 systems without an architectural foundation. The resulting C3 systems have often failed to meet user requirements, been interconnected over inadequate communications systems, and lacked proper security and interoperability in Joint Operations. As a result, the U.S. DoD has mandated that no C3 systems will be proposed by U.S. Joint Warfighting Commanders in Chiefs (Pacific, Atlantic, Europe, Southern Region, etc.) unless the proposed system is firmly based on a C4ISR Architectural Framework. This insistence on development of an Architectural Framework before funding approval is slowly gaining global acceptance. This paper proposes this C4ISR Architectural Framework as the best way to integrate SEDM/PFP regional coalition C3 initiatives. The Framework is shown in Figure 3.

The Framework, like a gear train, develops 3 distinct—but coupled—architectures:

1) A Technical Architecture (TA) that defines current and emerging C4ISR standards for both requirements development and systems design. The standards are analogous to a blueprint for a house.

2) An Operational Architecture (OA) that defines C4ISR requirements, the resulting data flows between command nodes and the network connectivity needed to transmit and receive the defined data flows. The Operational Architecture is analogous to building blocks for a house.

3) A Systems Architecture (SA) that defines the technical parameters of hardware and software components needed to satisfy the OA. The SA is analogous to furnishing a house.

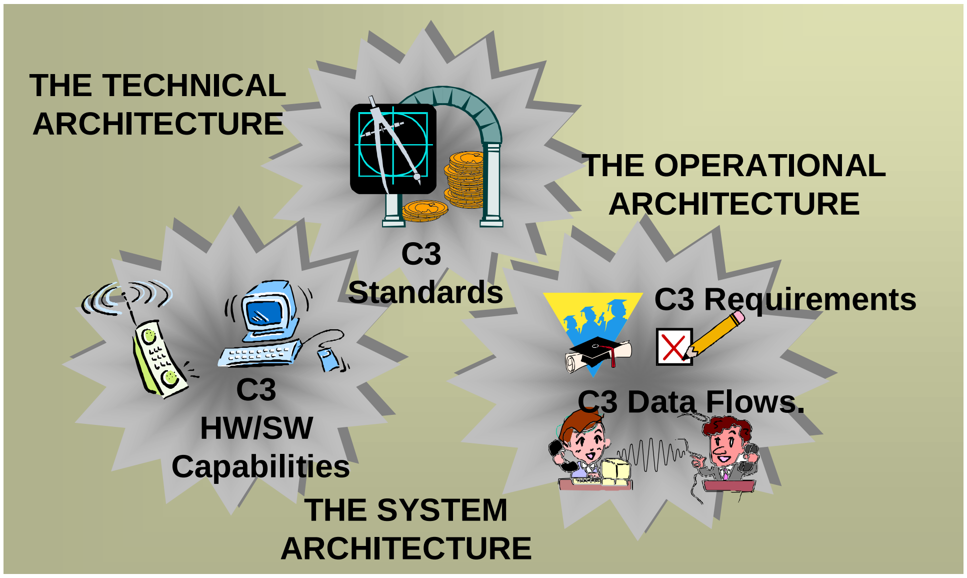

Figure 3. The C4ISR Architectural Framework.

The C4ISR Framework (*DOD Architectural Working Group , C4ISR Architecture Framework Version 2.0, 20 August, 1997 and Department of the Army, Army Enterprise Architecture Guidance Document (AEAGD), Version 1.1, 23 December 1998*) defines many products to be developed within the OA and the SA. Only the products applicable to this task are addressed in the following architectural discussion.

Note: The Framework does not identify or purchase hardware or software systems or components. The Framework only defines the parameters that the hardware and software components must possess to meet the stated C3 requirements of the OA. National or coalition-sponsored acquisitions then acquire hardware/software products to satisfy the Framework Architectures.

An Enterprise Architecture Approach Applied

The Environment

How do we apply this architectural methodology to the myriad of PFP-driven coalition initiatives now emerging in SEE? We can look at the challenge as a 3-circle Vinn diagram.

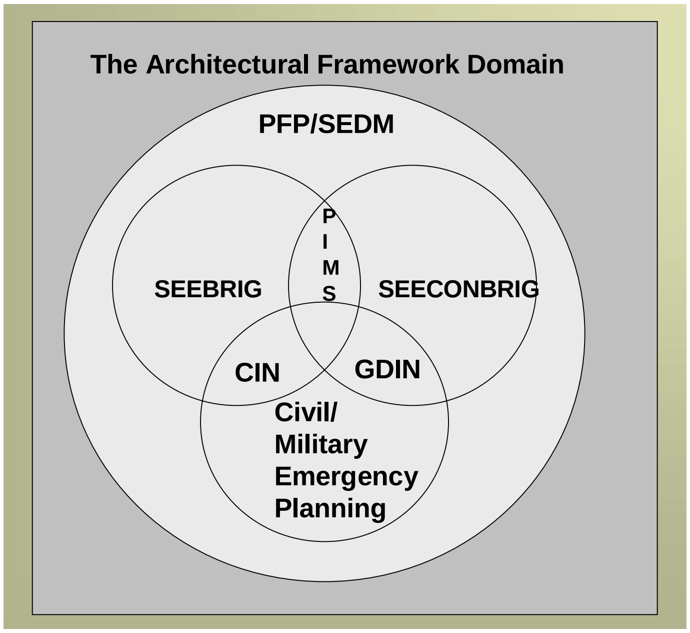

Figure 4. The SEE Coalition Initiative Challenge

Within the Architectural Framework domain, the architectural solution must encompass the 6 cited SEE coalition initiatives generated by PFP/SEDM-sponsored actions. This includes the following:

- Three C2 organizations or systems (SEEBRIG, SEECONBRIG, CMEP). Each will generate C2 data for transport by any of the 3 network initiatives.

- Three communications initiatives (PIMS VSAT, CIN, and GDIN). Each will be networked to meet the C2 requirements of the 3 C2 organizations or systems.

The task is to apply the 3 architectures of the Framework to define the coalition C3 requirements and hardware/software characteristics that will meet the goals and objectives of the PFP/SEDM domain, as described above. Each of the 3 architectures is addressed in relation to that task.

The Technical Architecture

Setting common technical standards through the Technical Architecture is of crucial importance given the number of countries involved in the PFP/SEDM initiatives, all with different legacy C3 systems. The broad scope of potential applicable standards is illustrated in Figure 5.

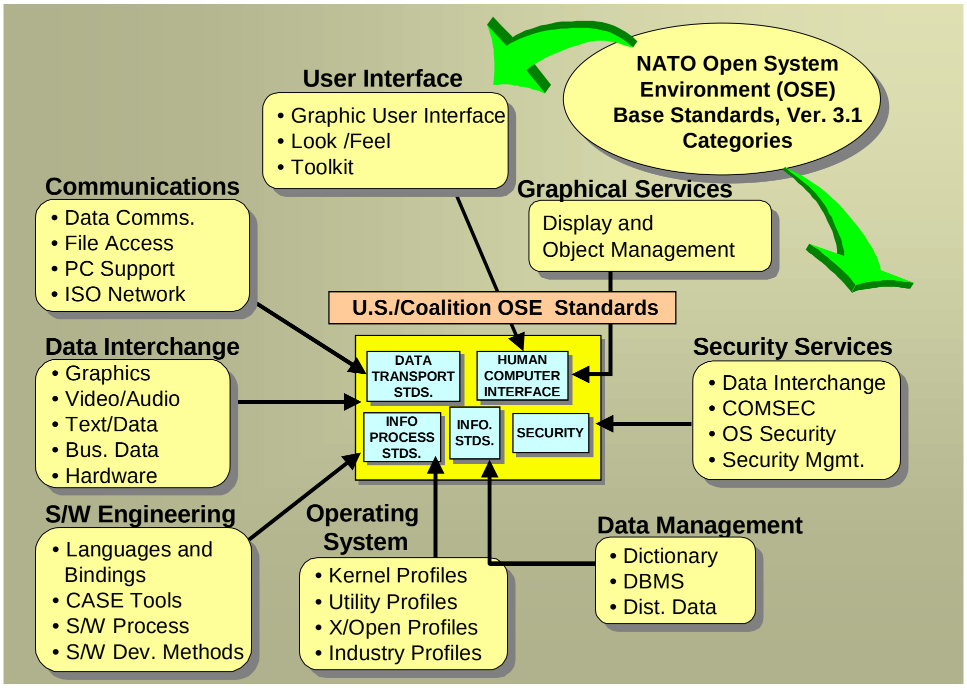

Figure 5. The Technical Architecture Standards Domain

The 8 standards domains, as defined in the NATO Open Systems Environment, Version 3.1, govern all aspects of OA and SA development. The standards come into play, however, mainly in the SA. Global IT industries now recognize the importance of integrating many of these standards in COTS products. The process of winnowing (from this broad standards array) those standards that are germane to the coalition task is thus simplified to a degree. The process of identifying and applying only those standards needed to ensure the success of the architectures is key to the success of the methodology. The initial list of standards selected will, however, be dynamic—changing through additions or deletions as the architectural process progresses. (NATO *Open Systems Environment, Base Standards, Version 3.1, 7 July, 1997).*

The Operational Architecture

Developing the OA for the mix of 6 initiatives, all with multinational interests, seems a daunting task. It is a task somewhat akin to developing the OA for a newly emerging NATO. Conversely, had IT existed at that time and an architectural approach of this type been undertaken, the evolution of NATO may have been a smoother process. This conjecture has no answer, but there is every reason to believe that the Framework, properly applied, could save time and dollars, both precious assets. The key OA products are shown in Figure 6.

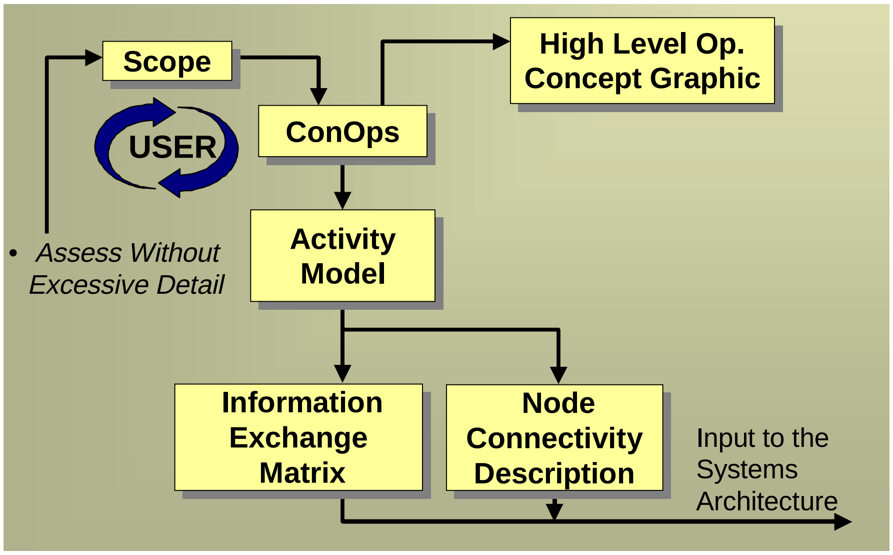
Scope
USER
ConOps
High Level Op. Concept Graphic
Activity Model
• Assess Without Excessive Detail
Information Exchange Matrix
Node Connectivity Description
Input to the Systems Architecture

Figure 6. The Operational Architecture-Key Products

Scope: A key to successful Framework development is to limit the scope of the OA to the minimum consistent with providing adequate products to the SA. Neglecting this simple step has spelled doom for many C4ISR Framework efforts. Defining requirements, data flows, and connectivity to a cumbersome level can result in voluminous, near-useless product inputs to the SA.

Concept of Operations (CONOPS): The true driver of the Operational Architecture is the CONOPS. The CONOPS must be succinct and objective. As a baseline, it should use the 6 crucial factors that U.S. Joint Forces apply in defining user interest in all system development efforts. These 6 factors are briefly addressed below:

1) *Doctrine:* How will the user employ his or her military/crisis forces to perform his or her coalition mission?

2) *Training:* How will the user train his or her people to employ the doctrine?

3) *Leadership:* What principles of leadership development will the user follow to ensure mission accomplishment within the coalition environment?

4) *Organizations:* What organizational concepts will the user follow to support both national goals and coalition missions?

5) *Materiel:* What materiel characteristics (human factors, user unique modes of employment, etc.) apply to fit both national and coalition tasks?

6) *Soldier:* The key factor! What added features apply to make the soldier feel comfortable working in both his or her national and coalition environments?

The Activity Model: The most difficult product of the OA. The Activity Model must, in as little detail as possible, decompose the common coalition C2 functions to the minimum number of tasks considered necessary for NATO/SEDM/PFP Joint Crisis Action. The functions and tasks, once approved, become the functional baseline for the OA. The 3-dimensional matrix, below, portrays a small slice through the Activity Model process.

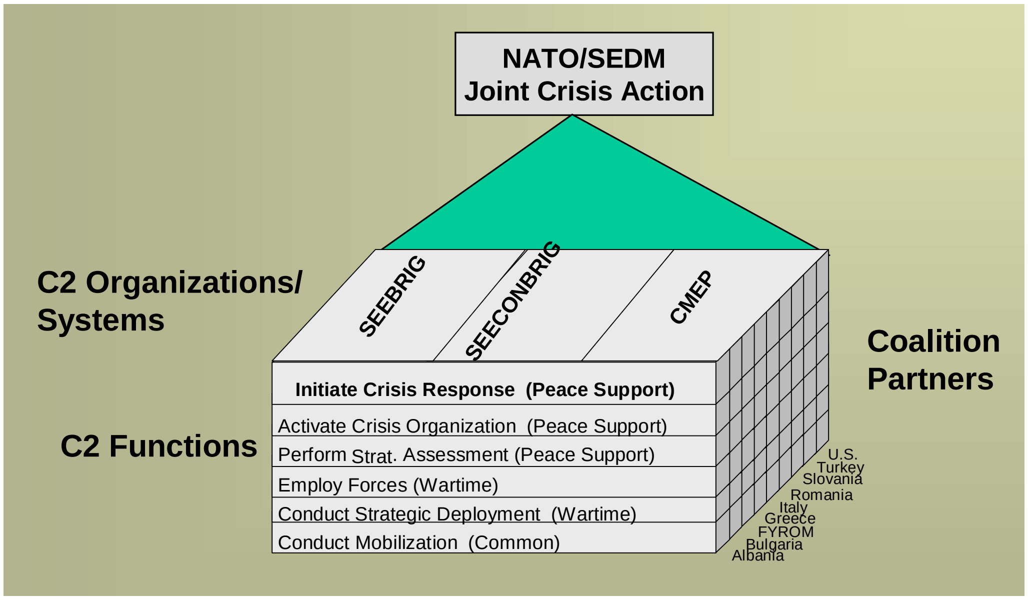
NATO/SEDM
Joint Crisis Action
C2 Organizations/ Systems
SEEBRIG
SEECONBRIG
CMEP
Coalition Partners
C2 Functions
Initiate Crisis Response (Peace Support)
Activate Crisis Organization (Peace Support)
Perform Strat. Assessment (Peace Support)
Employ Forces (Wartime)
Conduct Strategic Deployment (Wartime)
Conduct Mobilization (Common)
U.S.
Turkey
Slovania
Romania
Italy
Greece
FYROM
Bulgaria
Albania

Figure 7. The SEDM Requirements Decomposition Process.

Six sample functions are shown in the slice: 3 Peace Support functions, 2 Wartime functions, and 1 function that is common to both Peace Support and Wartime. The success of the activity Model depends on horizontal coordination between the 3 SEDM C2 entities and the vertical coordination between each C2 entity and the 9 SEDM partners in defining each function and the associated tasks.

Then, the resulting task list determines the information flows between C2 Nodes and the Connectivity Descriptions for the information flows to complete the OA. Examples are shown in Figure 8.

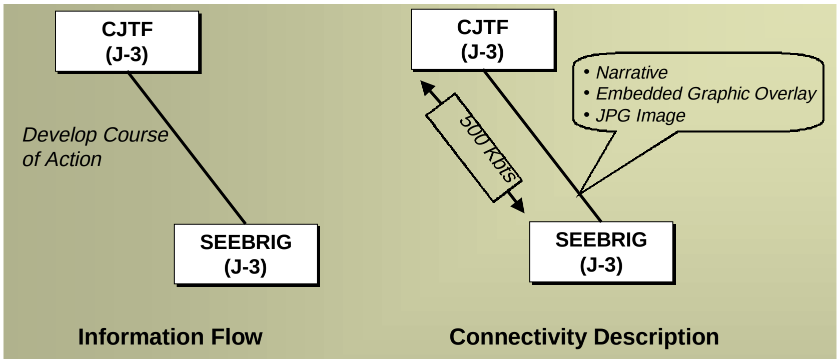

Figure 8. Examples of Information Flow and Connectivity Descriptions

A final point about the OA. The OA does not address hardware, software, or any other material product. The architecture only scopes requirements, information flows, and connectivity. A common failing is to address component development in the OA. This can lead to confusion in developing the SA.

The Systems Architecture

In a normal C4ISR Framework development, the SA defines hardware/software parameters for a civil or military C4ISR system. An example is the U.S. Army development of a fully digitized Corps. Operational and Systems Architectures have either been—or are being—developed for both the Corps and the major sub-elements of the Corps.

In applying the Architectural Framework in a coalition environment the objective is quite different. The objective is not to define new C3 systems to replace national, civil, or combat force legacy systems in each country of the coalition. The objective is to determine a common and agreed-upon set of equipment characteristics and interfaces for both C2 and communications systems that communications systems that are acceptable to the total coalition. The coalition has the responsibility of obtaining the necessary hardware/software components to meet the SA parameters. Each coalition partner, having approved the OA, must, then, through their own means, provide legacy systems that are compatible with the SA design, or they must acquire new hardware/software components that are compatible. The essential products of the Systems Architecture that are consistent with this objective are shown in Figure 9.

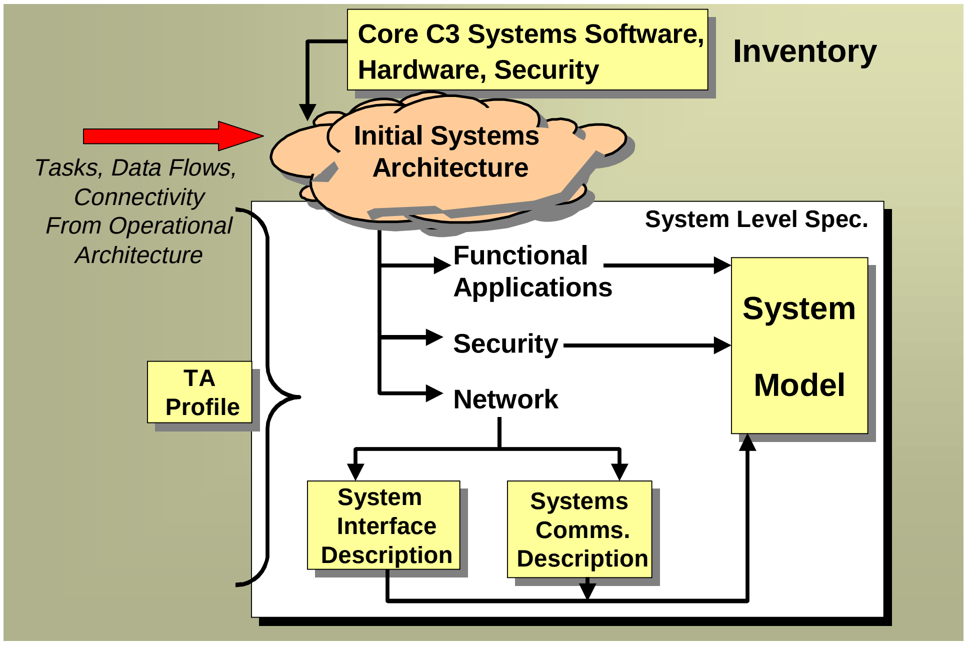
Core C3 Systems Software, Hardware, Security
Inventory
Initial Systems Architecture
Tasks, Data Flows, Connectivity From Operational Architecture
System Level Spec.
Functional Applications
Security
Network
System Model
TA Profile
System Interface Description
Systems Comms. Description

Figure 9. The System Architecture Products

The first product of the SA is an initial C3 Systems Architecture. The OA has defined the information exchanges and connectivity requirements. Based on these OA products, the Core Systems inventory for each coalition partner catalogs national legacy C2 system candidates, irrespective of operating standards, that may meet some of the OA requirements. These national systems set the initial C2 baseline. In like fashion, legacy Wide Area Network (WAN) communications systems, both national and international, are catalogued to set the communications network baseline. Together, the SE C2 and communications systems define the initial C3 architecture. The initial architecture ensures optimum use of all national legacy inventories that may be compatible solutions to the final SA design parameters. The initial architecture also identifies functional, network, and security shortfalls that will drive the development of the subsequent SA products.

The shortfalls of the initial C3 architecture in standards compliance, information exchange, security, and connectivity define the tasks that the remainder of the SA development must address. Standards shortfalls are key because standards drive all of the other SA taskings. The standards shortfalls aid in determining standards entries in the initial version of the SA Technical Architecture Profile. The SA Technical Profile is a dynamic product to which other standards will be added or deleted as the SA proceeds. In addition, the Profile guides the subsequent development of the functional, network, and security sub-architectures as the shortfall tasks derived from the initial architecture are addressed and resolved.

It is beyond the scope of this paper to address the cumulative tasks involved in completing the functional, security and network descriptions of the SA. As a simple example, functional application needs, as defined from the OA and initial architecture shortfalls, may require trade-off analyses of competitive COTS products to determine cost-effective OA compliance characteristics.

As a final step, the applicable C3 systems candidates from the initial architecture, the detailed description of the required functional applications, the security architecture, and the coalition network design parameters are combined in a systems-level specification that will govern national or coalition-wide acquisitions.

Pulling It All Together

Developing an overall C3 architecture for a multinational coalition poses a distinct challenge. Conversely, a failure to accept the challenge invariably leads to C3 products that fall woefully short of objective performance. It is the author’s opinion that a Framework, as defined above, offers the best architectural approach to the defined task. Should the challenge be accepted, some key fundamentals apply:

- Both the initial objective and the scope of the architectural effort must be limited. The objective should be limited to a reachable goal on which later architectural expansions can be built. The scope should be limited to avoid an unmanageable functional decomposition of activities and tasks that is beyond the level required by the SA. Unreasonable operational architectural detail is the primary reason many architectural efforts fail.

- The framework must focus solely on an overarching C3 structure that interfaces with the national partners of the coalition. The architecture must not develop products that impugn the fundamental doctrine, training, leadership, organizational structure, or soldiering culture of any coalition partner.

- The technical standards that comprise the TA Profile of the SA must be minimal. This ensures that the SA system-level specification does not demand standards of limited value that up the price of vendor-provided, compliant products.

- The proposed architecture should be validated through a limited user prototype before any product development. This may add expense and duration to the architectural effort, but it will save time and money in the long run.

A Global View

The PFP/SEDM regional coalition chosen as the example for this paper is by no means unique. Other global regions abound with regional crises and disasters that may prompt similar coalitions with similar goals and similar needs. Regardless of the type or geographic orientation of these coalitions, the architectural processes defined in this paper apply. The value to be derived from this Framework approach is proportional to the speed with which the Framework is approved and implemented by any burgeoning coalition that is similar to PFP/SED. In the early stages of the multinational coalition—minds are flexible, C2 functions are negotiable, and few coalition acquisitions have been started. All too quickly this will change, and the benefits of the Framework will lessen.