Paper ID 004

16th ICCRTS

"Collective C2 in Multinational Civil-Military Operations"

NATO Network Enabled Capability (NNEC) challenges: Why NATO Air Command and Control System (ACCS) might be a good case?

Topics:

- C2, Management and Governance in Civil-Military Operations
- Experimentation, Metrics and Analysis
- Architectures, Technologies and Tools

Authors:

Dr. Alain Mutambaïe (NACMA)
Mr. Daniel Finney (MITRE, US NATional EXpert (NATEX) at NACMA)
Edited by Mrs Diane Phaetos (NACMA)

Organization:	**Point of Contact:**
NATO Air Command and Control System Management Agency (NACMA), Building Z NATO HQ, Boul Leopold III, B 1110 Brussels, Belgium	Dr Alain Mutambaïe Email: amu@nacma.nato.int Tel: +32 2 7078560

Abstract:

NATO is in the 2nd phase of its "NET-CENTRIC" or "Web enabled" transformation. NATO nations have ongoing C4ISR programmes and many of their legacy systems were industrialised or contracted before this Net-Centric transformation. The nations, like NATO, have the recurrent need to evolve their capabilities and converge to the NATO Network Enabled Capability (NNEC). Realizing the key NNEC goal of interoperability among "unexpected" parties remains a daunting challenge. Reference documents intended to specify the principles of the NNEC and to guide its implementation have been developed. Nevertheless, a comprehensive technical approach that can be applied to a broad range of likely systems and stakeholders has not been defined.

The concept of the NNEC is complex and constantly evolving. At this point it seems reasonable to expect NNEC to be implemented using a Services Oriented Architecture (SOA) based approach. The authors investigated the potential of employing an Enterprise Service Bus (ESB) federation strategy for converging to the NNEC. Using the NATO Air Command and Control System (ACCS) as a case study, they present an ESB federation strategy that can be adopted by the Nations and other NATO programs to address technical interoperability challenges for converging to the NNEC.

Keywords: ESB, ACCS, NATO, NNEC, nations, unexpected capability, technical interoperability

Table of Contents

List of Figures

List of Tables

1. Background

Several technology related concepts, such as Services Oriented Architecture (SOA) and Enterprise Services Bus (ESB) are being used to explain steps toward NATO's NNEC transformation. This section defines these key terms and clarifies their use in support of the objectives of this paper. First it identifies the challenges to implement NNEC reported by NATO and Nations.

1.1. NATO Network Enabled Capability (NNEC) and Reported Challenges

NATO architects have stated that NNEC is the ability of NATO to deliver precise and decisive military effects with greatly enhanced speed and accuracy as a result of closely linking sensors, decision makers and weapon systems[1]. While this may seem to be a rather simple and obvious goal for any military initiative, the concept of the NNEC is complex and constantly evolving. In order to properly define a NNEC implementation strategy that will help improve NATO interoperability, it is important to understand the characteristics of the environment in which the NNEC will be implemented.

The NNEC Feasibility Study (FS)[2] defined NNEC, recognizing that about 90% its implementation will be accomplished through individual NATO nations and about 10% through NATO organizations. In addition to the technology aspect, the FS also recognized that the NNEC paradigm includes network, information and people dimensions. Given the assortment of military and technical abilities of the nations within the Alliance, and their varying levels of funding and ambition, national contributions to the NNEC will range from nothing to substantial. The challenge is to accommodate all sizes of contribution to the overall NATO capability.

The principal goal of the NNEC is to provide information superiority to Allied Forces. This is accomplished through the implementation of procedural, operational and technological interoperability. Interoperability is the ability of different forces to exchange services so as to operate effectively together. NATO AAP-6[3] characterizes interoperability as the ability to operate in synergy in the execution of an assigned task. This is challenging when the requirement is to interoperate with unexpected capabilities. It is even more complex when the context is unanticipated and evolves rapidly. Therefore, to be effective, the NNEC must be robust and able to accommodate interoperability with the "unexpected", including non-military entities.

As for the nations, some are at a more advanced stage in their NNEC implementation, while others have not started. Some NATO nations have well established net-centric programs and capabilities that can play a significant role in NNEC, while others are still discussing the value of NNEC. The construction of the NNEC has already begun and its implementation timeframe is continuous. The NNEC is evolving as independent programs in the nations and NATO agencies and will continue to be implemented until it is declared unnecessary or ineffective by the NATO leadership. A good portion of the NNEC will be fixed, but much of the capabilities will be connected or disconnect by the nations in response to support requests for the various NATO missions. The NNEC strategy adopted by NATO should be enduring enough to base far term architecture and technical decisions on, but it should also permit the quick introduction of new technology and concepts, this is a challenge.

[1] O. Kruidhof NC3A, New Approach to Architecture at NATO, Arlington VA, NC3A, 2008.
[2] NNEC Feasibility Study, AC/322-N(2005)0059, Dec. 2005.
[3] NSA, NATO AAP-6 (2009) NATO Glossary of Terms and Definitions, Apr. 2009.

The types and complexity of technology and tools provided to the NNEC will include old or very basic along with sophisticated and leading edge, and everything in between. This technology will be developed by industry vendors or government from many nations. The NNEC strategy should be flexible enough to support a broad range of capabilities and the set of standards adopted should be practical for and available to as many equipment developers as possible. This is another challenge.

Finally, contextual and environmental parameters will continue to evolve. The future areas of operations, including the specific threat, are unpredictable and while the mandate dynamically changes, the technology and standards are quickly obsolete[4]. Therefore, NATO challenge is to build models for NATO systems convergence to NNEC that are flexible and enduring.

While the implementation of NNEC is already underway, progress is slow and efforts have not been effectively coordinated among the various stakeholders. Modest progress has been made on the recommendation outlined in the NNEC FS to perform NNEC readiness audits for projects within NATO's existing Capability Packages (CPs). Furthermore, the NATO C3 Organization (NC3O) stipulated that current efforts should focus on systems that are yet to be delivered[5]. Programs that are currently in development, such as ACCS, have received little guidance for their NNEC implementations. Certainly, the speed of the NNEC implementation is not sufficient to meet NATO's level of ambition, specifically in the area of NATO Air C2. While some important initiatives have been taken in the air domain, like those in current ACT's Mid Term Plan, the efforts are not part of a comprehensive NATO strategy.

In this section, we attempted to describe the NNEC identified challenges from a NATO capability point of view. The focus of this paper is on NNEC technological implementation challenges, plans and related strategies. It specifically examines the technological challenges for NATO Air Command and Control (C2) to convergence to NNEC. We make assumptions about other aspects of the NNEC paradigm where they directly affect the technology dimension. The challenge now is to determine the best way to implement the principles specified in the FS study and to share strategies for developing, fielding and using NNEC in support of NATO and multi-purpose coalition operations. The paper is aimed at the management, interoperability and implementation communities in NATO and National organizations who are responsible for the development, management, provision and use of NNEC in NATO led coalition environment. The paper will share with them our way to address the identified challenges.

1.2. Service Oriented Architecture (SOA)

A NNEC FS recommendation is to utilize a component-based SOA approach in implementing the NATO Information Infrastructure (NII). The NNEC FS identified SOA as a catalyst for technical convergence to NNEC and advised a stepped approach rather than a "big bang" approach for implementation. Little steps should not be misconstrued as simple steps. Each step may involve great complexity. It is, therefore, necessary to conceptualize the key elements of an SOA approach, namely visibility, services, implementation cycles and types, and governance. These elements will support the constructs established within the paper.

1.2.1. SOA Definition

According to OASIS[6], SOA is a paradigm for organizing and utilizing distributed capabilities that may be under the control of a different ownership domain. SOA is an architectural style based

[4] DND CANADA, The Force Employment Concept for the Army, Canadian National Defense, Ottawa, 2006.
[5] National C3 Representatives Meeting, AC/322(NC/3-REPS)DS(2008)0012 (INV), held in Amsterdam on 11 July 2008.
[6] OASIS Reference Model for Service Oriented Architecture (SOA), Apr. 2008.

on flexibly linked software components that leverage web standard and services. SOA practices are intended to create an agile, integrated Information Technology (IT) infrastructure that is scalable, reliable, and can rapidly respond to an organization's changing needs by employing loosely coupled and dynamic services. An SOA approach enables business needs to drive an organization's strategic IT decisions. As a result, SOA allows a business to become more efficient in meeting its current business needs and more agile in meeting future (and possibly unknown) business needs. It is important to note, however, that an SOA is neither a panacea nor something that can be purchased. There are challenges with employing SOA effectively.

1.2.2. Visibility

According to OASIS[7], "Visibility refers to the ability of those with needs and those with capabilities to see each other". Enabling visibility requires addressing the visibility of services and the correct descriptions of services and related artifacts. Attaining visibility in a SOA can range from word of mouth to formal service descriptions in a standards based registry/repository. SOA visibility concept is, later used within the paper, to support proposed coarse grain strategy.

1.2.3. Services

US DOD described a service as a mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description[8]. A service has the five following characteristics: modular, network accessible, reusable, standard based, and distributed capabilities. Within the Alliance there is no consensus on the definition and ontology of a service. Industry, NATO and nations have identified comparable services categories with different names and services scales within different perspectives. For instance, Cap Gemini[9] groups services in three distinct categories with different levels of granularity:

1. Core Services: services central to the actual business being considered.
2. Support Services: services which are not core to the general business or problem but which provide required functionality for the overall environment to function correctly.
3. Technical Services: non business requirement functions that are needed for the IT system to be delivered.

Vendors like IBM, nations like the USA, and NATO use other semantic and categories for services: core services, support services and shared services. NATO working groups under the NC3O are currently working on defining services semantics, ontology and rationale, but preliminary results have not been vetted[10]. For simplicity, this document assumes the following categories adopted by Cisco,[11] which are consistent with the service categories incorporated by most nations. Services can be:

1. Functional: providing specific business functionality from an operator point of view. Typically for Air C2 systems, the Recognized Air Picture (RAP), Air Tasking Order (ATO), Air Coordination order (ACO), etc.

2. Non Functional: providing all other functionalities, e.g. IA/security, logging, registry, collaboration, discovery, storage, etc.

[7] OASIS Reference Architecture Foundation for Service Oriented Architecture 1.0, Committee Draft 2, Oct.14, 2009.
[8] Department of Defense, Net-Centric Service Strategy: Strategy for a Net-Centric, Service Oriented DOD Enterprise, The Pentagon—Washington, D.C, May 2007.
[9] S Jones & M Morris, A methodology for services architecture, Capgemini UK plc, London, Oct. 2005.
[10] Core Enterprise Services Framework, AC/322-D(2009)0027, May 2009.
[11] C. Bussler, The Fractal Nature of Web Services, Cisco Systems, IEEE Publications, Los Alamitos, CA, Mar 2007.

1.2.4. SOA Development Cycle

As with system centric paradigms there is a SOA Life Cycle. **Table 1** describes the different phases of a service in a typical SOA life cycle (source IBM). These phases are applicable to a new service or application that needs to be interoperable with any capability using a middleware. SOA cycles are used in this document to implement the different ESB patterns (to be described later in the document).

1. **Model**	Gather and analyze business requirements. Design, simulate, and optimize the business processes
2. **Assemble**	Assemble new and existing services to form the business processes and optimize them
3. **Deploy**	Deploy the business processes
4. **Manage**	Manage and monitor these business processes from both an IT and business perspective
5. **Governance**	Feed information gathered during the manage phase back into the life cycle to enable continuous process improvement[12]

Table 1: SOA Life Cycle (IBM, 2008)

1.2.5. SOA Implementation Types

Industry defines three SOA implementation categories: project, infrastructure and enterprise driven[13]. Table 2 lists characteristics of each SOA implementation category. These categories are used to highlight the context of the technological implementation of NNEC initiatives proposed later in the document.

Project-Driven	Infrastructure-Driven	Enterprise–Driven
SOA scope confined in an individual project	SOA scope is building the utility/ foundation services	SOA scope wide. SOA is built for business responsiveness
Not focused on reuse	SOA platform that is reused across projects	Portfolio of reusable services
Management skeptical Need convincing	Management not bought in 100%	Management behind enterprise SOA
New project, innovative concept Build everything from scratch	Strategic portfolio planning, architecture and design policies limited in scope	Architecture standard applied
Specific Quick win	Governance requires increased cost, effort, time	Requires organizational alignment

Table 2: SOA implementation types

Table 2 is valuable for identification and categorizing the SOA implementation type. Therefore, the NNEC implementation projects and initiatives for existing and future NATO systems will fall on project-driven, infrastructure-driven or enterprise-driven categories with their respective characteristics in the project management behavior and environmental parameters. It should be noted that SOA implementation categories are independent of the project size or timeframe.

1.2.6. SOA Governance

SOA governance is a concept used for development and enforcement of SOA principles, policies and procedures. SOA governance can be seen as a subset of IT governance which itself is a subset of Corporate governance[14]. The focus is on those resources to be leveraged for SOA to deliver value to the Enterprise[15]. The ESB federation strategy, as developed later in this document, will benefit from SOA governance and as a whole NNEC governance if the NNEC governance does not lead to bottlenecks and impractical restrictions.

[12] B. D. Goulikar, K.L.P. Srinivas, U. Samudrala, Speed CBS development using IBM WebSphere Business Services Fabric industry content packs, Part 1: Model phase, USA, Oct. 2008.
[13] M. Afshar, SOA Governance: Framework and Best Practices, May, Oracle Corporation World Headquarters, CA, USA, May 2007.
[14] T. Biske, SOA Governance, Pakt Publishing, Oct. 2008.
[15] P J. Windley, SOA Governance: Rules of the Game, InfoWorld.com, 23 Jan. 2006.

Currently, the NATO Consultation, Command and Control Board (NC3B) is responsible for NNEC governance[16]. The assumption is that NNEC governance will establish efficient guidance and momentum in support of the NATO technical interoperability challenges. This not only by investigating an accurate list of the NATO Bi-Strategic Command (Bi-SC) capabilities shortfall areas, it is also by enforcing mechanisms that will leverage information superiority using NATO standards and sustain NATO's ability to interoperate with the unexpected. For instance, the assumption will be true if the NNEC governance can guide, regulate and enforce NATO standard agreed technologies (STANAGs) usage for NATO led operations[17] while facilitating temporary not (yet) NATO standard gateways usage for coalitions information exchange needs without undermining NATO C3 acquisition processes and priorities. Specifically, efficient NNEC governance is nowadays needed for addressing challenges, located at the Service Interoperability Points (SIOP[18]) level, to interoperate with unexpected capabilities as it is finger pointed within this document.

1.3. Enterprise Service Bus (ESB)

Another emerging concept that is often differently understood is the Enterprise Service Bus (ESB). The term was popularized by Gartner in 2002 when they declared ESB as a strategic investment. Since then, the concept has evolved, but still means different things to different people[19]. The authors view ESB as a tool to solve technical interoperability challenges. It is not the panacea, but, within NATO's specific context, it is an affordable way to address the identified interoperability challenges. The reference definition used for this document is the Wikipedia. ESB refers to a software architecture construct. This construct is typically implemented by technologies found in a category of middleware infrastructure products, usually based on recognized standards, which provide fundamental services for complex architectures via an event-driven and standards-based messaging engine (the bus). The ESB is the piece of software that lies between the various business applications and enables communication among them. Ideally, the ESB should be able to replace all direct contact with applications on the bus, so that all communication takes place via the bus[20]. An ESB generally provides an abstraction layer on top of an implementation of an enterprise messaging system. The primary advantage of such an approach is that it reduces the number of point-to-point connections required to allow applications to communicate[21].

Within the paper, we considered that an ESB has the following characteristics:

1. It is standards-based, flexible, and supports many transport mediums. An ESB is not necessarily web-services based.
2. It provides an abstraction for endpoints. This promotes flexibility in the transport layer and enables loose coupling and easy connection between services.

ESBs are more and more used by national Ministries of Defense (MOD) to address their SOA implementation challenges. Finland, Germany, Italy, Sweden, the United Kingdom, the United States and others reported that they are currently running ESB-based implementations for their respective architecture and SOA experiments. According to Forrester surveys, in the past five years, ESBs have been the number one product acquisition associated with SOA program[22]. Furthermore, Forrester stated that COTS ESB vendors provide better products than open

[16] Governance for NATO Network Enabled Capability, C-M(2008)006, dated 18 Jan 2008.
[17] One of the seven strategic goals according to NNEC Technical Services Strategy, AC/322(SC/5)N(2009)0036 VER 0.8.6, Oct. 2009.
[18] P Blomqvist and al, Guidelines using design rules in NATO NEC federated environment, NISPv4 development, March 2009.
[19] Enterprise Service Bus: A Definition, Anne Thomas Manes, Burton Group, Midvale, Utah, USA, Version: 1.0, Oct. 05, 2007.
[20] Enterprise service bus - Wikipedia, the free encyclopaedia, 2008.
[21] The Enterprise Service Bus as an Architecture Component, IBM, G Wilcox, presentation at NATO TIDE SPRINT Oct. 2010.
[22] The Forrester Wave: Enterprise Service Buses, Q1 2009.

sources and you will not find adequate adaptors with open source ESB solutions if you want to connect to multiple legacy systems using a combination of proprietary and legacy protocols. A rather simplistic but erroneous view often perpetuated by vendors is the ESB product itself provides the SOA. This is not accurate; as the SOA is neither a product nor an aggregation of web services.

To be complete, there are solutions other than ESBs for achieving interoperability within the NATO enterprise. However, we propose, later in the document, to benchmark any other solution with the ESB approach and to avoid the ESB whenever better solutions are found (Ref Table 4).

1.4. Patterns

The pattern concept is used to describe approaches and practices that can be shared in an ESB federation strategy. The ESB federation strategy is discussed later in the document. A pattern is a documented and repeatable solution to technical interoperability challenges located at the SIOP[23] within their respective service granularity levels. Patterns outside the SIOPs are not addressed in this document because they are specific to each capability. For instance, there are many different topologies that can be used to implement and federate ESBs. One mechanism is the Distributed ESB, or DSB. A DSB is a hierarchical structure that is built from the top down whose components are distributed or replicated throughout the various nodes and domains in the enterprise, and all are controlled by a "Master ESB."[24] The idea of a Master ESB that specifies boundaries and a set of allowable patterns is one of the ESB topologies suitable for a capability joining the NATO environment. However, the DSB concept is not the main pattern for this coalition environment of multiple NATO and non-NATO domains, where each domain owner is responsible for achieving the conditions required to make their ESBs interoperable with others in the enterprise at the SIOP level

Within the ESB federation strategy, patterns are generated through proof of concepts and SOA implementations using one or more ESBs to connect different capabilities. According to SOA researchers, patterns are contextual and are very pervasive in any enterprise grade solution implementation[25]. Historically, Patterns help architects overcome frequently faced problems during the design phase.

2. ACCS and NNEC

The Alliance's air defense mission is to protect the NATO nations' interest in the air, space and cyberspace. The NATO ACCS is key to NNEC success. ACCS is a NATO Security and Investment Program (NSIP). It is a key element of NATO's Common Funding, directly contributing to improving NATO's defense capabilities. The ACCS vision is to provide European NATO nations with an integrated, modern air C2 system that enables defensive, offensive and support air operations in a joint environment. Even though ACCS was conceived long before the NNEC Feasibility Study, it fits well with NNEC FS recommendations and it embodies many of the tenets necessary for Net-Centric Operations (NCO). Together with the NATO General Communications System (NGCS), which will form the backbone of a multinational global information grid, ACCS can enable the Alliance to exploit the benefits of NCO.

ACCS was conceived in the mid 1980s to provide an integrated European Air Consultation, Command and Control (C3) capability to face a Cold War threat. NATO will field the initial ACCS system at the completion of the ACCS Level of Capability 1 (LOC 1) contract in the 2010-

[23] SIOP serves as focal point for service interoperability between interconnected systems, and may be logically located at any level of service granularity. Its detailed technical specification is contained within a Service Interface Profile (SIP).
[24] ESB Federation for Large-Scale SOA, Françoise Baude & al, SAC'10 March 22-26, 2010, Sierre, Switzerland. SOA4All: http://www.soa4all.eu.
[25] Capitalizing on SOA by Arulazi Dhesiaseelan, 2008.

2012 timeframe[26]. ACCS LOC 1, including two crucial Engineering Change Proposals (ECPs), will provide the Alliance with a formidable Air C3 capability, integrating an array of command and control facilities that operate at various levels in the NATO command hierarchy across Europe. Additional enhancements to ACCS, including Link 16 enhancements, deployable sensors, and an Active Layer Theater Ballistic Missile Defense (ALTBMD) functionality, have been identified and are at various stages of planning and procurement.

The NNEC vision underscores the war fighting advantages gained from networking military enterprises and enabling geographically dispersed military forces to exchange information and create a shared awareness of the battle space. The ACCS program seeks to network sensors, real-time and non-real-time command and control facilities, and shooters located across NATO territories and in deployed locations. While ACCS does not encompass all of the tenets of NNEC, such as new strategies, emerging Tactics Techniques and Procedures (TTPs), or new organizational theories, it can be used as a test bed to mature these, as well as the technological aspects of NNEC.

Several inherent attributes make ACCS a good model for maturing NATO's NNEC objectives. Many of ACCS' architectural features are consistent with the technical tenets of NNEC, including (1) a J2EE architecture that provides a separation of the data, presentation, and business logic layers; (2) well-defined internal interfaces, and (3) standard interfaces to external systems (such as weather and air traffic control systems).

NATO organizations at various levels are involved in activities to develop NNEC-related policy and governance, NNEC architectures, and net-enabled capabilities. The ACCS program has distinctive attributes that make it suitable to become a model for many of these efforts. NATO has taken on new types of operations and technology has evolved since the ACCS LOC1 contract was signed in 1999. Obviously, current and future ACCS requirements should be regularly revisited in the light of new operation types and technologies. Formal NNEC-related requirements and implementation plans are needed for NATO and ACCS as well. This will depend on NATO collective will to transform and to reflect NNEC level of ambition for the air domain.

2.1. Stakeholders for ACCS Transformation

The transformation of ACCS to NNEC is not a concern for the NATO Air Command and Control Systems Management Agency (NACMA) only. While the way ahead for the ACCS program is still being decided, there are many stakeholders who will influence its transformation. The roles and perspectives of the main ACCS transformation actors are described in this section.

Several stakeholders are involved in this multifaceted decision making process. The following list reflects the existing organizations and processes for making transformation decisions affecting the NATO ACCS program:

1. The *NATO Air Defence Committee (NADC)* advises the North Atlantic Council and the Euro-Atlantic Partnership Council on all aspects of air defence, including tactical missile defence. It promotes harmonisation of national efforts with international planning related to air command and control and air defence weapons systems.
2. The role of the *NACMO BOD* is to oversee the planning and implementation of NATO's legacy and future air command and control systems. The BOD is supported by subordinate committees staffed by operational and technical experts nominated by participating nations.
3. *Allied Command Transformation (ACT)* is charged with leading at the strategic command level the overall transformation of NATO's military capability and *Allied Command Operations (ACO)* is charged with ensuring NATO's Minimum Military Requirements

[26] Depending on ACO's decision to declare ACCS operational with Block Upgrade 2.

(MMR) are met for all ongoing Alliance operations. The role of the Strategic Commands (SC) in ACCS transformation is to identify and prioritize all air C2 requirements consistent with NATO's and national NNEC goals.

4. Once new ACCS operational and technical requirements have been identified by operators and engineers, the NATO financial committees work with the operational community and the nations to manage NATO common funding with the aim to reinforce decisions and priorities established by NATO's senior committees.
5. As host nation for the overall ACCS program, *NACMA's* role is to conduct the central planning, system engineering and implementation of new ACCS requirements and to support NATO's overall goals for system integrity, interoperability and transformation.
6. The *NATO C3 Organization (NC3O)* is the senior policy body for NATO's C3 capabilities. The NC3O establishes the security, interoperability, CIS support and other policies for NATO C3 systems and will create and execute the governance structure for the NNEC.
7. *The NATO Programming Center (NPC)* runs the ACCS System Test and Validation Facility (STVF) and, together with *NATO Communication and Information Systems Services Agency (NCSA)* and *NATO Maintenance and Supply Agency (NAMSA),* will provide complete through-life management for all ACCS entities.
8. *The Nations* will continue to be central to all aspects of the NATO transformation. They are directly involved in the transformation of ACCS to NNEC, as ACCS is funded by NATO common, as well as national, funding and ACCS ARS will have dual roles for NATO and national security.

These are the key organizations that will influence the evolution of ACCS towards NNEC. Conway's law[27] states that the structure of a software product reflects the structure of its sponsoring and supporting organizations. Conway added that we will be able to create perfect software as soon as we learn to create perfect organizations. The success of the ACCS transformation depends on having a viable plan that the stakeholders are willing to adopt and on consensus. Therefore the recommendation is to gather full stakeholders support for any implementation of the paper's outputs within a comprehensive approach.

2.2. ACCS Current Status and Net Readiness

To develop an effective strategy to converge ACCS toward NNEC, it is important to first understand or determine the thresholds for NNEC convergence. These thresholds were defined by NACMA, which audited ACCS program documentation and used open source tools to evaluate its level of net centricity.

Several open source tools are available that evaluate the ability of a system or system component to operate in a net centric environment. One such tool is the Network Centric Analysis Tool (NCAT) developed by the Network Centric Operations Industry Consortium (NCOIC). Another is the Net-centric Enterprise Solutions for Interoperability (NESI) Compliance Evaluation Tool developed by the United States Navy. The ACCS reference architecture was evaluated by NACMA against both NCAT and NESI tools and a profile was developed following a Net centric checklist established by Assistant Secretary of Defense for networks & Information Integration (US ASD (NII)).

According to the Military Committee (MC), ACCS plays a strategic role for NATO air defense. ACCS is interoperable with more than 8000 external interfaces. Specifically ACCS provides innovative mechanisms for IP convergence of the NATO agreed Tactical Data Link (TDL) for the air domain. ACCS LOC1 interoperability is mostly accomplished using the ACCS Wide Common

[27] Conway, Melvin E. (April, 1968), "How do Committees Invent?", Datamation 14 (5): 28-31, retrieved on 2009-04-05, full text.

Information Exchange Standard (AWCIES)[28] or data links to exchange information among ACCS entities and between ACCS and AWCIES-capable external systems. The results of the ACCS Net readiness analysis concluded that the ACCS design and reference architecture are coherent, standards-based, and can be extended to comply with an SOA framework. Notably, other assessments have reached different conclusions with respect to the NNEC maturity of the ACCS. For example, the FUMIX roadmap[29] assessed ACCS as not yet being at NATO Maturity Level (NML) 2. The roadmap maintains the ACCS at the same maturity defined color level from 2010 until 2015. We agree that there are currently no NATO plans to converge ACCS toward NNEC but, as this initiative has not been coordinated with NACMA, we question the authors' real motivations for assessing ACCS NNEC maturity. Furthermore, without disputing the assessors' concept and knowledge of ACCS, we need to know the methodology and tool applied, and the ACCS baseline used as their reference, in order to judge the credibility of their conclusion. Of course, this situation is not unique to the ACCS: any differences in methodology, tools and baselines used when assessing the maturity state of systems could lead to very different conclusions.

There are many problems with these NNEC assessments: (1) there are no agreed NATO NNEC thresholds; (2) there are no agreed NATO net centricity evaluation tools or check lists; and (3) ACCS is not a fielded system. Given the lack of a clear NATO-wide vision for operating in the NNEC environment and the absence of tools or models to help NATO and national program offices chart a course consistent with NNEC convergence, this analysis yielded little useful data. It became clear that our goal to converge ACCS to NNEC would be better served with an empirical approach. NACMA, therefore, initiated a prototype development called ACCS NNEC, during NATO demonstrations, to validate the ESB federation as a strategy for achieving NNEC.
SAS-065 group lately produced a document providing an initial NATO NEC C2 maturity model. NNNEC concept, context and operational environment are well tackled, in the document, and include the challenges identified within the current paper. However, the angle of the document is wider and furthermore, the group addressed and assessed NATO C2 transformation at a higher level more organizational and fundamental. Currently, and using the model proposed from a technological and interoperability point of view, we are not able to benchmark NATO C2 through the procurement/fielding time frame and their efficiency to adapt to the unexpected. The current document addresses a different level of granularity. The inquiry is more applied to C2 technical requirement capture where the maturity level could be a tool to identify such NNEC requirement for NATO C2 in practice[30].

3. ACCS Transformation Initiatives and ESB Federation Strategy

Since 2005, many risk reduction activities were conducted by NACMA related to NNEC. This paper could not address all these initiatives within its boundaries. Therefore, this paper will discuss only the ESB strategies and vision for an ESB federation. The paper will illustrate how the ACCS NNEC prototype used ESB middleware to achieve interoperability goals within a short timeframe and how a vendor-independent ESB federation could be incrementally built, added or replaced in a repeatable pattern. This section also provides the rationale for ACCS NNEC prototype and a proposed NATO ESB federation strategy. It explains how any systems could be connected to an ESB federation. The ESB federation strategy is, therefore, presented in term of coarse and fine grain granularity. Finally, the strategy is detailed within a case study.

[28] AWCIES uses standard messages to exchange information over an IP network. AWCIES is a grammatical collection of six harmonized standard messaging sets (ASTERIX, ADEXP, DIS, ADatP-3, LINK-16, XML).
[29] Future Maritime Information Exchange (FUMIX) Concept Version 3, EAPC(AC/322-SC/1-AHWG/1)N(2009)0008, Nov. 2009.
[30] NATO NEC C2 Maturity Level, SAS-065, CCRP Publication serie, Feb. 2010.

3.1. ACCS NNEC Prototype

The ACCS NNEC prototype effort began in 2006. At that time we connected the latest available ACCS software (both the real time and non-real time components) a COTS ESB and continued to install each new software update as it was released to NACMA. The ESB is perceived by ACCS architecture and policy mechanisms as another ACCS entity or controlled sensor. Both parts combined are what we called the ACCS NNEC prototype. The ACCS NNEC prototype provides, within short time, services to the real and non-real time information consumers without affecting ACCS architecture. The consumers are both internal ACCS entities and external capabilities operating in the same or different domains.

The ACCS NNEC and its SOA implementations are developed independently from ACCS LOC1. Also the name ACCS NNEC avoids confusing the community with expectation on what will be available in ACCS LOC1. This prototype is not part of the ACCS LOC1 contractual development. Therefore, the prototype does not interfere with the ACCS LOC 1 delivery. It is perceived as risk reduction activity, to address future ACCS NNEC challenges. For instance, it provides an alternative that shortens the acquisition process, increases agility and allows the comparison of elements to satisfy future ACCS requirements. Furthermore, the ACCS NNEC prototype is representative of any other NATO or national SOA implementation belonging to the ESB federation strategy, as defined in the next section.

3.2. ESB Federation Strategy

Hypothetically, the federation is characterized by the fact that each ESB owner is responsible for their system interoperability, effect, visibility, security and governance. Agility is the key. The strategy involves federating all ESB initiatives and allowing NATO and Nations' systems to flexibly share information. In such complex environments, some services may be shared or reused only within a single domain, while others may be shared or reused throughout the enterprise[31]. Federated ESB enables the implementation of services across different entities, nations and domains through multiple ESBs providing desired real world effect. IBM believes that ESB federation allows different ESB products to be used in different domains, allowing an optimal match between domain requirements and product capabilities[32]. We believe that several implementation patterns exist for achieving ESB federation.

The hypotheses, developed in the paper, said that there are many reasons for adopting the ESB federation approach. Here is an overview of the most obvious one. The ESB federation strategy enables NATO's information superiority goal by providing technological interoperability across NATO, nations, partners and coalition.

- The strategy is an appropriate model to address interoperability challenges for NATO or nations with their different level of ambition and speed with regard to SOA implementation and converge to NNEC.
- The strategy allows coherent information exchanges, between different NATO and national systems, not using the same standard data and protocols without affecting existing architectures.
- The strategy provides NATO and national systems the agility to adapt to any NATO coalition or partnership or ad hoc need to share information.

Specifically, the ESB strategy addresses with a different focus external and internal ACCS LOC1 interfaces. Furthermore, the ESB strategy positioned ACCS as a transparent service provider for external consumers belonging to different domains. The focus is on loose coupling,

[31] IBM, WebSphere Enterprise Service Bus, Frequently Asked Questions, USA, June 2009.
[32] G Flurry & R Reinitz, Exploring the Enterprise Service Bus, Part 2: Why the ESB is a fundamental part of SOA, IBM, USA, Sep. 2007.

rationalization, scalability across several dimensions and resource virtualization. ACCS has a J2EE architecture and the proposed ESB implementation concept is vendor agnostic.

The perspective selected to describe the ACCS ESB federation strategy is fine and coarse grain. The objectives are to help represent both the challenge of connecting unexpected applications/services to federated ESBs from an ACCS NNEC point of view and the challenge of identifying patterns with heterogeneous organizational interfaces needed to meet the expectation of NATO operations.

A fractal is a complex shape which, when viewed in finer and finer detail, shows itself to be constructed of ever smaller parts, similar to the original[33].

Topologically, ESB federation can be seen as a complex network of systems, applications and services connected to nodes. The nodes are the middleware ESB when connected (at the SIOP) to any capability joining the federation. Using the fractal theory on networks and its self-similarity properties around a recursive aspect; the connection to a node helps to illustrate the different ESB federation strategy granularities from ACCS taken as a starting point. The ESB federation architectural concept is coherent with the UK MOD NEC Generic Networked Information Environment (GNIE)[34] federation specifications and requirements..

3.2.1. Coarse Grain Strategy

The coarse grain strategy provides the larger view of the ESB federation strategy from an ACCS NNEC perspective. Within such a topological perspective ACCS NNEC is the fractal starting node.

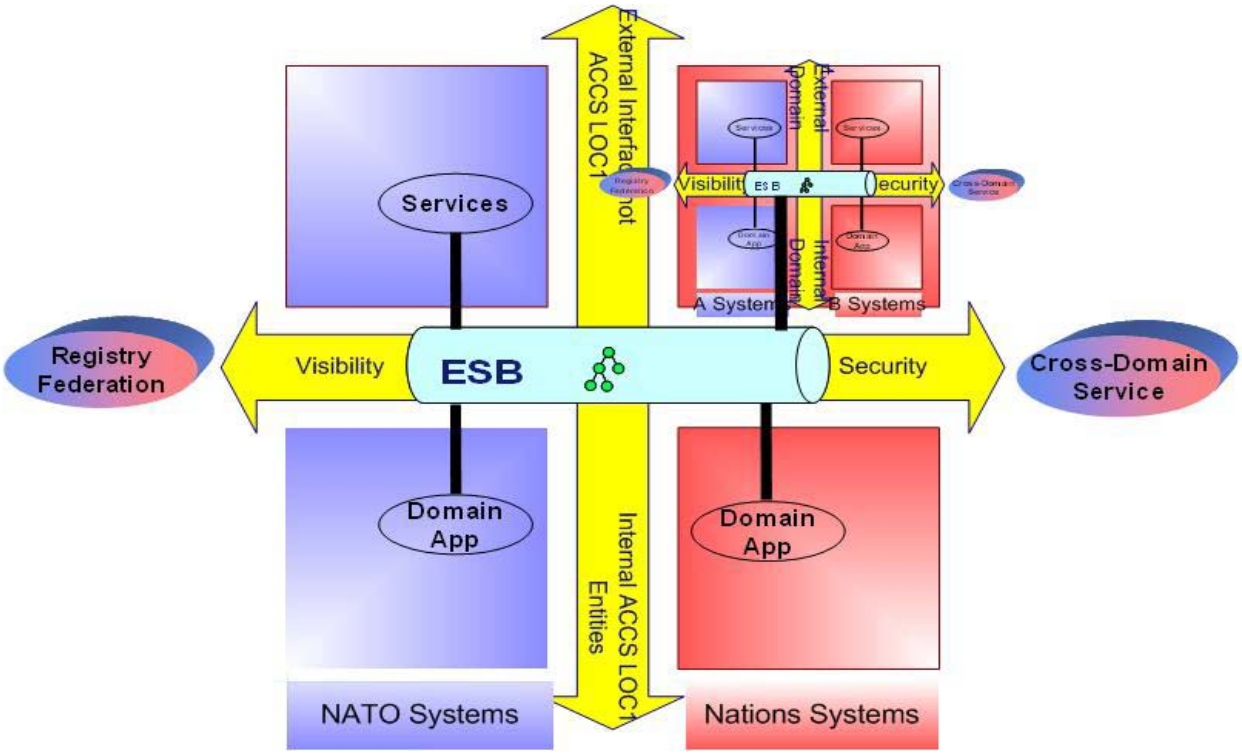

Figure 1: ESB federation strategy pattern (Coarse Grain)

Figure 1 provides the architectural concept and fractal patterns overseen for a federated ESB strategy involving ACCS NNEC prototype taken as starting point. In this case, ESB federation strategy consists of connecting ACCS NNEC ESB together with other vendor-independent

[33] Gleick, James. "Chaos: Making a New Science." Penguin, 1988.
[34] Carolyn Gill & Ian Scott, ESB Interoperability Specification for Federation, UK MOD, April 2008.

ESBs belonging to external systems, domain application, functional and non-functional services, entities within NATO and national or coalition environment. Each ESB node is connected to self-similar elements that provide visibility, security, required information and recursively other ESB connections. The ESB federation strategy is a composition of efficient ESB patterns addressing technical interoperability challenges. ESB federation strategies are dynamic and are evolving according to environmental parameters.

Figure 1 illustrates coarse grain pattern found in the ESB federation strategy from an ACCS perspective. The self-similarity is characterized by four similarity elements recursively connected to the ESB in an irregular way as listed in **Table 3**.

Similarity Element	Description
Visibility	Elements that enable awareness, willingness and reachability, like registry service, discovery mechanism, metadata, collaboration services...
Security / IA	Elements that enable adaptive Information Assurance/key security concepts across different security domains; confidentiality, integrity, authentication, authorization, non-repudiation and availability. Like security classification, policy mechanism, trust authority, cross domain security guard, auditing & login services...
Information Required	Elements that compose the functional services. It is Information Requirement[35] (IR business related) between internal external, national, NATO and ACCS entities/Systems
Other ESB connections	Elements that connect the patterns and nodes of the federation strategy. There is at least one connection to another ESB. The connections between ESBs are irregular and are depending on the environmental parameters

Table 3: Similarity elements description

Within coarse grain, the different patterns reflect the ESB federation irregularities. ESB federation irregularity, scale and fractal dimensions will depend on variation of environmental parameters. When deploying an ESB federation strategy, there are limits - the environmental parameters. The environmental parameters provide the ESB federation strategy boundaries and generate its irregularity of patterns. We have focused our grounded approach on the following environmental parameters:

1. Operation type (i.e. relief, asymmetric…)
2. Stakeholders: NATO partnership (i.e. EU, UN, PfP,...)
3. Technology availability (i.e. IPv6, Web…)
4. Interoperability targets (i.e. ambition, strategy, objectives, effects...)
5. Time (i.e. operations duration, deployment timeframe, operation date…)

However, other unanticipated parameters might also generate irregularities.

Once environmental parameters are identified and a fixed value given, it is easier to delimit ESB federation strategy patterns and specify federated ESB profiles. This also enables us to respectively compare efficiency of different ESB patterns and profiles having similar environmental parameters. The ESB federation strategy could provide inputs to the development of force structure options and providing input in the development of plans and taskings for coalition operations.

In the absence of vetted NATO Services/Applications assessment tools, it might be possible, given the environmental parameters, to establish technical interoperability indicators, performances and measurements using the ESB federation strategy. This approach could be considered for further investigations and inclusion in the NATO Interoperability Standards and Profiles (NISP)[36].

[35] APP-15 Draft 2 NATO Information Exchange Requirement Specification Process Feb. 2009 for STANAG 2519 by NSA.
[36] NATO Interoperability Standards and Profiles (NISP), STANAG 5524/AdatP-34 Version 5, Jan. 2011.

Before being replaced by another strategy, ESB federation strategy might remain since ad hoc situations and changes in the environmental parameters will occur and evolve. Also, a corresponding federation strategy approach could be developed from a different node perspective i.e. visibility elements, security or communication like federated registry strategy, federated security guard strategy, federation communication strategy, etc.

3.2.2. Fine Grain Strategy

The fine grain strategy provides the closer view of the ESB federation strategy life cycle from an ACCS NNEC perspective.

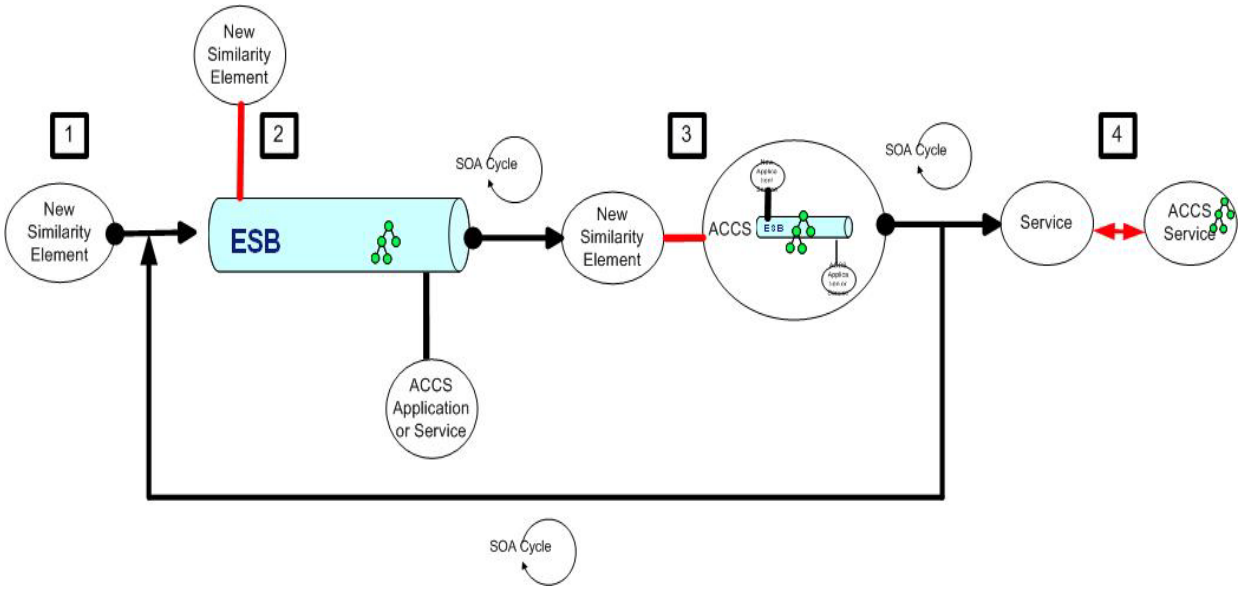

Figure 2: ESB federation strategy life cycle (Fine Grain)

Figure 2 illustrates the fine grain granularity of ESB federation strategy. In particular, it represents the ESB federation strategy life cycle and the potential state of a similarity element (applications/services/ESB) when connecting to an existing ESB node (e.g. ACCS and its ESB). The connectivity requirement is driven by the actual environmental parameters. The Information Exchange Requirements (IER) are iteratively matured during the ESB connection life cycle with the aim to optimize the information sharing to break down barriers to identifying, accessing and understanding data. The ESB federation strategy IER approach is compliant with the NATO IER Specification Process (APP-15)[37].

The life cycle shows the minimum architecture elements required and their connectivity evolution during the process to validate/benchmark the most efficient pattern and available technical interface for a specific environmental context at a SIOP level. Patterns and similarity elements will evolve over time because of environmental parameters uncertainty, constraints, governance and assumptions. There are four identified similarity element states in the ESB connectivity life cycle (fined grained strategy); each similarity element state, except the first one, is generated by a change in the environmental parameters and separated by a SOA implementation type, cycle and IER specification process.

Table 4 describes the similarity element connection states details. Usually, governance principles (choice of similarity elements relations, competition, coexistence or obsolescence) need to be applied when competitive patterns are found. The SOA implementation cycle for a similarity element connection to the ESB federation strategy can follow any one of the three

[37] APP-15 Draft 2 NATO Information Exchange Requirement Specification Process, Feb. 2009 for STANAG 2519 by NSA.

different SOA implementation categories identified: Project-driven, Infrastructure-driven and Enterprise-driven. Therefore, the ESB federation strategy will propose different possible patterns.

With a common aim to achieve interoperability of different capabilities, the ESB federation strategy can also be adopted as an agile transition to a potential direct/better interface in the future. Again, the agile ESB federation strategy could remain or be avoided because of the irregularity of environmental parameters. The ESB federation life cycle will continue until it is replaced by a better strategy as explained in table 4.

Application/Service Connection to ESB State	Description
1. Identify new similarity element not part of the ESB federation strategy	• Determine the environmental parameters • Describe the interoperability gap • Perform an IER process • Compare the ESB potential interface to other possible interfaces not using ESB • Propose or reject the new similarity element as a candidate to the ESB federation strategy; report findings
2. Connect a new similarity element to a single ESB	• Validate the environmental parameters • Perform an IER process • Compare available standard and ESB adaptors and select the best ESB performance according to the environmental parameters • Assess if the new similarity element is candidate to be connected to ESB federation (pattern or anti-pattern availability) • Perform SOA cycle
3. New similarity element shared within federated ESB	• Validate the environmental parameters • Identify, compare and rationalize the new similarity element with other network enabled interdependent similarity elements belonging to the ESB federation • Perform the IER process • Apply governance policies for connecting/optimizing similarity elements specific to the environmental parameters: ▪ Identify and compare the different possible ESB federation patterns and reject anti-patterns ▪ Benchmark the results and decide whether it is good enough to be operational with the new similarity element or modifications are required ▪ Check if any similarity element needs to be disconnected from the federation (to be decoupled as a new mature service or retired) • Gather shortfall and perform iteration/optimization if required • Perform SOA cycle
4. Disconnect similarity element ESB (direct service to service/ or retirement)	• Validate the environmental parameters • Apply governance policies for retiring/disconnecting similarity elements specific to the environmental parameters: ▪ Assess impact of disconnecting a similarity element, identify pattern and reject anti-pattern • Perform the IER • Identify and compare the potential service interface resulting from the disconnect; determine new service interoperability point; report gap and short fall • Perform a SOA cycle • Model and document appropriate architecture, metadata and views to be registered in the appropriated Registries/repositories • Document whether the service/ similarity element is not needed anymore and is retired

Table 4: Similarity element implementation states

3.3. Advantages of the ESB Federation Strategy

This section explains how the authors consider the ESB federation strategy benefits within NATO context. It summarizes the strategy outputs (in case the reader needed to know it before reading the case study). No single, overarching entity owns or governs the entire NNEC[38]. To make the NNEC viable, mechanisms are needed to facilitate the interaction between service requestors and providers on NATO, national, and partner systems[39]. NATO will fully control only the part of the capability provided through NATO-procured systems, and the interfaces to the NNEC. Services and information on these NATO systems will be distributed through one or more ESBs or other types of SOA mechanisms. Contributions to the NNEC from nations and NGOs will be provided through network domains controlled by the nations, not by NATO. The ESB federation strategy will enable requestors to access information and services from any place on the NATO network, while maintaining the intrinsic governance and security structures of the various ESBs and service providers connected via the NNEC. This autonomy not only enables the Alliance members to implement their national capabilities and connect to the NNEC at different timeframes, but it will also support a speedier deployment of NNEC and allow for quicker capability upgrades.

The autonomy and flexibility obtainable through a federated ESB will allow NATO to more quickly adapt to unexpected mission types, new technologies, evolving operational constraints, changing partnerships, and other unanticipated situations. The ESB federation strategy enables such adjustments while maintaining coherence during technology transitions, preserving the integrity of legacy architectures and information exchanges, and reducing the cost of implementing or modifying interfaces. Therefore, the ESB federation strategy is in line with NNEC data strategy[40].

The ESB federation strategy provides a host of practical benefits[41] for NATO's convergence to NNEC, including:

- enables legacy systems to incrementally implement new technology and interfaces;
- maintains data exchange capability between systems as data standards evolve;
- supports incremental fielding of new capabilities;
- allows for wider range of solution to satisfy information requirements;
- provides more flexibility to interface to unforeseen systems;
- provides ability to more quickly address future operational needs;
- localizes maintenance cost and lifecycle management responsibilities;
- reduces integration expenses for NATO and nations;
- reduces testing time and cost;
- reduces time to develop and validate new interfaces.

3.3. Benefit of the ACCS NNEC Prototype

The work achieved on the ACCS NNEC prototype is a practical, rapid and inexpensive way to address the SOA readiness of the ACCS system and explore approaches for converging to

[38] *Conditions for Achieving Network-Centric operations in systems of Systems*, Jan 2007, CMU/SEI-2007-TN-003, D. A. Fisher, B. C. Meyers, P Place.
[39] NATO Networked C3 Interoperability Policy, AC/322-D(2008)0041, Oct. 2008.
[40] NNEC Data Strategy, AC/322-D(2005)0053-REV2, Sep. 2009.
[41] Gartner's Reference Architecture for SOA Application Infrastructure, Mar 2009

NNEC. The audience will easily make a parallel between ACCS and many national systems when implementing the NNEC and be able to adopt the strategy. This is the main output of the ESB Federation strategy case study with ACCS NNEC described later in the document.

Within a coarse grain perspective, ACCS faces many of the same current and future interoperability challenges other Alliance and partner systems will encounter. ACCS has multiple operational entities, static as well as deployable, that will be fielded in geographically dispersed locations. ACCS will support NATO operations, and interface with external military and civilian systems. In addition, ACCS needs to be interoperable with unexpected capabilities. The ESB federation strategy, as proposed in the case study, demonstrates how ACCS entities connected through AWCIES could benefit from external capabilities and, therefore, share information with neither AWCIES nor NATO TDL compliant systems. This avoids creating a SOA or new technology demand. As illustrated later in the case study, the strategy maximizes complementarities rather than merely additive effect[42]. Finally, we believe that the strategy will avoid explosion of maintenance costs and provide adequate service management.

Within fine grain perspective, ACCS will have to interface with unexpected Alliance and partners' systems not covered by current CONOPS. The ACCS NNEC prototype can serve as a reference model for NNEC convergence and provide a good case study for comparable national systems. NATO benefits from the ACCS NNEC by having an internal reference program to identify and help resolve NNEC process and technology challenges, making it easier for the nations to converge to NNEC. Fine grain perspective shows the transition solutions for interoperability with unexpected without breaking current architecture integrity and maintenance. The ESB federation strategy enables connectivity adjustment while maintaining coherence in the technology transition when new technology or standards emerge. Only new added similarity elements have to be challenged. AWCIES can evolve within a short period. AWCIES standard can be maintained and incorporate new emerging standards or legacy systems within the strategy life cycle. The strategy will allow reusability of successful pattern/profile within similar environmental context. The strategy will enforce interoperability to unexpected until emerging standards are agreed or legacy systems phase-out.

Bottom line, agility is the key: one size fits all strategy will not be sufficient to address multiple potential adversaries and to fight and interoperate with partners[43]. The patterns built on the top of the ESB federation strategy avoid developing ad hoc stove pipes, where doing so adds complexity without compensating advantages. The ESB federation strategy allows us to also disable interoperability with the unexpected, when appropriated, without affecting contributors to the overall capability. It might be fruitful to compare the ESB federation strategy with other available interoperability strategies to implement equivalent information sharing within short time.

4. Strategy Implementation Case; ACCS NNEC Proof of Concepts

This section describes how the ESB federation strategy was pursued using the ACCS NNEC prototype. The ESB federation strategy has provided technical interoperability between ACCS and unexpected capabilities within short time. A similar approach can be applied by any other system when implementing SOA.

4.1. Context

An agile transformation approach depicting ACCS convergence to NNEC strategy was proposed by NACMA at the NNEC Conference 2007 for the NATO community as illustrated in Figure 3.

[42] United States Capstone Concept for Joint Operations Version 3.0 , 15 January 2009
[43] Independently Secured Networks, NCW 2009 Conference, MITRE, Mary Ann Malloy.

Figure 3 illustrates the framework we used to mature, experiment with, and implement an ESB federation strategy from an ACCS NNEC point of view. The strategy was presented as a pattern to ACCS transformation and convergence to NNEC. We adapted and applied the OASIS model. The OASIS reference model was identified to guide the ESB strategy implementation framework. All combined, it provided to ACCS NNEC services accurate visibility, interaction and real word effect.

The challenge was to demonstrate how ACCS could easily adapt to future operations types and threats (i.e. Effect based Operations (EBO), asymmetry), since the surest way to invite a threat is to be unprepared for it. Part of the constraint was to provide technical solutions with vague requirements and never interfere with the current ACCS LOC1 contract. Does this sound familiar to other systems? This is part of the contextual situation on which the ESB federation strategy was proposed as a vehicle to implement SOA principles in ACCS.

The ESB federation strategy implementation, from an ACCS NNEC perspective, was realistic because of its holistic approach involving different players: NATO players (NATO agencies and SC), industry (Oracle, EADS, LUCIAD, IBM, BEA, Raytheon, etc.), fielded national systems, NATO systems and prototypes (Euro Fighter, ICC, JADOCS, JCOP, JTS, MUSIC, NE-3A, Nor BFTS, SHIFT, etc.). Operational advice was provided by ACO/J3, ACO PCT and elements from the NATO CAOC1 (2007 and 2009). The lists of capabilities and people involved are not exhaustive (see annex 1.). The trials and demonstrations, when not performed remotely, were most of the time located at NPC[44] (from 2006 until 2010), and annually performed at NATO CWID in Norway (from 2006 until 2009). Some trial activities were conducted in France and USA (form 2007 until 2010). Definitely more of those trials, demonstrations and exercises have to be carried out in the future.

4.2. Methodology

The information was empirically collected from various NATO forums. For instance, information related to SOA concepts and principles was derived from NNEC FS and periodically additional refined technical specifications were collected by engaging industry and monitoring innovative findings from NC3B working groups and sub committees. Such SOA concepts were not required for the current ACCS contract and the challenge was to determine possible technical solutions addressing NNEC challenges and to propose and validate potential MMR for ACCS without interfering with ACCS LOC1 planning. This is part of the system context constraints.

The ESB federation strategy was initiated taking into account the following contextual constraints. In order to capture ACCS future requirements, as well as to be reusable with ACCS LOC1 (in short and midterm), the prototype evolvement depended on ACCS LOC1 software availability and its scheduled releases[45]. Within a six month development cycle, trial activities were conducted on the prototype using the most recent ACCS software release and every year an increment was performed with a longer term improvement vision. ACCS NNEC was initially prototyped with ACCS 2.0 software version and is currently upgraded to version 5.1. Additional constraints are to maintain ACCS architecture as defined in the contract, to avoid any Intellectual Propriety Right (IPR) issues and, finally, to acknowledge that there is no available mature INFOSEC solution for cross domain information exchange specifically for TDL. NATO emerging standards and policies were used to guide the SOA implementation, architecture and design. Depending on the case study field of interest, it was likely to deal with strong resistance or support from the NATO staffs management during the SOA implementation process.

SOA implementation in ACCS and the ESB federation strategy findings could start and be included with DARS and ALTBMD delivery. However, it will be possible only if it is contractually specified. As the ACCS LOC1 contractual requirement was specified during the last century,

[44] ACCS-JTS NNEC INTEROPERABILITY EXPERIMENT-1 FINAL REPORT, NC3A 2007.
[45] NPC Study Report, JEP Experiment (ACCS interoperability), T Kiersling, Sep. 2010.

they must be revisited in light of the new operational paradigms and, obviously, there is a need for new requirements before any SOA implementation. Current findings are already reported and if the MMRs are validated, the SOA technical solutions will be proposed to the SC and all appropriate stakeholders for implementation.

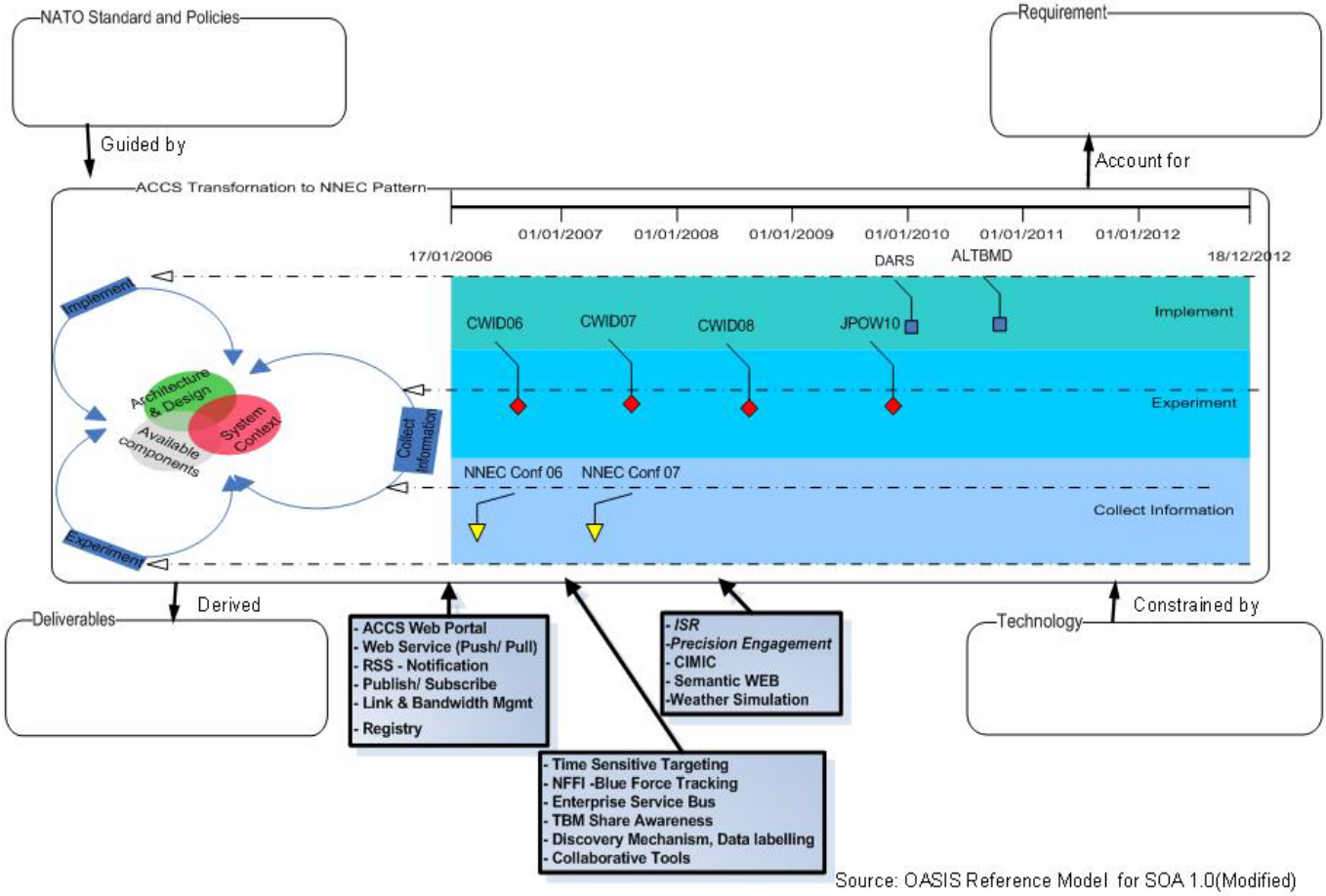

Figure 3: ACCS NNEC approach and framework (published at NNEC Conference 2007)

4.3. Results

Table 5, in Annex 1, provides a technical overview of some results achieved since 2006 related to ACCS NNEC case study. One objective was to incrementally capture the technical requirements, develop, implement and operate SOA concepts in ACCS NNEC with the aim to validate and build a comprehensive ESB federation strategy. The SOA based results and the ESB federation strategy, implemented in the case study, are proposed to the stakeholders for operational inclusion in ACCS current and future capabilities.

Table 5 also illustrates how the SOA implementation using the ESB federation strategy was achieved with ACCS and its constraints. This constitutes a SOA implementation reference for ACCS. While, others SOA implementation approaches might be possible, nowadays, a comparative assessment can be conducted between available ACCS transformation initiatives and the ESB federation strategy achieved. ACCS stakeholders are welcome to contribute on the NNEC governance, directions and possible realignment.

The objective to implement ESB federation, using ACCS NNEC, was successfully achieved within short time. ACCS NNEC was able to act and share services with external and internal entities within a few weeks. The ESB federation strategy was validated at the coarse and fine grain level of granularity using an agile approach. Furthermore, this helps to gather useful technical requirement and patterns for sharing information with unexpected capabilities.

Several patterns were established with the ESB federation strategy. We could incrementally add all identified similarity element types to vendor independent ESBs and recursively. It also allows benchmarking the strategy performance, for instance, the RAP and FFT dissemination to internal as well as to external entities. The approach will be of benefit to ACCS and NATO C3 in the future. It illustrates the way to interface to unexpected capabilities (that uses proprietary format), to create, and to generate federated service groups within different patterns. It proposes a valid and flexible strategy for NATO coalition operations. It demonstrates ACCS flexibility for sharing information with no AWCIES compliant capabilities, for transition of other capabilities to ACCS and finding avenues for deployable entities and ALTBMD.

ACCS NNEC activities allow to test and benchmark new technologies before any commitment for capability acquisition. We could interface ACCS to evolving proprietary format and emerging NATO standard format like the NATO Friendly Force Information (NFFI). This gives the opportunity to reduce future (ad hoc and costly) specification changes in the traditional contractual acquisitions process. The strategy allows us to investigate and mitigate the impact of future standard and technology trends like adoption of EoIP or new sensor type data feed. However, some issues have to be addressed related to NNEC governance, operational priorities and technology. The patterns identified using the ESB federation strategy are not perfect and always need to be challenged, but it works; it provides efficient interoperability to unexpected capabilities, it is agile, it will not break the capability architecture, it is rapidly operational and nonetheless it is affordable.

The ESB federation strategy applied to ACCS NNEC allows implementing all identified SOA implementation types; the lessons learned are valid and transferable to other NATO capabilities when they have to prepare strategies to operate and share with unexpected capabilities.

4.4. Way Ahead

There is a need to clarify ACCS role in future operations and a specific need for governance on AWCIES evolvement. As current standards used within AWCIES are evolving, there is an urgent need to adapt AWCIES to support those evolutions. Another concern is that it appears that some NATO capabilities funded after ACCS cannot implement AWCIES while they were supposed to. Maybe, new standards have to be added to AWCIES in order to satisfy NATO C3 coherence and establish a minimal interoperability with those capabilities. Governance and guidance is needed for NATO newly agreed or emerging standards like JC3 IEDM, JRE and NVG. In addition, there is a lack of new operational requirements and future operational perspectives for ACCS. There is a clear need to revisit ACCS CONOPs against current and future operations supported by NATO coalition. During the NNEC initiatives process, many technical requirements were captured and potential implementation identified pending an MMR formulation by SC.

The ESB federation strategy needs to be challenged to improve its performance and pattern and against other NNEC implementation strategies. There is a need for more systematic, NNEC related, coalition capabilities interoperability tests and events. NATO needs to develop SOA testing methodologies for large scale acknowledged systems of systems[46], Net-ready capabilities must be tested together regularly in ad hoc and coordinated fashion to measure NNEC implementation speed and level of ambition. It will enable to test both small ad hoc ESB federation and larger ESB federation deployments. Will Net-ready capability declared operational without full test within the environmental parameter states they will use, and capabilities they will have to share information with? Meanwhile the ESB federation strategy is evolving other strategies will emerge. A follow up ESB federation strategy assessment is planned within two years. The ACCS stakeholders' involvement is needed for the way ahead to address ongoing issues, e.g. questions are still not answered about deployable ACCS

[46] Systems of Systems and Net-Centric Enterprise Systems, J Dahmann, K Baldwin, Kristen J. Baldwin MITRE Corporation, 2009-2010.

participation to DJSE. Future efforts in SOA area are usage of SOA in real time (handle the strict delivery and timing requirements), Cyber security, and information management in cross organization environments.

5. Conclusions

NNEC implementation strategy aims to support interoperability and NATO capabilities transformation. The transformation of ACCS, as one of the major NSIP, is a good indicator/case to assess SOA implementation speed and NATO's level of ambition to transform its air defense toward NNEC. Currently there is not enough evidence of NATO willingness to implement a comprehensive NNEC strategy in the air domain. Taking into account the duration of the NATO acquisition process, it is better to start early. Despite of that, this paper highlights several patterns enabling NATO to rapidly converge large and distributed capabilities toward NNEC technical interoperability.

Therefore, Enterprise Service Bus (ESB) can be used by NATO as a flexible connectivity infrastructure for integrating capabilities. Actually, NNEC strategic goal is to deliver precise and decisive military effects by adopting a state-of the-art SOA approach, taking the benefit of available COTS and tools like ESB. When addressing unexpected the aims is to reduce services integration complexity, promote reuse, add new services faster and dynamically change services with little impact on existing architectures. Since the NNEC requirements are not yet formalized for ACCS and for some other NATO systems, the paper proposed to adopt the ESB as an affordable tool to address the technical interoperability challenges. Specifically ESB is a tool enabling to share information with unexpected capabilities (handle the interfaces complexity, incrementally assess potential IER and related emerging technologies, and finally benchmark those requirements).

The findings indicate that the ESB federation strategy is a composition of efficient ESB patterns addressing technical interoperability challenges. The ACCS case study showed that the ESB federation strategy addresses unforeseen changes in the NATO environmental context; time, technology availability, interoperability target, operations type and partnership. In addition, it is also addresses Nations' different speed and level of ambition when implementing SOA. The way ahead is the ESB federation strategy adoption by the Alliance, an incremental implementation in any operational context, its deployment in multiple geographic locations (Theatres) as well as multiple security domains.

The Alliance will benefit from ESB federation strategy if appropriate changes are carried out on NATO capabilities acquisition, usage, planning, governance and maintenance processes. In order to sustain its information superiority, adapt to new paradigms and enforce a proactive NNEC implementation, NATO needs a tailored approach for consolidating new requirements and its architecture federation. There is a call for social and cultural change. The following bullets are concerns and takeaways related to those NATO processes:

- To move faster toward NNEC convergence, the Alliance needs to identify criteria that must prevail to achieve comprehensive acquisition, development and use of Net-ready capabilities. A clear NATO commitment on its NNEC level of ambition, for current and future NSIP, will help capture the criteria.
- Effective guidance, governance and practices for acquisition, development, and operation of Net Ready capabilities are not yet mature. NATO capabilities, including ACCS, could addresses NNEC challenges if there is an immediate improvement in the way NATO plans future capabilities and how it does its acquisitions.
- Experimentation and benchmark of the candidate NNEC solutions is crucial to NNEC implementation. NATO has an absolute requirement to confront bad news early in the acquisition process; this is the essential element of success.
- NATO NNEC implementation strategies should rapidly leverage its speed, be agile and dynamic because of continuous evolution of the environmental parameters, the

necessity to interoperate with both unexpected and legacy systems and the requirement to adapt to unforeseen situations.

- The difficulty will be for NATO to build comprehensive NNEC plans and implementation strategies not only focused on immediate and urgent requirements. These should be balanced. To be robust and coherent, the plans and strategies should be revisited more frequently and the air pieces cannot miss. Definitively, better coordination between ACCS stakeholders for capturing requirement and planning NNEC transformation is needed. The NNEC implementation strategies have to be multi-faceted - no single implementation strategy is sufficient to give the needed result.
- Practical NNEC Governance will be required to regulate and measure effectiveness of the ESB federation strategy. ESB federation strategy could be successful if the stakeholders enforce cooperative and selective governance distributed across the ESB owners. It should also be selective because governance should not lead to bottlenecks and impractical restrictions. Otherwise, there is a risk to collapse the NNEC implementation strategy aim; building a bridge or a highway does not require the same Lego composition.

Annex 1. ESB Federation Strategy Achievement Examples

	2006	2007	2008	2009
Objectives/ Strategy	• Identify and provide ACCS NNEC services to external capabilities • Initiate ESB federation Strategy	• Optimize current ACCS NNEC services • Improve situation Awareness in the air domain	• Validate ESB federation strategy by connecting to other ESBs • Improve ACCS NNEC services visibility • Propose alternate pattern for transition to ACCS	• Investigate and implement security mechanisms • Connect ACCS NNEC to unexpected sensor sources • Enforce ACCS services' versatility
Coarse grain	• Investigate patterns for connecting Information required (targeting information) • Investigate internal ACCS LOC 1 entities information exchange not provided by the current architecture	• Mature patterns for connecting Functional Services (sensor information and high echelon Information sharing)	• Provide patterns for enabling ACCS with visibility related similarity elements (registry synchronization, discovery mechanism) • Investigate patterns for connecting to other vendors independent ESBs. Connect ACCS NNEC to three different ESBs directly and recursively	• Investigate patterns for enabling security I/A related similarity elements (authentication, policy mechanism, security classification, cross domain security guard) • Consume unexpected information for sensors not controlled by ACCS • Provide versatile services to unexpected customers like versatile ACO/ATO format
Fine grain	• Identify a COTS ESB and connect it to ACCS (RT+NRT) • Connect to targeting web services • Connect ACCS system information to COTS ESB and externalize its business logic	• Expose ACCS RAP service in XML • Connect to external imagery/Intel information related to ACCS target list, orchestrate and display it in ACCS NNEC	• Benchmark registry and discovery mechanisms across ESB federation • Share ACCS' ATO/ACO information via Web services • Disseminate ACCS JEP within Federated ESB	• Create generic tagging mechanism for current ACCS NNEC services enabling security classification description • Expose ACCS tagged information to other systems • Manage multiple format sharing within Federated ESB • Connect non functional services like independent notification mechanism management
Added value	• Investigate NNEC convergence strategies • Exchange information using machine to machine web service technology • Expose ACCS NNEC as a SOA service provider and consumer	• Provide information not available in the AOD • Possible inclusion of the finding, for implementation, in DARS and ALTBMD; will depend on SC decisions • Generate a Situation Awareness service group • Create generic mechanisms to expose ACCS information	• Provide alternate solutions for transition to ACCS • Generate patterns for coalition environment • Improve ACCS information controlled visibility in the operational environment • provide interface to proprietary format on request (i.e. NVG) • Demonstrate ability to Connect ACCS to national IEG and share information	• ACCS NNEC could collect SA on areas not covered by ACCS and disseminate it using different standards • Provide a collaborative alert mechanism between ACCS NNEC and other capabilities • Improve ACCS deployability in unforeseen operation types • Enable better SA and coordination with land, maritime and national capabilities • provide linkage to unexpected sensors

Focus on SOA and Capability Implementation (Implementation Type; PD, ID, ED[47])	• Retrieve targeting information (PD) • Select ACCS adaptors to ESB (PD) • Connect to JTS ICC Web Service (PD)	• Build adaptors to NFFI and provide FFT information to aircraft cockpit (ED) • Improve target information exchange web service performance (ID) • Collect imagery and intelligence information via web services and caching mechanism (PD) • Create agile SA by disseminating RAP and TBMD picture in Xml using SOAP (PD) • Connect to different ESB vendors (IBM, BEA,)(PD)	• Enrich ACO and RAP dissemination to NATO-JCOP, CAN TBMCS (ID) • ACO ATO information exposed via Web Services (PD) • Retrieve Meteo (Ge) information through IEG and displayed on ACCS NNEC GIS (PD) • Operate ESB federation with GER FIN (SHIFT), ITA , and others Registry synchronization (ID) • Provide realistic approach and clear measure for ACCS NNEC SOA readiness	• Improve SA with FFT, MSA, OTH Gold data by including it in ACCS JEP(ID) • Expose ATO, ACO versatility on web services (PD) • Registry and discovery features improvement (ID) • Use collaborative tools to share ACO/ATO and Target information with NATO AWACS • Investigate EoIP implications on ACCS • Generate metadata specification and tagging of tactical information with security classification (PD)
Issues	• Difficult to assess ACCS with available Net-Ready Key Performance Parameters • Vague NATO and Nations' operational priorities for NNEC • Never ending arguments for ESB strategy to be accepted; inertia from certain engineers	• Difficulty to validate the environmental parameters in available test context • Need caching imagery when update not available to avoid loading the network with the same information • No consensus on AWCIES way ahead and maintenance strategy	• UDDI and ebXML registries provides different advantages; difficult to choose the one to adopt • Lack of NNEC governance principles and vision on its practical implementation	• Operational need and justification for AIS, MSA OTH Gold or new sensor format type not expressed for ACCS • Limited number of partners to exchange messages and test the federation • Insufficient NII availability, security rules and mechanisms
Findings	• SOA implementation having project driven characteristics creates high inertia • Helped to generate rules for data transformation and to establish mapping of targeting information between different systems • Ground to identify core functional services with ACCS NNEC • Current net-readiness tools are not adapted to ACCS (NESI, NCAT) • Describe ACCS internal information distribution mechanisms limitations • Identify patterns for connecting ACCS to ESBs and share services; similar targeting information could be exchanged with unexpected capabilities like JADOCS	• Potential requirement to provide RAP in XML • Potential midterm solution for providing ground FFT to aircraft (Fratricide reduction). This demonstrates technical ability to receive FFT positions horizontally from national sources and provided it to Euro Fighter. This might require appropriate update in TTPs and CONOPS • Patterns require to be benchmarked in more operational context • Need to adapt current procurement processes and decide how SOA add on and ESB federation acquisition should be. Procurement timeframe should be shortened • Similar SOA mechanisms could be enforced to exchange information with unexpected WOC/SQOC	• Found potential interoperability solutions for operators participating in C2 activities but having limited communication or software resources like FAC and NE-3A operators • Need governance on the AWCIES evolvement. NATO systems might implement interfaces to current AWCIES. What will happen to non NATO systems? Technically AWCIES evolvement remains possible • Registry benchmark results; ebXml more appropriate for ACCS service types • ACCS RAP could be shared across several domains for Situation Awareness	• Need resources for more C2 technology test facilities for NATO and coalition ESB federation test in different environmental contexts if we have to prepare for unforeseen • Need to test interfaces with JC3 IEDM, and other emerging standards • Lack of new operational requirement (EBO, Asymmetry) and operational perspectives adapted to ACCS descoped the security related trials. Need ACCS stakeholders' involvement. What about adapting CONOPS and the doctrine? • Result difficult to compare with similar activities. Lack of other strategy to compare

Table 5: ESB federation strategy achievement examples (ACCS NNEC from 2006-2009)

[47] SOA implementation types: Project Driven (PD), Infrastructure Driven (ID), Enterprise Driven (ED)

Annex 2. Acronyms

Acronym	Description
ACCS	NATO Air Command and Control System
ACCS LOC1	ACCS Level of Capability 1
ACCS NNEC	ACCS prototype implementing NNEC concepts
ACO	Allied Command Operations
ACO	Air Coordination Order
ACT	Allied Command Transformation
ALTBMD	Active Layer Theater Ballistic Missile Defense
ARS	ACC, RPC and SFP
ATO	Air Tasking Order
AWCIES	ACCS Wide Common Information Exchange
Bi-SC	(of the two) Strategic Commands
C2	Command and Control
C3	Consultation, Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CONOPS	Concept of Operations
COTS	Commercial-Off-the-Shelf
CP	Capability Packages
CWID	Coalition Warrior Interoperability Demonstration
DJSE	Deployable Joint Staff Element
EAPC	Euro-Atlantic Partnership Council
EBO	Effects Based Operations
ECP	Engineering Change Proposal
EoIP	Everything Over IP
ESB	Enterprise Service Bus
FFT	Friendly Force Tracking
GNIE	Generic Networked Information Environment
IER	Information Exchange Requirement
IPR	Intellectual Property Rights
J2EE	Java 2 Platform, Enterprise Edition
JC3IEDM	Joint Command, Control and Consultation Information Exchange Data Model.
JRE	Joint-Range Extension
MOD	Ministry of Defense
NACMA	NATO Air Command and Control System Management Agency
NACMO BOD	NATO ACCS Management Organization Board of Directors
NADC	NATO Air Defense Committee
NAMSA	NATO Maintenance and Supply Agency
NATO	North Atlantic Treaty Organization
NC3B	NATO Consultation, Command and Control Board
NC3O	NATO C3 Organization
NCO	Net-Centric Operations
NCOIC	Network Centric Operations Industry Consortium
NCSA	NATO Communication and Information Systems Services Agency
NFFI	the NATO Friendly Force Information
NGCS	NATO General Communications System

Acronym	Description
NII	NATO Information Infrastructure
NISP	NATO Interoperability Standards and Profiles
NNEC	NATO Network Enabled Capability
NNEC FS	NNEC Feasibility Study
NPC	NATO Programming Center
NSIP	NATO Security and Investment Program
OASIS	Organization for the Advancement of Structured Information Standards
RAP	Recognized Air Picture
SIOP	Service Interoperability Points define the boundaries at which the various services actually interact.
SOA	Service Oriented Architecture
STANAG	NATO Standardization Agreement
TDL	Tactical Data Link
TTP	Tactics Techniques and Procedures
U.S.	United States
US ASD (NII).	Assistant Secretary of Defense for Networks & Information Integration
US DOD	USA Department-of-Defense

Table 6: Acronyms Description