18th ICCRTS

Paper ID 013

“C2 in Underdeveloped, Degraded and Denied Operational Environments”

How to increase NATO capabilities interoperability, when dealing with the 'unexpected'?

Suggested Topics:

1. Networks and Networking
2. Architectures, Technologies and Tools

Abstract:

During North Atlantic Treaty Organisation (NATO) led operations, the environmental situation often will change unexpectedly; this may involve either the participants, the threat, the objectives, the (mission/operations) duration or the technology availability. Such events will challenge the interoperability between the coalition capabilities.

From a technical interoperability point of view, this paper proposes an innovative strategy to adapt, and meet unexpected environmental situation changes. In such cases, the strategy consists of increasing interoperability through a gateway based federation of capabilities and efficient patterns. A (Grounded) theory is derived from multiple case studies on strategies to connect the NATO Air Command and Control System (ACCS) with an Enterprise Service Bus (ESB) federation when addressing comparable situations.

From a NATO capabilities point of view, this paper’s added value is to generalize the innovative strategy and to efficiently address the 'unexpected'.

Keywords:

AirC2, ESB, ACCS, NATO, Federation Strategy, SOA, NNEC, Future Mission Network, Smart Defense, Unexpected Environment, NATINAMDS, Asymmetric Operations, Innovation, technical Interoperability, KPI, ROI, Connected Forces Initiative, Network.

June 19-21, Alexandria, VA USA.

Organization:

NATO Communication and Information Agency (AirC2 PO)
Building Z NATO HQ, Boul Leopold III,
B 1110 Brussels, Belgium

Author & Point of Contact:

Dr. Alain Mutambaïe
Email: alain.mutambaie@ncia.nato.int
Tel: +32 2 7078560

1. Situation Overview and brief Analysis

During the 21st century, NATO's environment has changed and NATO needs to adapt to unexpected environment changes, which includes the global recession (Binnedijk & Al, 2010). The future NATO areas of operations, including the specific threat, are unexpected and whilst the mandate dynamically changes, technology and standards quickly become obsolete (DND, 2006). NATO missions/operations require to evolve and adapt to address the environment, short, mid and long term changes, as long as the changes will go on.

To address environment changes, NATO nations have adopted a new strategic concept (Lisbon Summit, 2010) promoting a Comprehensive Approach, the Connected Forces Initiative and Smart Defense (Chicago Summit, 2012). The later introduced the principle to specialize, prioritize and pool capabilities; nations are invited to cooperate using geographical arrangements and/or common funding mechanisms to acquire capabilities.

To address short and mid-term operational changes, NATO has developed new concepts and acquired lessons learned including from the NATO Network Enabled Capability (NNEC), the Afghanistan Mission Network (AMN) and the Future Mission Network (FMN). The NNEC paradigm consists of network, information and people dimensions (NC3B, 2005). NNEC provides information superiority (ability to get the right information to the right people at the right time). The AMN concept is a practical application of NNEC and consists of the International Security Assistance Force (ISAF) secret network as the core with multiple national extensions (ACT, 2011). Therefore, two AMN lessons learned are specifically considered in this paper. First is the joining instruction for the AMN and second it is the commander's decision to connect all capabilities within one domain. Whereas, FMN is a 'governed conceptual framework consisting of processes, plans, templates and capability components to plan, prepare, instantiate, use and terminate mission networks in support of Alliance/Multi-National operations in dynamic federated environments' (ACT, 2012). Since FMN is still at its development stage, we foresee that the practical and innovative federation of capabilities approach, proposed later in this paper, been a significant contribution to the final FMN concept.

The Multiple Futures Project (MFP) addresses NATO longer term challenges. General J.N. Mattis (USA) said ' The project aimed to strengthen our understanding of the Alliance's future threat environment through rigorous analysis of emerging security challenges...The security implications and resulting recommendations contained in the report will provide a solid foundation from which we can build a common understanding of the nature of the risks and threats facing the Alliance and our populations' (ACT, 2009).

From a NATO capabilities point of view, the NATO Air Command and Control System (ACCS) LOC1 programme is key to NATO common funded success. 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 including Ballistic Missile Defense (Lisbon & Chicago Summits). ACCS consists of deployable and fixed entities interoperable with hundreds of well-defined external NATO and national interfaces within almost all European NATO nations. In specific terms, the paper is intended and in support to the NATO Air and Missile Defence System (NATINAMDS) capability planners and decision makers. And in general terms, the paper's audience is the NATO Defence Planning Process (NDPP) stakeholders.

This paper's aim is to illustrate an innovative strategy aligned with NATO responses to unexpected environment and mission/operation changes. An ACCS prototype is taken as the case study to illustrate the capability gateway based federation strategy, as developed later in the document. The strategy supports NATO responses to changes by addressing the 'unexpected' technical interoperability challenges (Mutambaïe & Finney, 2011). Finally, the paper's benefit is to report on a successful strategy that could be implemented and reused in the short, mid and longer term within the NATO-led operations.

2. Innovative Approach and Methods Employed

This section describes the innovative strategy that addresses the "unexpected environment situation changes". The strategy accommodates all sizes of contributions to the overall NATO capability in coalition. From a C2 perspective, the aim is to be technically interoperable with unexpected capabilities, including non-military entities, and to develop an enduring strategy that will enable new technology and concepts (Mutambaïe & Finney, 2011).

2.1. Innovative Approach

The Enterprise Service Bus (ESB) federation strategy, as described later in this section, is a user-centered (democratized) innovation (Von Hippel, 2006). According to Von Hippel, innovation and diffusion paradigms, the strategy could be possible because of two combined lead user innovations.

1. In 2006, staffs working in the NATO agency that is procuring the ACCS developed the ESB strategy for their own in-house use in Brussels HQ. They needed, in equal measure, to demonstrate the easy convergence of the ACCS to NNEC (by implementing agile and inexpensive Service Oriented Architectures (SOA)) and to capture new requirements for the evolution of the ACCS. The innovative strategy was to use commercial gateways called ESB[1], to smartly connect ACCS to undefined external interfaces, and to enable ad-hoc information sharing.
2. In 2010, ISAF commander Gen S.A. McChrystal, in his effort to overcome situation awareness, interoperability and security cross domain information sharing issues, decided that all ISAF capabilities must move to a common network; to more effectively share information and resources across Afghanistan. This strategy promoted an innovative way to operate in coalition, whereby; all participants could share information in the same domain.

[1] Within the paper, COTS ESBs have the following characteristics;-provide interoperability between capabilities at Service InterOperability Point (SIOP) level; Are standard based and support many transport mediums; Are not necessarily web service base; Provide an abstraction for endpoints.

2.2. ESB Federation Strategy

Hypothetically, the federation is characterized by the fact that each ESB owner is responsible for their capabilities interoperability, effect, visibility, security and governance. To set up the ESB federation strategy, agility is the key, combining joint action and self-governance (King, 1982).

From a SOA perspective, the strategy is to federate all ESB initiatives and allow NATO capabilities, within a coalition, to flexibly share services and to maintain information superiority. In such complex environments, some services may be shared or only reused within a single domain, while others may be shared or reused through the enterprise (IBM, 2009). For the purposes of this paper, the pattern concept is used to describe approaches and practices that can be shared in an ESB federation strategy. A pattern is a documented and repeatable solution to technical interoperability challenges located at the SIOP[2] within their respective service granularity levels.

2.2.1. Coarse Grain Strategy

Topologically, an ESB federation can be recognized 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 within the federation. From a capability perspective, the fractal theory on networks and its self-similarity properties helps to illustrate the different ESB federation strategy' granularities

Figure 1 (in annex) depicts the architectural network concept and fractal patterns (coarse grain) overseen for a federated ESB strategy from an ACCS perspective. The self-similarity is characterized by four similarity elements recursively connected to the ESB in an irregular way as described in Table 1. The four similarity elements are: visibility; Security; Required information and the ESB. One or multiple similarity elements can connect to an ESB. When they are connected to an ESB, the reusable similarity elements contribute to an ESB pattern. The ESB federation strategy is a composition of efficient ESB patterns (or profiles) addressing technical interoperability challenges. More than a profile, the ESB federation strategies and related patterns are dynamic and are evolving according to coalition environment parameters.

Unexpected environment parameter changes must be taken into account when deploying an ESB federation strategy.t of. Such changes provide the strategy boundaries and generate its irregularity of patterns. Specifically, the unexpected environment parameter changes in NATO-led coalition considered are:

a) Operations, threats, objectives or mandate changes.

b) Stakeholders, coalition participants.

c) Technology availability in situ.

[2] Service Interoperability Points define the boundaries at which the various services actually interact

d) Interoperability targets.

e) Time (mission/operation duration, instantiation, timeframe, termination).

2.2.2. Fine Grain Strategy

Figure 2 illustrates the ESB federation strategy (fine grain granularity) from a similarity element (applications/services/ESB) perspective. It represents the ESB federation strategy life cycle and the four possible states of a similarity element when (dis)connecting to an existing ESB node (e.g. ACCS and its ESB). Therefore, figure 2 combined with table 2, provide generic technical implementation instructions to instantiate, use and terminate the ESB federation strategy. The (dis)connectivity requirement is driven by the actual coalition environment parameters. Each state is generated by a change (unexpected or not) in the coalition environment parameters. Therefore, the identified change leads to an associated Information Exchange Requirement (IER) specification process and, a SOA implementation cycle.

Several (fractal) patterns are possible when implementing an ESB federation strategy, but the aim is to implement the most effective pattern addressing the environmental changes. The SOA implementation cycle, for a similarity element connection to the ESB federation strategy, can follow any one of the three different SOA implementation categories identified in table 3 (Afshar, 2007): Project-driven, Infrastructure-driven and Enterprise-driven. Eventually, the ESB federation strategy could lead to different competitive patterns. Usually, governance principles (selection of similarity elements relations, competition, coexistence or obsolescence) need to be applied when competitive patterns are found. At the end, the measure of the coalition information superiority success, describes later in the document, is key to the pattern and ESB strategy selection.

2.3. Case Study

From 2006 to 2009, the authors used case study methods to develop the ESB federation strategy as a grounded theory (Mutambaïe & Finney, 2011). Data collection, analysis and discussion were conducted following Miles and Huberman methods (Miles and Huberman, 1998). OASIS architecture framework for SOA and its reference model were adapted to guide the strategy implementation framework (OASIS, 2009). SOA implementation type developed by Afshar, as shown in table 3, helped to identify and categorize up to twenty SOA projects and compare their performances and governances (Afshar, 2007).

The ESB federation strategy was developed as follows. The ACCS NNEC prototype, that has been produced, was based on the latest ACCS software. It was connected to one or multiple vendor independent ESBs. It was, at therefore, interfaced with capabilities that could not technically interoperate with ACCS. The objective was to quickly and affordably address unexpected environment changes by enabling SOA services in a federated coalition environment as shown in table 4. Every ACCS case study project had an agile development period lasting up to 6 months as soon as the latest ACCS software release was available. Trials and demonstrations were performed in distributed locations such as Belgium, France, Germany, Netherlands, Norway and USA. Trials involved, in a non-exhaustive way, multiple vendors' independent COTS ESBs, NATO operators, prototypes, NATO systems, industry companies and ISAF fielded national systems.

3. Outcomes, KPI, ROI and Conclusion

Table 4 represents the unclassified outcomes of the ESB federation strategy from 2006 to 2009. It reports how ESB federation strategy enabled several agile implementations of services and interoperability between capabilities using different standards. It shows how the dynamic patterns were loosely coupled and how it addresses a large spectrum of unexpected information sharing requirements. The findings will be implemented in current and future capabilities as soon as Minimum Military Requirements (MMR) are formally declared and funded by the relevant stakeholders.

Multiple metrics could be used to measure ESB federation strategy performance. We focused on the coalition information superiority success as a reliable metric that allows us to quickly select/compare different strategies and patterns performance from a commander (or decision maker) perspective. There are 8 Key Performance Indicators (KPI) to measure coalition information superiority success. The indicators are; Operator/coalition participants satisfaction/expectation; Interoperability targets fulfillment; Acquisition cost of ownership/procurement duration/saving/priority; Security/IA; Information visibility/timeless/quality; Technology/infrastructure availability in situ; Pattern reusability/value/standard profile;And Coalition time/deadline/duration.

For each indicator the commander needs to establish meaningful target(s) and select/compare different strategies and patterns performance using a five point Likert scale of 1 to 5(per indicator) as a decision support system (Binmore, 2007). The 8 indicators derived from project success KPIs (Chan & Chan, 2004) balanced with strategic environment parameter and Return On Investment (ROI) indicators when applying smart defense. This provides decisive indications to a commander like hotel stars are facilitative when travelers seek advice on accommodation.

As a result, across the cases studied, the strategies and patterns performances are different from one project to another. It seems that project driven implementation performed less well than infrastructure driven and enterprise driven implementations. Independently of the project size and complexity, the poor performances are mainly attributed to lack of management support and commitment to the projects. On the other hand, there are few coalition federation strategies with which to compare.

The quantified ROIs, when applying smart defense, are identified but not yet set by NATO. In this case, ROIs would be the productivity improvement, the service quality and cost saving on the total cost of ownership due to the ESB federation strategy. It makes room for common funding, it supports incremental fielding of new capabilities and, it reduces testing time and cost. In particular the similarity element joining instructions/connection conditions generates savings on the total cost related to governance and maintenance to be performed by each ESB federation participant on the similarity element they own. Indeed, it reduces time to develop and repeatedly validate new interface for each federation participants. To be ready for the future, there is a need to capitalize on lessons learned, develop patterns and maintain the ESB federation strategy profiles in a repository or STANAG like the NATO Interoperability Standard and Profiles (NISP). The main qualified ROIs are the following: improved information superiority having the right information visible across the federation; higher operator confidence and productivity; more effective prioritization and pooling of capabilities; greater flexibility and comprehensive approach and, finally, better response to unexpected coalition environment changes.

The proposed ESB federation strategy will always save cost and time when connecting NATO forces in coalition. Anytime, the strategy performance can be optimized and quickly measured by decision makers using the proposed KPIs and ROIs. The strategy is definitely a good illustration of NATO smart defense, allowing (within multiple cases studied) common funding, pooling of capabilities and enabling comprehensive approach. Nevertheless, other coalition environment changes remain unpredictable; therefore NNEC security and governance adjustments to the strategy need to be continuously reviewed as required.

These relevant ACCS cases study demonstrated how the ESB federation strategy can address NATO coalition technical interoperability complexity and unexpected challenges. as long as changes go on, other capabilities with less external interfaces and footprint will benefit from ACCS case and easily be able to implement the strategy in current or future NATO-led operations. Another perspective is to reuse the strategy in other civilian domains for challenging business needs.

Annex 1: References, Figures and Tables

References:

1. ACT, AMN Concept, NATO ACT Tidepedia, Nov 2011
2. ACT, Future Mission networking (Food for Thought paper), NATO ACT Tidepedia, June 2012
3. ACT, Multiple Futures Project, navigating towards 2030, NATO ACT, Apr 2009
4. Afshar M., SOA Governance: Framework and Best Practices, May, Oracle Corporation World Headquarters, CA, USA, May 2007
5. Binmore K, Does game theory work? The bargaining challenge, MIT Press, Cambridge, MA 2007
6. Binnedijk & Al, Affordable Defense Capabilities for. Future NATO Missions. Center for Technology and National Security Policy. National Defense University. February 23, 2010
7. Chan A & Chan P.L., "Key performance indicators for measuring construction success", Benchmarking: An International Journal, Vol. 11 Iss: 2, pp.203 - 221, 2004
8. Chicago Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012
9. DND CANADA, The Force Employment Concept for the Army, Canadian National Defense, Ottawa, 2006
10. IBM, WebSphere Enterprise Service Bus, Frequently Asked Questions, USA, June 2009.
11. King , Federalism and Federation, Johns Hopkins University Press, 1 Aug 1982
12. Lisbon Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon, 20 Nov. 2010
13. Miles and Huberman, Qualitative Data Analysis: An Expanded Sourcebook , 1998
14. Mutambaïe A. & Finney D., NATO Network Enabled Capability (NNEC) challenges: why NATO Air Command and Control System (ACCS) might be a good case?, 16th ICCRTS - International Command and Control Research and technology Symposium dodccrp, Québec City, Canada June 21–23, 2011
15. NC3B, NNEC Feasibility Study, AC/322-N(2005)0059, Dec. 2005
16. OASIS, Reference Architecture Foundation for Service Oriented Architecture 1.0, Committee Draft 2, Oct.14, 2009
17. Von Hippel E, Democratizing Innovation, The MIT Press, 2006

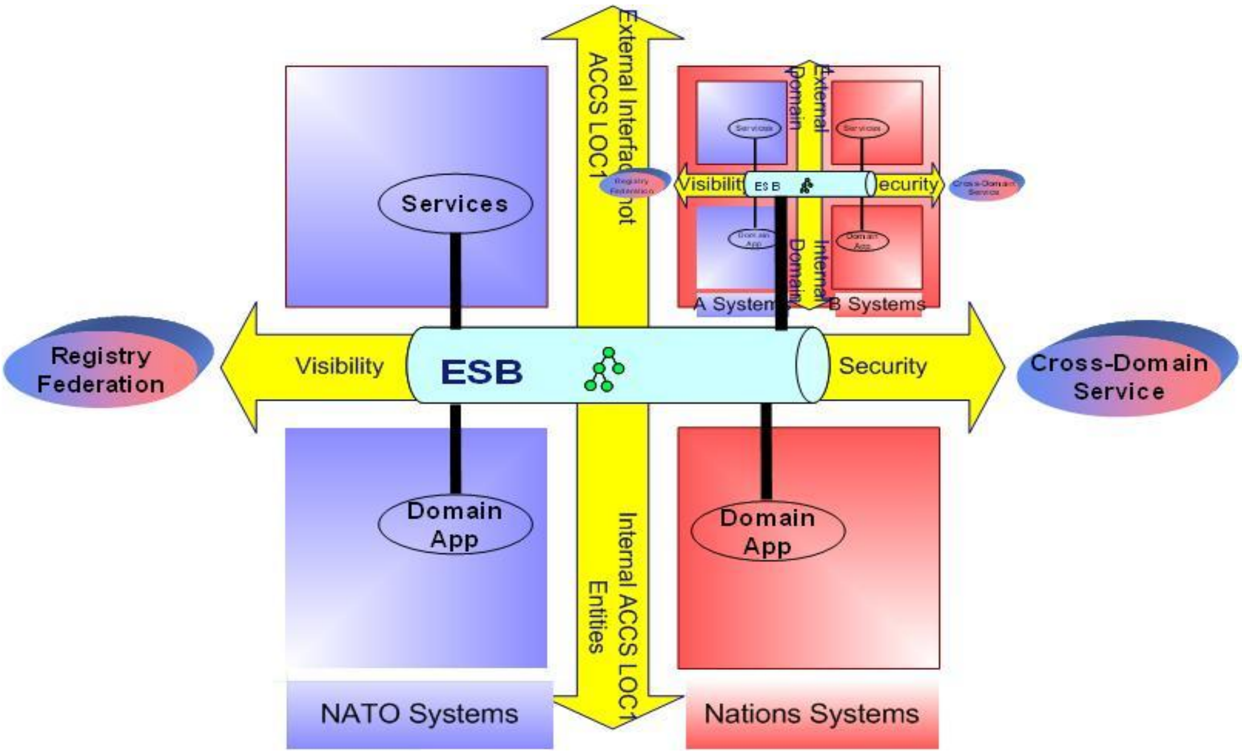

Figure 1: ESB federation strategy pattern (Coarse Grain)

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, Identity Management Service, trust authority, cross domain security guard, auditing & login services
Information Required	Elements that compose the functional services. It is Information Requirement [1] (IR business related) between internal external, national, NATO and ACCS entities/Systems (NSA, 2009)
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 1: Similarity elements description

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

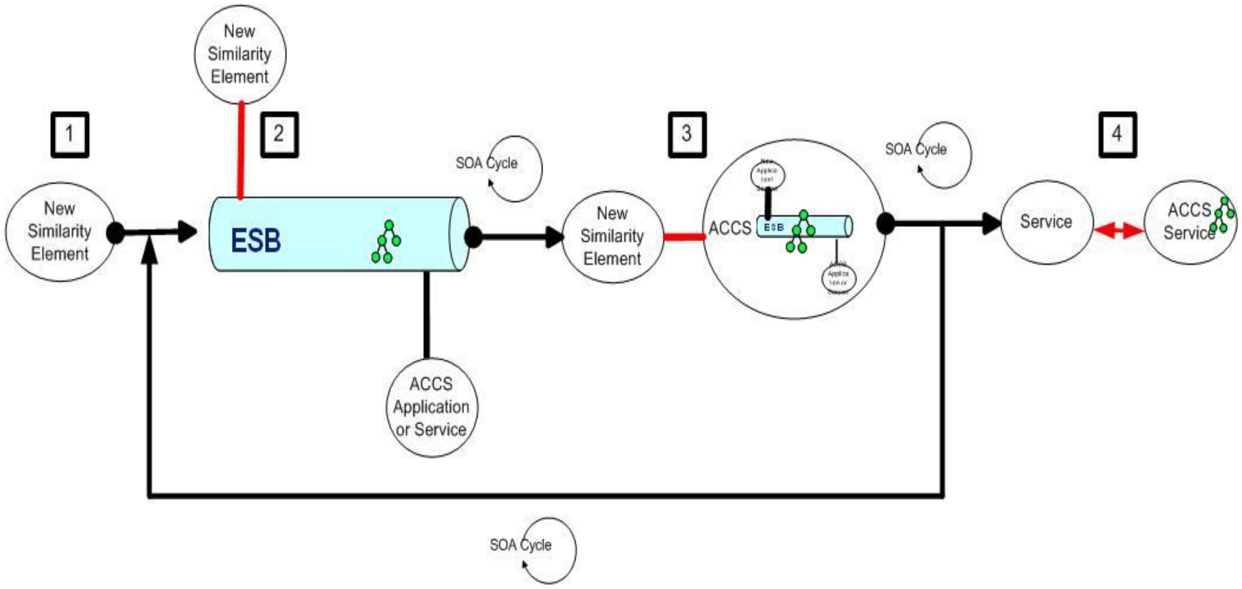

Figure 2: ESB federation strategy life cycle (Fine Grain)

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 2: Similarity element implementation states

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 3: SOA implementation types

Annex 2. 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[2])	• 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 4: ESB federation strategy achievement examples (ACCS NNEC from 2006-2009)

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

Annex 3. 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
AMN	Afghanistan Mission Network
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
FMN	Future Mission Network concept
GNIE	Generic Networked Information Environment
IER	Information Exchange Requirement
IPR	Intellectual Property Rights
ISAF	International Security Assistance Force
J2EE	Java 2 Platform, Enterprise Edition
JC3IEDM	Joint Command, Control and Consultation Information Exchange Data Model.
JRE	Joint-Range Extension
MFP	Multiple Futures Project
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
NATINAMDS	NATO Air and Missile Defence System
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
NDPP	NATO Defence Planning Process
NFFI	the NATO Friendly Force Information
NGCS	NATO General Communications System
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
PKI	Performance Key Indicator
RAP	Recognized Air Picture
ROI	Return On investment
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 5: Acronyms Description