Paper

Success Factors for SOA Implementation in Network Centric Environment

Joanna Śliwa[a] and Marek Amanowicz[a,b]

[a] *Military Communication Institute, Zegrze, Poland*
[b] *Military University of Technology, Warsaw, Poland*

Abstract—This paper discusses challenges and success factors for service oriented architecture (SOA) implementation in network centric environment. The authors identify 9 fundamental challenges for the SOA approach in order to make the biggest benefit for the NATO NEC (NNEC) and increase the mission effectiveness to the highest extent. They cover the areas of applicability to existing military communications and the ability to reflect military processes. Their range is quite broad, pointing out technological as well as SOA governmental problems. The authors emphasize that any COTS solution available on the market today is able to overcome all of them at once. However, they propose solutions to some of the problems and present quick wins that can speed up the process of achieving capabilities in a heterogeneous multinational NEC environment.

Keywords—NEC, SOA challanges, SOA success factors, tactical networks.

1. Introduction

Modern coalition operations are conducted in a dynamic environment, usually with unanticipated partners and irregular adversaries. This new situation has forced the NATO Alliance to pursue the achievement of the so-called "NATO network enabled capabilities" (NNEC) concept, which is the "ability to collect, fuse and analyze relevant information in near real time so as to allow rapid decision making and the rapid delivery of the most desired effect"[1]. The main tenet of the net-centricity is to achieve information superiority by sharing reliable information collected from various sources, creating situational awareness and distributing it among mission participants, across domain, context and organizational boundaries on the basis of extended collaboration.

The NNEC concept, followed in the "NNEC Data Strategy" [2] emphasizes two primary objectives in this process, i.e., the necessity to increase the data that is available to communities in the network-enabled environment; and to ensure that the data is usable by authorized anticipated and unanticipated users and applications. In order to accomplish this goal, the change of focus must take place: from the idea of standalone, stovepiped systems (i.e., platform-oriented) to the idea of shareable, universal information. This would allow unanticipated (but authorized) users to discover information, as opposed to being pushed to them via a pre-defined mechanism.

The improvement of collaboration and information sharing in a highly dynamic, unpredictable NEC environment is a great challenge. It assumes transfer of information with a required quality of service and security, independently of the underlying infrastructure as well as a common access to relevant information by the authorized users. These requirements are to be satisfied by the use of service oriented architecture (SOA), that succeeded in commercial world lately and is recommended by NATO as the crucial NEC enabler [3]–[5]. SOA can make military information resources available in the form of services that can be discovered and used by all mission participants that do not need to be aware of these services in advance.

2. Service Oriented Architecture in the Context of NEC

Service orientation is a conceptual architecture which asymmetrically provides services to arbitrary service consumers, facilitating the information sharing in a heterogeneous environment, and thus supports to some degree the open-ended aspects of net-centricity.

By OASIS definition [6], service oriented architecture (SOA) is "as an architectural paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains". It provides a "uniform means to offer, discover, interact with and use capabilities (as well the ability to compose new capabilities from existing ones) all in an environment that transcends domains of ownership".

The use of service oriented architectures has emerged as a major trend within the commercial sector and among nations developing NNEC type capabilities, because of the flexibility they provide in sharing information and information processing capabilities. SOAs provide mechanisms for using existing information services as well as providing the basis for developing new, more advanced information services. Such mechanisms will allow many command and control processes to be satisfied by linking together existing information sources in a modular, flexible fashion that can be readily adapted to changing operational context. The flexibility provided through the use of SOAs is particularly

[1] Citation from [1].

well suited to support the needs of coalition based network-centric operations using systems of various nations, on different levels of transformation, without the need to replace, but only to integrate them into the SOA environment. The concept is that clients see other servers and applications as "services", accessible using a known and common technology, independently of the underlying implementation of the service (platform – independent approach). In fact, this interaction does not have to be between client applications on user terminals and the servers, but can be between peer applications that relate to each other as a client and a service. This approach allows both user-to-system – and direct system-to-system – interactions that have not previously been generally feasible except by system specific and proprietary implementations.

It is also worth noting that, in a true service oriented environment, developers of services do not know who will access their services at run time. There is a great flexibility in how, when and by whom the services will be used. This idea of "unanticipated users" is a key element of SOA, particularly advantageous in the dynamic NATO environment, where the components of missions change over time and the consumers of services today may not be the consumers of the services tomorrow.

The technological background of NNEC implementation, i.e., networking and information infrastructure (NII) strategy assumes that the NII will be implemented as a federation of systems[2] (FoS), involving the use of SOAs [1], [3], [4], [7]. The NNEC feasibility study [4] has made it clear that the Information and integration services (IIS) layer of NII will be formed by a federation of services, within which any NATO or national information system will be autonomous and will provide specific services by means of implementing a standardized service interface [4].

The most mature implementation of SOAs, recommended by NATO and widely applied in the commercial sector, are web services (WS) and other extensible markup language (XML) technologies. Current trends show great levels of maturity and adoption of these technologies – within the IT industry, within the NATO nations, and within various multinational programs – leading to the belief that this is a direction already being followed and that there is already much force behind it. WSs are described by a wide range of standards that deal with different aspects of WS realization, transport, orchestration, semantics, etc. They provide the means to build a very flexible environment that is able to dynamically link different system components to each other. These XML-based standards have been designed to operate in high bandwidth links. XML gained wide acceptance and became very popular for the reason that it solves many interoperability problems, is human- and machine-friendly and facilitates the development of frameworks for a software integration, independent of the programming language. Nevertheless, it undoubtedly adds significant overhead, both in terms of computation and network resources while being transported.

The value of SOA is though, that it provides a simple scalable paradigm for organizing large systems that require the interoperability to realize the value inherent in the individual components. Moreover, apart from its inherent ability to scale and evolve, the SOA – based infrastructure is also more agile and responsive than the one built on an exponential number of pair-wise interfaces. Therefore, SOA can also provide a solid foundation for developing operational context, based on business agility and adaptability.

The remainder of this paper is organized as described below. Section 2 describes a set of challenges that SOA application in military NEC-centric environment must overcome. They derive both from the architecture itself and from the characteristics of the environment, that must integrate systems owned and governed by different nations/organizations, built by use of different (modern and legacy) technologies, lacking standardization in many areas (e.g., management, cross-domain security, QoS, etc.), and facing disadvantaged communications links. Section 3 presents the SOA success factors that should be taken in order to support dynamic, flexible and scalable SOA – based environment to conduct a net-centric multinational operation. We conclude this paper in Section 4.

3. SOA Challenges

Service oriented architecture, as presented above has a great potential deriving from the paradigm and framework it relates to. It has undoubtedly many benefits, however its

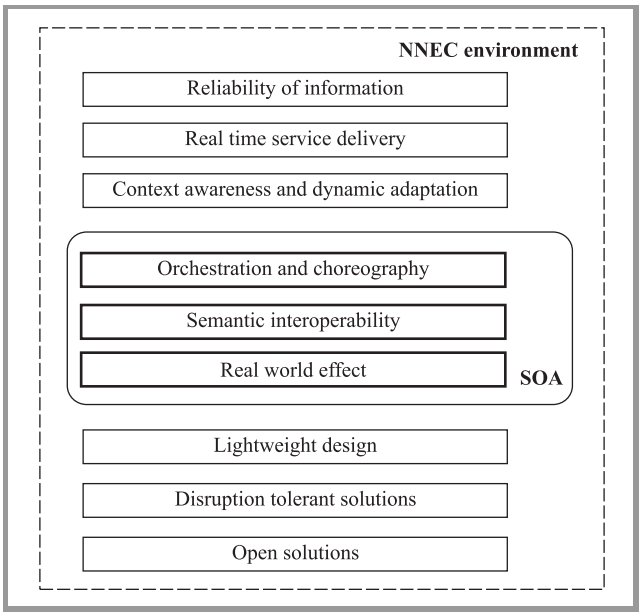

Fig. 1. SOA challenges deriving from the SOA concept and NNEC environment.

[2]Federation of systems – complex environment built of heterogeneous autonomous systems governed independently, taking advantage of cooperation. "*(. . .) formed by the synergistic amalgamation of a dynamic set of globally interconnected, multi-national, autonomous systems, each comprised of networking and information infrastructure components, providing information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information to authorized users on demand, on an end-to-end basis*" [4].

application in a highly dynamic, heterogeneous and disadvantaged NEC environment is a challenge.
This paper identifies 9 fundamental challenges for the SOA approach in order to make the biggest benefit for the NNEC and increase the mission effectiveness to the highest extent (see Fig. 1). They cover the areas of applicability to existing military communications and the ability to reflect military processes. Their range is though, quite broad, pointing out technological as well as SOA government problems. No COTS solution available on the market today is able to overcome all of them at once.

3.1. Real World Effect

A service is a mechanism that enables access to one or more capabilities, based on the use of a predefined interface and exploited consistently with constraints and policies as specified by the service description.
Following OASIS SOA Reference model [6], the main tenets of SOA services are:

- visibility (provided by the service description),
- interaction (described in the service contract and realized between SOA components),
- real world effect.

The first two of them are inherent to the interaction patterns that will exist in the system. However, the last one is strongly related to the business model that exists over the technical model. The design of the SOA services layer must start with identifying business processes that are the heart of the "military enterprise". Only after identifying actors that take part in the net-centric operation and defining the information needs and flows between them, it is possible to create services of a true value to the enterprise.
Business processes are considered to be the basis for developing service oriented architecture [3], [4]. At the national level, it is necessary to initiate activities that are to develop overarching architecture of the C4I on the basis of the service oriented architecture in order to have a SOA – based C4I system that supports creation of the national NNEC. It should integrate new and legacy systems and reflect real user requirements. It is impossible to carry out this process without having previously defined and properly described the operational processes conducted in every moment of a net-centric operation. These actions would lead to development of the service map and service layer based on real information needs.

3.2. Semantic Interoperability

Taking advantage of the wide spectrum of services that will arise in the federation of systems (FoS) built based on SOA, requires that all of the domains connected speak with "the same language" and "understand" each other. Achieving the interoperability in terms of network protocols (e.g., based on TACOMS STANAGS) or data (e.g., based on the NC3A Data Strategy), does not cover all its aspects. It must be ensured that the meaning of terms used by applications in domains owned by different countries, different kinds of military services (land, air, navy) is the same. It is necessary to establish a high degree of correlation and similarity between the details of their respective descriptions and definitions, on which they intend to reach an agreement. This implies that a shared understanding requires shared definitions. It is, though highly recommended to provide ontological models for different domains of the NEC environment within NATO that could be used by every country joining a multinational operation.

The role of ontologies in transformation to NNEC has been emphasized by the NC3A in the NC3A Technical Architecture [7] supplement. It points out that in a dynamic multidomain environment, the goal is to implement semantic web solutions that would enable the users to locate, select, employ, compose and monitor the web services automatically. Ontologies are needed especially in the area of services description, enabling semantic services selection, as well as providing the possibility to employ orchestration and choreography. To make use of a NNEC service, software agents need a computer – interpretable description of that service, and the means by which it is accessed. An important goal for semantic web languages is to establish a framework within which these descriptions are made and shared.

It should be emphasized that for automated tasks of the systems, it is also necessary to provide semantic metadata descriptions needed, e.g., for provision of the quality of service, service level agreement (SLA) support, security, management, etc. What is more, in order to achieve the understanding of data distributed among systems, common data ontologies for domains (e.g., particular communities of interest) are needed.

The application of ontologies and providing foundation for creating the, so called, semantic web, does not restrict itself to the formal semantic description of service resources for machine-to-machine exchange and automated integration and processing. One important feature of formally describing resources is to allow computers to reason by inference. Once the resources are described using facts, associations, and relationships, inference engines, also called reasoners, can derive new knowledge and draw logical conclusions from the existing information.

Sharing information among different systems creates the problem of understanding what the data means. Ontologies and inference services, by expressing the meaning in ontology for the specific data sources and defining the relationships among the different concepts or terms appearing in those apparently different ontologies, are able to perform the data and information integration. Moreover, the application of ontologies provides the possibility of an automated reasoning, semantic search for information, enabling the decision support and advanced searches for information in the SOA environment. It is though, very important to start work on developing domain ontologies en-

abling to provide such information integration. This may be done on the basis of the JC3IEDM model, developed by the MIP community and applied by many NATO countries to provide automated data exchange and replication. It must be emphasized, however, that JC3 is very broad, and not divided into smaller ontologies, would be inefficient to be processed by devices with limited computational resources.

3.3. Orchestration and Choreography

One of the most important advantages of the service orientation is that, it supports, by the use of service reusability, the automation of processes. The orchestration and choreography makes it possible to create new services and arrange them into process flows on demand. Therefore, in order to take full advantage of what SOA brings, it is necessary to provide a high level management of the business processes mapped into services, enabling a dynamic reaction on new information needs, change into business process to create dynamic service environment that flexibly changes in order to meet the information needs. These functionalities that may be built on top of SOA services are getting more and more popular as the amount of work on building ontologies also increases.

In order to support the realization of operational processes' goals, services form a set that can be orchestrated. These orchestrations may be reconfigured differently, when needed, to regain support of an operational process after its ad hoc arrangement has changed to suit new or changed operational needs.

A service orchestration, in general, refers to an executable business process that may interact with both internal and external services, capable of satisfying certain operational objectives that cannot be achieved by any of the services alone. It requires the various composing systems to collaborate in a controlled (orchestrated) manner. Depending on the purpose, it may not be enough to only determine which services are used. It may also be necessary to resolve timing issues, semantic misunderstandings, and the quality of service discrepancies, which may appear when services interact.

Orchestration leads to the emergence of higher level services, where the combined use of services is to deliver a higher level functionality or effect. In case of web services, this creates a composite web service.

On the other hand, choreography is more collaborative in nature. Each party involved in the process describes the part they play in the interaction. Choreography describes a process flow between services and processes themselves and tracks the sequence of messages that may involve multiple parties and multiple sources.

Orchestration and choreography become more and more popular among solutions for semantic search for services, trying to correlate offered inputs and required outputs. More and more often, the search for services bases also on proprietary quality of service descriptions that makes it possible to provide services meeting user preferences, adapted to the possibilities of the network. The utilization of orchestration and choreography together with ontologies, enables to automate many processes realized during the course of the operation and to provide the possibility to gather all the necessary information for the operators involved.

Furthermore, it is necessary to emphasize that the semantic description used on the daily basis in the software applications need to be tailored to the computational resources of that devices. Web ontology language (OWL), most commonly used to express ontologies, is a very expressive language, and enables to perform reasoning over ontologies and infer knowledge that is not explicitly stated. However, the reasoning engines for OWL typically require a lot of resources, and are, therefore, not well suited for resource-limited handheld devices. It has been stated in [3] that in an ad hoc wireless environment utilization of ontologies is possible only when ontologies are small, so that the handheld devices can process them and reason over. That is why creating ontologies need to be carefully carried out, preferably based on one of the commonly applied methodologies (e.g., methontology), acquiring them to the environment where they will be used.

3.4. Open Solutions

Realizing the benefits of the SOA approach will require agreeing on a standardized set of protocols, data formats and foundational (core) services (e.g., covering such areas as service discovery security, metadata management, identity management, service management and mediation), that provide means to establish the interoperability in the technical field. NII is to be formed based on the Internet model, major advantage of which is the use of common set of protocols enabling to create dispersed, dynamic environment for sharing information without central governing authority [3], [4]. In order to take advantage from the success of the Internet, the utilization of open standards that will help to ensure interoperability is necessary.

Obviously, a military environment differs from the Internet in many aspects (e.g., security constraints, policy), so that it will be impossible to adhere only to commercial standards. However, in order to provide coherent NATO – supported coalition network environment enabling to act efficiently in multinational missions, it is recommended to revise the consequences of using open standards and assess the risk that is related to the increased interoperability problems when using some proprietary solutions. There should be also taken initiatives to standardize the mechanisms and protocols that are of great importance to provide a secure and dynamic service-oriented net-centric environment (e.g., cross-domain security solutions, quality of service principles, common ontologies). Such initiatives are taken, e.g., in NATO (by the working groups and other research initiatives provided by NATO Research and Technology Organization[3]) and by Network Centric Operations

[3]More information on RTO web site, http://www.rta.nato.int

Industry Consortium (NCOIC[4]), that plays an important role in establishing a common view of net-centric capabilities and provides technical solutions to enhance the interoperability in a multinational environment.

It is also very important to emphasize the need to create a common technical framework for developing SOA-based solutions that is based on open or agreed standards. This process is carried out, e.g., by the standardization bodies (e.g., OASIS, W3C), but the military environment often requires additional functionalities, not supported by organizations working mainly for the commercial sector. It has been shown in many multinational exercises (e.g., Combined Endeavour CE, Common Warrior Interoperability Demonstration CWID – currently CWIX, MultiNational Experimentation MNE, etc.), that the interoperability is crucial for the mission success in a NATO community. Systems created for the sole purpose of the country (e.g., crisis management systems) must also interoperate with many national systems. The interoperability is though, necessary on many levels. That is why adherence to the open, agreed standards makes it easier to solve the problem on the technical grounding.

3.5. Disruption Tolerant Solutions

The utilization of SOA-based systems in a NEC environment has been shown in many international experiments [5]. They prove that SOA technologies improve the collaboration, interoperation and information sharing in complex environment of heterogeneous systems. However, the NATO concept of FoS relying on the exchange of information implies that communications are of critical importance to the entire (C2) system. In order to achieve an efficient information exchange between the users, the SOA solutions need to work with different types of information and communication systems. The challenge is though, to use this – simple in concept and providing a big flexibility – means of communications on every echelon of command – from the strategic and operational to the tactical and individual soldier's level.

Going down in the command structure, the network environment is getting more and more degraded providing worse and worse communications, e.g. low bandwidth, high level of unpredictability of quality factors, lack of connectivity guarantee, changing topology, radio silence and high error rates. The fragile nature of tactical radio networks requires robust communication mechanisms which current SOA solutions (e.g., mainly enterprise SOA implementations, such as Enterprise Service Buses (ESBs)) do not provide. This includes methods to deal with large delays, communication failures, network splits and merges. It is necessary to provide SOA solutions that enable to integrate network elements on all command levels and a smart communication infrastructure which would deal with peculiarities of the wireless medium. This will allow to create the situational awareness also on the lowest command levels and supply users of the tactical systems with necessary information and decision support.

3.6. Lightweight Design

In order to adhere to the open standards tenet and take advantage of the most common WS-based realization of SOA, it must be ensured that the solutions implemented, originally derived from the commercial world, do not overload the network nor overuse the existing resources (network and terminal ones). SOA solutions, very often based on XML, known from significant overhead it adds, will have to be effective in the whole NEC environment. They should have though, a lightweight design that minimizes the demand on the network and implements a minimum range of functionality.

The requirement for minimum functionality is the most important in the tactical domain, for nodes with a limited memory, storage capacity, processing power and battery life. Such nodes are usually man-portable nodes or sensor nodes powered by battery, where the minimum functionality can also serve the important goal of energy conservation. However, the use of complicated, "heavy" software components on low command levels should be avoided.

3.7. Real Time Service Delivery

The most obvious tenet of net-centricity is the information exchange (see Fig. 2). This capability should, however, be seen not only in terms of what derives from the usual relation between the commander and the subordinate. Looking down to the battalion, platoon and lower levels, apart from regular exchange of formalized messages, operators more and more frequently exchange information horizontally, sharing information within small formations (platoon or squad), e.g., positions, alarms, video streams, pictures and other important elements of building situational awareness at the tactical level. Individual soldiers are often equipped with high-quality sensors and hardware that make them complex technical systems on their own. Each actor engaged in an operation can thus be considered both a consumer and a provider of data. Down the echelons of command, actions are getting more and more dynamic, decision-making time is shorter, so that actors need real-time information. Moreover, the information granularity, low in the military hierarchy, is greater, which means that military staff needs detailed information about their area of operation.

SOA solutions must be applicable to the tactical domain providing the possibility to create common operational picture (COP) on various levels of command. COP created at high command levels, tailored to the needs of the operators and giving them the overview of coalition, neutral and enemy forces, enabling to plan and conduct operation in real time, should be also achieved at the lowest levels including the individual soldier. This would support creating shared situational awareness and enable military staff to make reliable decisions in a short timeframe, work to-

[4]More information on NCOIC web site, https://www.ncoic.org/home/

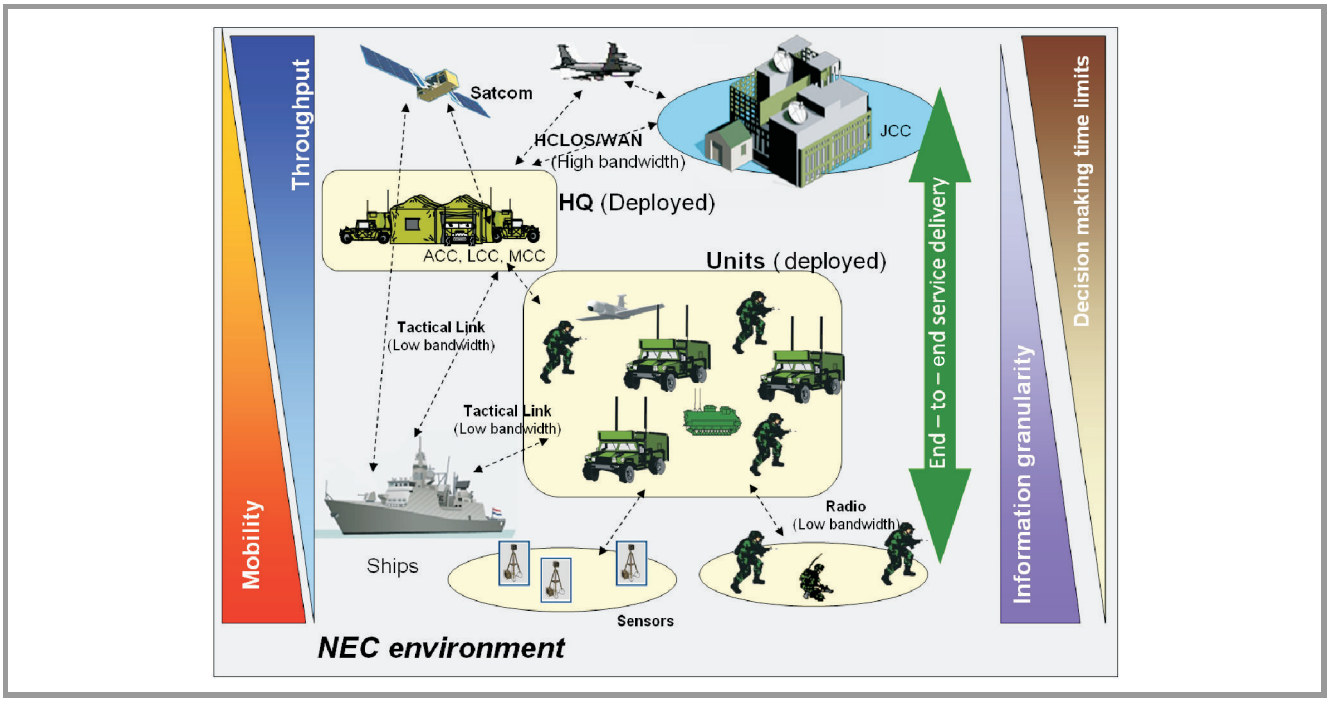

Fig. 2. SOA application in NEC environment on different command levels.

gether in new, more effective ways and thus, to improve the speed of command, leading to a dramatic increase of mission effectiveness.

It is though necessary to provide technical means to realize services in real time. This includes messaging mechanisms that do not necessarily base on web services often considered not well applicable for real time requirements but provide good efficiency in disadvantaged networks and enable the realization of time-constrained services.

3.8. Context Awareness and Dynamic Adaptation

SOA, as an architecture covering the whole FoS will be used (obviously depending on the level of transformation particular systems acquire) to integrate all connected systems. In order to adhere to different types of communication networks and meet the requirements of users on every command level, SOA solutions must be "aware"of the context of the service call. Middleware layer of the SOA should though, maintain a shared perception of the network state. In order to do so, it should serve as a mediator for collecting, organizing, and disseminating relevant context information to the upper layers (application) and lower layers (transport mechanisms). The context may be also used for selecting the best service realization mode and can include device, network characteristics, service and user activities and requirements. It can characterize static elements that can be defined before a service call is executed, as well as dynamic elements that depend on the type of request, type of response and temporary network QoS parameters.

The solution to this problem, related to providing interoperation with other layers of the architecture, should enable realizing SOA services in a constrained environment and facing another challenge, which is to provide the possibility to adapt to environment limitations.

There are no standard solutions that provide the possibility for SOA to adapt to limitations of the underlying network. However, this problem is crucial in terms of SOA success in a military environment. In order for the services' layer to be responsive and provide dynamic access to information for the users that change their location, privileges and activity during the course of the operation, SOA solutions must provide end-to end service delivery in the horizontal and vertical dimension of the NEC environment. This derives the necessity of dynamic service discovery based also on the user/service requirements, QoS needs and geo-location, as well as the provision of technical solutions that enable SOA to adapt to current network situation.

SOA middleware should have the ability to recognize changes to its execution context and to adapt its behavior appropriately. An example would be:

- an adjustment of services provided to an application (e.g., reduction in frame rates for a real-time video streaming application), based on middleware awareness of reduced network throughput,
- providing the possibility to realize the service in a different pattern (e.g., peer-to-per instead of client-server in case of central server unavailability), and deliver messages when network is degraded, or
- searching for services in the surrounding of the user in case of service registry unavailability.

3.9. Reliability of Information

Mission – critical systems that support NEC operations these days are to deliver appropriate, fused and processed information in the right time. They assume that the infrastructure enables to appropriately deliver binary data. The problem SOA brings in terms of QoS is related not only to the quality of service that covers the mechanisms on the physical, network and data/object levels, but to the reliability of information provision that relates to the reliability of information sources, trustworthiness of data from that sources, support for using the information and supporting the realization of procedures, processes, strategy and doctrine, quality of information and quality of operations as well.

In terms of security, it is necessary to provide appropriate identity management together with the common understanding of privileges, access rights, as well as an agreed security policy. The solutions must enable to identify the users from different domains, appropriately handle their access rights and authorize to appropriate network/information resources according to the valid national security policy. The problem tackles the need for cross-domain handling of the public key infrastructures (PKIs), certificate chains, digital signatures supporting the process of authentication, authorization, messages integrity, non-repudiation, privacy, etc. This is particularly important in terms of the dynamic nature of NNEC environment and the main SOA tenet of common access to relevant information by the unknown but authorized users.

In terms of web services, the most commonly used OASIS WS security (WSS) [8] standard addresses message security and focuses on credential exchange, message integrity, and message confidentiality. It is possible to integrate it with XML digital signature (DSIG) [9] (e.g., using X.509 certificates), and support a cross-domain authentication using existing security standards, such as security assertion markup language (SAML) [10]. This is a good foundation for SOA security in NEC environment, however the interoperability tests prove a gap existing in requirements in terms of obligatory elements included in the WS-security part of the SOAP message or SAML assertion.

4. Potential Solutions

The challenges presented in Section 2 can be met by different solutions. There is no complete product that can be used for that purpose, but there exist some smaller good practices and solutions that should be perceived as quick wins and make a good technological step forward.

NATO started its way towards the transformation by defining the NATO NEC (NNEC) feasibility study together with the roadmap, and foundation of the project. Some countries followed this idea carrying out their own studies, reflecting the challenges in terms of both technology and personnel. This has been done, e.g. by the Swedish Armed Forces [11] that defined the overarching architecture [12] and solid foundation for SOA implementation in their systems, as well as for integration of the legacy systems and their transformation towards full SOA [13]. Coherent introduction of service oriented architecture into currently employed and new systems can only be based on previously defined reference architecture of the C4I system and real information needs resulting from the planned operational scenarios.

In order to maximize the gain from linking the needs with capabilities, the role of business processes as a basis for developing service oriented architecture has been pointed out in [3] and [4]. The architecture engineering methodology (AEM) – developed by the NC3A algorithm for creating architectures, points out the necessity of creating a model of dependencies between components and applying them to a real operational context, to be sure that the proposed architecture will provide the required operational effect. For the graphical notation of operational process diagrams, the business process modelling notation (BPMN) has been recommended by the NC3A [3].

In the area of the semantic interoperability, there is a strong need to provide coherent and agreed standards enabling to share ontologies, as well as semantic descriptions of metadata and data itself. Achieving the interoperability on the semantic level requires the involvement of multinational activities that enable to agree on ontologies, proposed to be used in interdomain relations. Any proprietary solutions in this area will be unsuccessful unless other nations and systems developers agree on using them. The first step to provide semantic interoperability in a heterogeneous environment, is to develop a common semantic description of services for dynamic semantic search and adaptation purposes. This may be done using, e.g., more and more popular OWL-S. Semantic search engines by means of explicitly defining the semantics of the sources and by providing a relationship among terms (like a taxonomy) – can provide, e.g., a concept-based search. For information discovery, depending on the user preferences or the type of user, the system would be able to group the possible results that matched the query or refine the result list by filtering those that are of interest to the target audience. On the basis of semantic services descriptions (e.g. using OWL-S), semantic service discovery is able to provide results tailored to the user preferences, QoS, etc. as well as support orchestration and choreography.

The effort for providing ontologies for the NATO has been taken by the TIDE[5] (technology for information, decision and execution superiority) community, that aims to rapidly improve the operational capabilities through iterative processes based on horizontal and vertical integration of existing and emerging products. Within its framework, it stimulates coexistence of NATO and national programs and services providing proposition of standards embracing service oriented architectures and discussing them during regular meetings (so called TIDE sprints). It has proposed the service and information dis-

[5]More information can be found by the authorized users on the TIDE web site http://tide.act.nato.int/tidepedia/index.php?title=TIDE

covery protocols (for request-response and publish subscribe modes) used, e.g., within the NATO MSA community in BRITE and other national solutions (e.g., finish MEVAT system). So far, it has also delivered 33 ontologies used by different TIDE focus groups (e.g., MSA, SUCBAS, NIRIS etc.), based on RDF/RDFS and OWL. There are, e.g., subscribe-publish ontology, location ontology, symbology ontology (for APP6A and MS2525B visualization symbols), JC3IEDM ontology and many others.

The conceptual framework developed within the TIDE initiative describes how the network enabled capabilities will transform raw data into intended effects, and how they support achieving NATO's transformation goals and objectives. The effort TIDE members put into technology development has been used also in real life scenarios (e.g., in the BRITE system for creating NATO Maritime Situational Awareness – MSA). This should be continued and followed by other existing and possibly new teams that would support the interoperability on the data and metadata level, also using ontologies.

Another big step forward in SOA implementation is to put it into operation at the lowest command levels. According to the NEC principles and modern command processes, military operations are conducted in a dynamically, very often based on the "mission command" pattern. Low level commanders need to be aware of the possible consequences of their decisions. This makes it necessary to provide users down to the individual soldier level with the possibility to use the information systems and feed them with information crucial for the mission effectiveness.

The most common realization of the SOA environment is based on web services. In order for the operators to use the information from sources located on high command levels, web services realization must be made reliable and it must be adapted to the characteristics of the network.

It must be noted that there are no commercial works on applying SOA and web services in disadvantaged grids. There have been undertaken a few initiatives that focused on the information distribution over disadvantaged grids. In very low bandwidth environments the use of asynchronous replication based middleware, provides static information distribution between partners that have agreed to use a specific database format [14]. This solution is, however, not very convenient for a highly dynamic operational scenario. For this reason, there have been carried out researches on WS-based SOA solutions that provide the flexibility and interoperability, and are well suited to work in federation of systems. The NATO C3 Agency (NC3A) report on using WS in tactical domain [15] concludes with a statement that web services remain promising even in low bandwidth links, as long as very fast response times are not required. Other interesting works on this subject have been carried out in Norwegian Defense Research Establishment (FFI) in Norway [5], [16]–[19]. These projects focused on applying mechanisms that diminish XML-based disadvantages of WS and experiment on new transport protocols instead of SOAP/ HTTP (hypertext transfer protocol), e.g., data distribution service (DDS) or message handling system (MHS).

Data-rate constraints in tactical networks impose great challenges that have to be faced in order to fully deploy SOA supporting NEC. There are several solutions that can be applied to adapt SOA web services mechanisms to the capacity of the systems at various C2 levels. The ones which bring the biggest advantage are compression (e.g., very popular and available in the application servers GZip algorithm), filtering, caching and non-SOAP transport mechanisms.

Two main disadvantages of using XML are as follows: big overhead related to human-readable format of the documents and significant parsing and processing times of the XML-based messages. In [15] there has been shown that XML is very compression-friendly and in many cases, depending on the data set and the size of the message, more than 95% gain can be achieved. This very simple method should be set as a requirement for the use of WS in disadvantaged networks. It must be noted however, that in order not to complicate the interoperability, compression algorithms should be standardized and known by the collaborating parties.

Another very efficient method of limiting XML disadvantages is using its binary form. Generally, it reduces the verbosity of XML documents and the cost of parsing. It can lead, though, to faster document processing and lower memory and central processing unit (CPU) requirements, which is especially appealing on mobile devices.

The filtering enables to limit the amount of information sent to the end user in order to relieve the tactical network from sending heavy traffic. This method is often used for the access control based on XML guards (XML filters), or for providing subscriptions based on the messages content. However, the utilization of this method for WS adaptation to disadvantaged grids is a very complicated matter since it is very difficult to propose very general filter rules that apply to most Web Services, and that can provide the end user with the right set of information that he really needs at that moment.

Some of the filtering functionalities are present it HTTP - like, e.g., requiring only a part of the HTTP page from the server. In force tracking systems [20] filtering may mean sending information about objects that are away from the end user (service requester) by x km creating some kinds of circles of the service accuracy. For provision of still images, it can mean sending the image with the resolution adapted to the end user terminal. For video it may mean decreasing the frequency of frames per second.

HTTP is one of the most popular binding protocols primarily designed to transport SOAP messages. HTTP holds its connection after the SOAP request is sent until the SOAP response is returned in the HTTP acknowledgment. If the connection times out (e.g., because of delays), the SOAP response will not be delivered to the service consumer. Therefore, using HTTP over disadvantaged grids or

a combination of heterogeneous networks may not work very well [17].

According to [15], sending new service requests is much more "expensive" (in a performance sense) than extending the existing ones. For instance, during the HTTP "handshaking" that takes place before each request, a lot of extra traffic is generated each time. Therefore, two 1000-byte requests will take far longer than one 2000-byte request. For the same reason, the performance of HTTP communications, which are made up of sets of data packets, are much more adversely affected by including more packets than more data. In other words, a 20-packet "conversation" equal 1000 bytes will be slower than a 15-packet conversation equal 2000 bytes.

It is a good practice to use a proxy element with a store-and-forward functionality that could cope with the unpredictability of QoS parameters of tactical communications networks, especially in terms of frequent network disconnections. Such an element can provide different transport mechanisms, like data distribution service [21] and military message handling system [18] that have been designed to work in disadvantaged environments. Caching is one of the functions of the proxy element that enables, e.g., storing information that crossed the proxy to be available for subsequent requests. If a user requests the same object, proxy can send it without the need to ask the server again. However, proxy must be able to handle stored information appropriately. This will not work well with short-lived information, that change frequently and information, the expiration of which cannot be assessed. Caching functionality should be placed at the edge of the low-bandwidth network – quite near the end user. It can decrease the network load on the server-proxy path and shorten the time to send the client response. Therefore, the good practice is to keep the frequently used (or infrequently changing) data at, or near the client, so that its retrieval does not impact the network considerably.

Web services compression and filtering can be used in the ultimate sender and receiver of information, however NNEC FS and other NATO documents [22] propose the utilization of edge proxies that provide the possibility to adapt web service realization to the possibilities of the network.

Norwegian Defense Establishment proposes, for that purpose, so called Delay and disruption tolerant SOAP Proxy (DS Proxy) [23] which is able to store-and-forward SOAP messages, compress them and provide prioritization of the traffic. It is placed between a web service consumer and a web service. When the web service is temporarily unavailable (also due to network disruptions), the DSProxy component will cache the Web service request, and retry the invocation at intervals, returning the Web service response when finally successful. The DSProxies can be working in a group. They are self organizing into an overlay network consisting of any number of DSProxy components, based on a mechanism which relies on UDP multicast. This provides the possibility to traverse multiple and heterogeneous networks.

Initial tests have proven that the DSProxy solution is able to bridge heterogeneous networks and offer store-and-forward capabilities. Using TCP and UDP transport protocols, web services were invoked in links with bandwidth equal 400 bit/s and 300 bit/s which is a very promising result.

Another approach presented in [24] assumes a situation when the client needs information, but the access network is degraded and he cannot receive it in a timely manner. In case when the QoS guarantees cannot be met, it is proposed that the client interacts with the proxy mediation service, which is able, on the basis of the current network parameters, to adapt his traffic to the possibilities of the network, and to enable sending it in some other way.

The proxy service aims at delivering web services to the users located in disadvantaged networks and minimizing negative effects of the wireless environment, including:

- Connection failures – due to store & forward capabilities and publish/subscribe approach;
- High delays and low throughputs – due to reduction of the packet size – e.g., compression, binary coding with compression (e.g., using Efficient XML);
- High error rates – due to reliability mechanisms and network monitoring.

When the client is temporarily disconnected from the network, the mediation service can store the data and forward them when it will be available again. The proxy actively interoperates with the service client and service producer, dynamically adapting contents of the XML messages, selecting the best communication means from within the available ones for the specific service call. Characteristics of the service call are described in the context of a call that provides the possibility to make appropriate and the most accurate decision.

The context consists of the user profile (static and dynamic), terminal profile, network profile (dynamic) and service description. All of them are described in OWL files. In order to take appropriate actions, there is also an adaptation ontology that defines all the actions that need to be taken in order to fulfil the user request.

It must be emphasized that for some types of services web service technology in the tactical domain can be replaced with, e.g., DDS middleware (data distribution service), that is a real time publish/subscribe data-centric platform for dynamic distribution of information in real time. DDS has strong and extensive supports for QoS and is used successfully in real life in many European armies.

5. Summary and Conclusions

The challenges and solutions presented in this paper have been gathered based on the available literature on this subject as well as the experience of the authors in SOA application in NEC environment. They show the basic steps in order to support dynamic, flexible and scalable SOA – based environment to conduct net-centric multinational

operation. Briefly, the SOA success factors can be summarized to the list of Quick Win solutions (see Table 1). This set provides a guide of best practices that enable the undoubtedly successful architecture paradigm to be used in highly dynamic and heterogeneous NEC environment that should technically support multinational missions.

Table 1
SOA success factors

1	Develop service layer based on real information needs
2	Provide semantic description of services for dynamic semantic search and adaptation purposes
3	Provide high level management of the business processes mapped into services, enabling dynamic reaction on new information needs, change into business process to create dynamic service environment that flexibly changes in order to meet the information needs
4	Provide low transmission overhead
5	Optimize service realization (minimize the number of interactions between architecture components)
6	Minimize the utilization of end-terminal resources, especially in the tactical domain
7	Provide interoperation of the middleware layer with the transport and application layers
8	Provide the possibility to negotiate a service contract and adapt service realization to available resources
9	Address the security issues by providing cross-domain authentication given local authorization and security policy

The SOA's greatest advantage is that it provides seamless information exchange based on different policies and loose coupling of its components. The use of SOAs facilitates the application and data sharing and provide a flexible mechanism for reusing existing services to enable the development of new, value-added information services [3], [4].

It appears that the service-orientation and SOAs can facilitate the implementation of net-centric capabilities, but by themselves do not guarantee net-centricity. It must be emphasized that even we have seen many of so called – net-centric solutions, like often shown in demonstrations – common operational pictures (COPs), the truth is that current service oriented technology standards and products only support achieving mission effectiveness. It is important that net-centricity is as much a business model or organizational relationship issue as it is a technology one. Many organizations, including R&D institutions, NATO and industry are beginning to address the issue of service orientation across enterprise boundaries, in FoS environment, on all the echelons of command, but still much work remains to be done.

The article points out SOA technical factors that can approach to the success of its application in NEC environment. It is very important to note that only tailoring the SOA design to military environment limitations, management and security constraints as well as operational needs can provide a true benefit of the SOA paradigm.

Acknowledgment

This work was carried out within the project PBZ – MNiSW – DBO-02/I/2007 supported by the R&D funds allocated for the years 2007–2010.

References

[1] P. Bartolomasi, T. Buckman, A. Campbell, J. Grainger, J. Mahaffey, R. Marchand, O. Kruidhof, C. Shawcross, and K. Veum, *NATO Network-Centric Operational Needs and Implications for the Development of Net-Centric Solutions*, vol. 1 of *NATO Network Enabled Capability Feasibility Study*, version 2.0, NATO C3 Agency, 2004/2005.

[2] "NNEC Data Strategy", Headquarters, Supreme Allied Commander Transformation, IS-NNEC IPT, September 2004.

[3] G. Babakhani, J. Busch, C. Dumas, R. Fiske, B. Holden, H. Lægreid, R. Malewicz, D. Marco-Mompel, and V. Rodriguez-Herola, "Web trends and technologies and NNEC core enterprise services", version 2.0, Technical Note 1143, NATO C3 Agency, The Hague, Dec. 2006.

[4] M. Booth, T. Buckman, J. Busch, B. Caplan, B. Christiansen, R. van Engelshoven, K. Eckstein, G. Hallingstad, T. Halmai, P. Howland, V. Rodriguez-Herola, D. Kallgren, S. Onganer, R. Porta, C. Shawcross, P. Szczucki, and K. Veum, *Detailed Report Covering a Strategy and Roadmap for Realizing an NNEC Networking and Information Infrastructure*, vol. II of *NATO Network Enabled Feasibility Study*, version 2.0, NATO C3 Agency, June 2005.

[5] R. Haakseth, T. Gagnes, D. Hadzic, T. Hafsøe, F. T. Johnsen, K. Lund, and B. K. Reitan, "SOA – Cross Domain and Disadvantaged Grids", NATO CWID 2007, FFI-rapport 2007/02301, Norwegian Defence Research Establishment.

[6] C. M. MacKenzie, K. Laskey, F. McCabe, P. F. Brown, R. Metz, Booz, and A. Hamilton, "Reference Model for Service Oriented Architecture 1.0", *OASIS Standard*, 2006 [Online]. Available: http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.html

[7] "NC3A Technical Architecture" [Online]. Available: http://nc3ta.nc3a.nato.int/website/home.asp?msg=logreq

[8] A. Nadalin, C. Kaler, R. Monzillo, and P. Hallam-Baker, "Web Services Security: 4 SOAP Message Security 1.1 (WS-Security 2004)", *OASIS Standard Specification*, 2006 [Online]. Available: http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

[9] M. Bartel, J. Boyer, B. Fox, B. LaMacchia, and E. Simon, "XML Signature Syntax and Processing (Second Edition)", *W3C Recommendation*, 2008 [Online]. Available: http://www.w3.org/TR/xmldsig-core/

[10] E. Maler *et al.*, "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V1.1", *OASIS Standard*, 2003 [Online]. Available: http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf

[11] O. Winberg, "SOA for NBD: principles and considerations", Försvarets Materialverk, 2006.

[12] O. Winberg, "Overarching architecture for FMLS 2010 technical system", Försvarets Materialverk, 2006.

[13] O. Winberg, "Deign Rule: legacy integration", Försvarets Materialverk, 2006.

[14] "Information Management over Disadvantaged Grids", Techn. Rep. RTO-TR-IST-030, AC/323( )

[15] J. Busch, "An investigation into deploying Web services", TN–1229, NATO C3 Agency, Dec. 2007.

[16] R. Haakseth, D. Hadzic, K. Lund, A. Eggen, and R. E. Rasmussen, "Experiences from implementing dynamic and secure web services", in *Proc. 11th ICCRTS*, Cambridge, UK, 2006

[17] T. Hafsøe, F. T. Johnsen, K. Lund, and A. Eggen, "Adapting web service publish/subscribe technologies for use in NEC C2 Systems", in *Proc. 12th ICCRTS Conf.*, Newport, USA, 2007 [Online]. Available: http://www.dodccrp.org/events/12th_ICCRTS/CD/Launch_CD.html

[18] F. T. Johnsen, A. Eggen, T. Hafsøe, and K. Lund, "Utilizing military message handling systems as a transport mechanism for SOA in military tactical networks", in *Proc. IST 083 Symp.*, Prague, Czech Republic, 2008.

[19] K. Lund, A. Eggen, D. Hadzic, T. Hafsøe, and F. T. Johnsen, "Using web services to realize service oriented architecture in military communication networks", *IEEE Commun. Mag.*, Oct., pp. 47–53, 2007.

[20] "Interim NFFI Standard for Interoperability of FTS", AC322(SC5)N(2006)0025, NC3B Information Systems SC, 16 Dec. 2006.

[21] "Data Distribution Service for Real-time Systems Version 1.2", OMG Available Specification, Jan. 2007.

[22] R. Faucher, R. Ladysz, D. Miller, S. Musman, S. Raparla, and D. Smith, "Guidance on proxy servers fpr the tactical edge", DoD C3I FFRDC, The Mitre Corporation, Sept. 2006.

[23] E. Skjervold, T. Hafsøe, F. T. Johnsen, and K. Lund, "Delay and disruption tolerant web services for heterogeneous networks", in *Proc. MILCOM*, Boston, USA, 2009.

[24] J. Śliwa and D. Duda, "Adaptive web services supported by Qos IP network", in *Proc. Military Commun. Inf. Syst. Conf.*, Prague, Czech Republic, 2009, pp. 448–456 (MK-291).

Joanna Śliwa was born in 1979 in Warsaw. She graduated from the Faculty of Electronics and Information Technology of Warsaw University of Technology (2003). At the moment she is a researcher in Military Communication Institute in Zegrze, Poland. She is working on her Ph.D. in the area of efficient realization of web services in disadvantaged networks. Her main areas of interests are: new telecommunication technologies, Service Oriented Architecture, Network Enabled Capabilities and QoS provisioning.
e-mail: j.sliwa@wil.waw.pl
Military Communication Institute
Warszawska st 22A
05-130 Zegrze, Poland

Marek Amanowicz was born in Poland in 1946. He received M.Sc., Ph.D. and D.Sc. degrees from the Military University of Technology, Warsaw, Poland in 1970, 1978 and 1990, respectively, all in telecommunication engineering. In 2001 he was promoted to the professor's title. He was engaged in many research projects, especially in the fields of communications and information systems engineering, mobile communications, satellite communications, antennas and propagation, communications and information systems modeling and simulation, communications and information systems interoperability, network management and electronics warfare. He is an author or co-author of over 200 scientific papers and research reports.
e-mail: marek.amanowicz@wat.edu.pl
Military University of Technology
Faculty of Electronics
Gen. Sylwestra Kaliskiego st 2
00-908 Warsaw, Poland
e-mail: m.amanowicz@wil.waw.pl
Military Communication Institute
Warszawska st 22A
05-130 Zegrze, Poland