18th ICCRTS

Title of Paper

IST-118 – SOA recommendations for Disadvantaged Grids in the Tactical Domain

Topics

Topic 7: Architectures, Technologies, and Tools

Topic 5: Experimentation, Metrics, and Analysis

Topic 3: Data, Information and Knowledge

Name of Authors

F.T. Johnsen, T.H. Bloebaum, Norwegian Defence Research Establishment (FFI)

P.-P. Meiler, TNO, Netherlands

I. Owens, Cranfield defence academy, UK

C. Barz, N. Jansen Fraunhofer FKIE, Germany

Point of Contact

Frank T. Johnsen

Norwegian Defence Research Establishment (FFI)

P.O. Box 25

NO-2027 Kjeller

Norway

E-mail: Frank-Trethan.Johnsen@ffi.no

IST-118 – SOA recommendations for Disadvantaged Grids in the Tactical Domain

Abstract

Service Oriented Architecture (SOA) can enable agile C2 functionality. The flexibility and loose coupling offered by the SOA paradigm means that both NATO and many of the NATO nations are basing their future information infrastructures on this paradigm. Web services, the most common and mature technology for implementing a service-oriented system, will inevitably be a part of this development, at least for use in fixed infrastructure networks. SOA, realized using Web services technology, is currently available at the higher levels of command such as (deployed) headquarters, but not necessarily at tactical levels. However, SOA is a proposed paradigm for delivering C2 at the tactical level.

IST-118 is a recently started research group intended as a follow-on to IST-090. IST-090 identified several challenges related to applying SOA at the tactical level, in particular disadvantaged grids (communication grids that are disadvantaged by line-of-sight connections, low bandwidth, intermittent availability, etc.). In this paper, we summarize the important findings of IST-090, and outline the program of work for the IST-118 group where the goal is to create a recommendation for a tactical profile for using SOA in disadvantaged grids.

1) Introduction

The Service Oriented Architecture (SOA) approach has been chosen by the NATO C3 Board as the recommended method to achieve information interoperability in NATO. Especially, service-orientation can help increase the level of interoperability for the NATO C4ISR and NEC areas. However, Web services technology was originally designed for civil use over robust, high-bandwidth networks, and it was not clear that it could properly function in the deployed military environment which suffers in many instances from inadequate or unstable connectivity. This fact remains a major impediment to achieving interoperability among the nations in the battlespace.

The IST-090 Task Group's primary objective was to identify challenges and show how to make SOA applicable at the tactical level, which typically included communication over disadvantaged grids [1]. Disadvantaged grids are characterized by low bandwidth, variable throughput, unreliable connectivity, and energy constraints imposed by the wireless communications grid that links the nodes [2].

The results of IST-090 created an awareness of the challenges related to extending a SOA to tactical networks and provided some possible solutions. The results also demonstrated that SOA can work at lower levels than previously thought. Evidence of this is found in the Data Distribution Service (DDS) demonstration by ESP as part of the IST-090 program [3], and in the final two IST-090 demonstrations by DEU [4] and NC3A, NOR, and POL [5], both at the Military Communications and Information Systems Conference (MCC) in 2011.

A key principle when building a service-oriented system is the use of standards in order to enable interoperability between domains. However, while basing system interaction on standards enables interoperability, it does not ensure it. This is because most standards contain optional features, allow several different approaches to solve a problem, might contain ambiguities, and leave a number of details up to the implementation. This means that while the standard can form the basis for interoperability, additional specifications of how one intends to use those standards are needed. Such specifications are often referred to as profiles.

For Web services technology, the Web services interoperability organization (WS-I) has published a number of interoperability profiles. These profiles give best practices for how to implement interoperable Web service based systems. NATO has, through the Core Enterprise Services (CES) Working Group, defined a number of core services that are needed in order to build a NATO-wide service-oriented federation-of-systems. They have published a SOA Baseline [6] document, which acts as a first step towards an interoperable service architecture by identifying which standards should be used to interface between NATO nations, and recommend which WS-I profiles and profile versions to adhere to. The recommendations outlined in the SOA Baseline are mostly focused towards use in wired networks, and do not specifically address the limitations of tactical networks.

Adapting Web services technology to make it suitable for disadvantaged grids will often require solutions that differ from those used in wired networks. It is however important to ensure that one retains the ease of interoperability that the use of Web services technology gives. In many cases the same standards can be used, but it might be necessary to use them in a different way than in wired networks. The goal of IST-118 is to provide guidance and best practices on how to make SOA applicable at the tactical level, in the form of a *Tactical SOA Profile*.

2) Important findings: IST-090

IST-118 builds on the findings from IST-090, which focused on SOA challenges for real-time and disadvantaged grids. The aim of IST-090 was not only to identify the challenges that arise when one applies the service-oriented paradigm in limited capacity networks, but also to suggest technical modifications that can be used to overcome those challenges. IST-118 expands upon the findings of IST-090, and aims to provide guidance on which technical modifications that should be utilized in a number of different types of disadvantaged grids.

The objective of IST-090 was to identify improvements to make SOA applicable at the tactical level, which typically includes communication grids that are disadvantaged by line-of-sight connections, low bandwidth, intermittent availability, etc. The goal was also to investigate how SOA could be used over disadvantaged grids and to build demonstrations that show how the challenges that are posed by disadvantaged grids can be mitigated.

2.1 Technologies for realizing a service oriented system

In IST-090 we focused on Web services as the key enabling technology for network centric operations. Initially the technology was identified by the NATO NEC feasibility study (NNEC FS) [7], and later the SOA baseline was specified using Web services standards [6].

Apart from the need to employ *interim solutions* [4] as a stepping stone on the way towards complete SOA support, we identified three possible approaches to extend SOA to the tactical domain:

1. Employing other technologies in certain sub-systems, and then integrating these with Web services through the use of gateways.
2. Adapting existing Web services standards for use in disadvantaged grids.
3. Employing other technologies in the entire information infrastructure.

In IST-090 the two first approaches were both investigated, as we both adapted Web services for use in disadvantaged grids, and used DDS together with a DDS to Web services gateway in a sub-system.

Because of the inherent interoperability benefits of basing a tactical service-oriented information infrastructure on Web services, the upcoming efforts in IST-118 will focus mainly on this technology. Below we summarize the findings from IST-090 that are relevant for the continuing work in IST-118.

2.1.1 DDS: Alternative to Web services in certain sub-systems

DDS is a standard based publish/subscribe middleware that focuses on providing support for Quality of Service (QoS) and real-time systems. These properties make DDS an interesting alternative to Web services when attempting to extend the SOA paradigm into tactical networks.

The DDS standard for exchanging messages ensures that different vendor implementations are interoperable. However, this standard is not efficient enough in disadvantaged grids, so different vendors implement different so-called tactical extensions. These extensions are proprietary optimizations of the communications protocol and they are not interoperable, leading to vendor lock-in.

In October 2010, the Spanish MoD, in cooperation with industry partners, demonstrated the use of DDS for military purposes. Spain had prepared a live demonstration in their lab facilities showcasing their vision for the future Spanish SOA infrastructure [3]: Using Web services in conjunction with DDS, where DDS was used in the disadvantaged grid.

The demonstration successfully created interoperability among several legacy C2 applications from different vendors. An interface was created to link two different SOA paradigms: Web services and DDS. This interface connected to the two technologically different SOA environments, enabling sharing information between them. It was a first step in solving the problem of interconnecting incompatible technologies, as well as sharing information among different operational levels (tactical and brigade).

In [8], results of the study on the exchange of data between Web services and DDS using a WS-DDS interface are presented. The WS-DDS Interface connects two architecturally different message exchange solutions dedicated for two different environments, and enables bi-directional traffic between WS and DDS, with regard to the timeframe of the protocol and data transformation, which is a very important success factor in a mission.

2.1.2 Adapting Web services for disadvantaged grids

The most common and mature technology for implementing a SOA is Web services, and many nations are already adding support for this technology in their information systems and infrastructures. By extending this technology into the tactical domain, interoperability with other systems is retained.

Web services promote interoperability between different systems, but at the same time they increase the information overhead significantly, resulting in higher data rate demands. In corporate networks this is not much of an issue, since bandwidth is abundant, but the situation is different for radio systems in military tactical networks. In IST-090 we considered methods to reduce the XML and Web services overhead, in order to make it possible to use Web services in tactical networks. To reduce the overhead, we can try to optimize the application by reducing its need to transmit data. Furthermore, we can try to reduce the overhead of SOAP, the Web services messaging standard. Since SOAP is transport protocol agnostic, we can also attempt to replace HTTP/TCP with other protocols. See Figure 1 for an overview of the optimizations that we considered in IST-090.

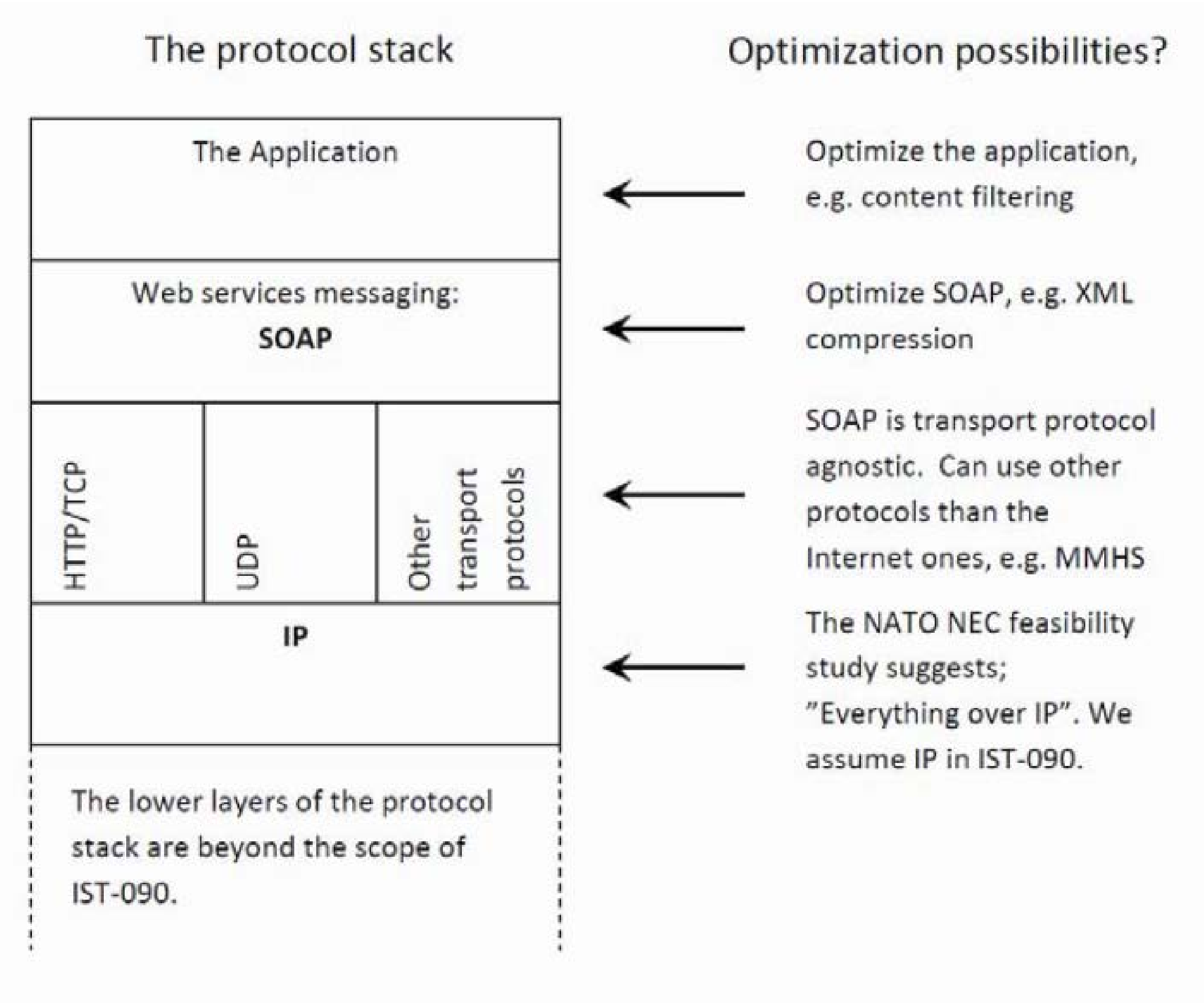

Figure 1: Optimizing the Web services stack (from [1])

We have identified three areas that need to be addressed:

1. Remove the dependency on end-to-end connections

   Attempting to establish and maintain connections in a disruptive environment can lead to increased communication overhead and, in the worst case, a complete breakdown of communication.

2. Address network heterogeneity

   There are several types of network heterogeneity. Networks can be heterogeneous with respect to the technology used to realize the information exchange, and in this case a bridging mechanism is required. When connecting a tactical communication infrastructure to a wired network, one also has to consider performance heterogeneity. Significant differences in resource availability between networks can, if not handled properly, lead to a buildup of data in buffers, with the subsequent risk of loss of information. There is also a risk of inadvertently overloading less capable networks.

3. Reduce the network traffic generated by Web services

   There are several approaches to reducing the overhead of Web services. Each technique can be used separately, or they can be combined for even greater gains. See Section 2.3 for an overview of techniques identified in IST-090.

In IST-090 we have addressed these issues both through national efforts and experiments, as well as through collaboration and the final IST-090 demonstration. Dependency on end-to-end connections can be removed by adding intermediaries (proxies) to the network that perform certain optimizations that we discuss below. Hiding network heterogeneity is, to a certain extent, made possible by adopting the "Everything over IP" mindset for addressing, and further mitigating differences in network capacities and quality by adding delay tolerance to the messages exchanged. Complexity which cannot be hidden has to be addressed by a middleware [4] that moderates between the network properties and application requirements. First, we discuss proxies before considering specific techniques for reducing network traffic. Finally, we discuss the requirements and challenges of efficient service discovery in military networks.

2.2 Proxies

A proxy is a node in the network between a client and a server through which the network traffic passes. A proxy can be used for several purposes, such as caching, firewalling and content adaptation [9].This means that a proxy can implement solutions addressing points 1 through 3 above. For example, HTTP proxy servers have been popular on the Internet for years, since they lower response times when surfing the Web. Web services proxies follow the same principle as HTTP proxies, in that they function as a "middle man" between the provider and the consumer of the service. However, they do not just understand the HTTP protocol, they must be able to recognize and process SOAP as well.

The NNEC FS [7] states that in order to apply SOA in a federation of systems with different network elements, special devices – so-called edge proxies that support information distribution over disadvantaged grids – should be used. As a consequence, we also pursued the gateway and proxy concept in our experiments in IST-090. The edge functionality implies to adapt service traffic to the capabilities of the tactical networks, sometimes in the form of technology gateways (e.g., the WS-DDS interface mentioned in Section 2.1.1 above).

To support Web services across operational levels and disadvantaged grids we experimented with a prototype solution, called a Delay and Disruption Tolerant SOAP Proxy (DSProxy) [10]. It is designed for use across heterogeneous military networks, and has been used in an operational experiment where it enabled us to use Web services in an actual disadvantaged grid [11]. The DSproxy was also used in the final IST-090 demonstration event [5]. It supports compression, multiple transport protocols, and adds delay tolerance to SOAP. Thus, it implements a number of the optimizations that we present in more detail below.

2.3 Reduce the network traffic generated by Web services

As described in point 3 above, there are different ways to optimize Web services for networks with low data rates: You can optimize the application, i.e., reduce the amount of information the application needs to transmit over SOAP. You can optimize the encoding, i.e., address the overhead of XML by for example compressing the Web services payload. Also, you can address the overhead of the transport mechanisms, and use different protocols to transmit your SOAP messages over the network.

In IST-090 we considered different means to reduce the network traffic generated by Web services:

- Reducing XML overhead with data compression.
- Reducing communication overhead by replacing the transport protocol.
- Reducing information overhead by optimizing the applications' need for information exchange.

The first two techniques can be applied to any Web service, but the latter technique needs to be considered for each and every service in turn. The latter technique should therefore not be a part of the middleware, since the middleware should not be concerned with the application data. But, as discussed in [4], the middleware could provide network status information to the applications to enable them to adapt their communication behavior to the available network resources. This functionality should be placed in the applications themselves or perhaps in proxies, since proxies provide a convenient way of adding functionality between COTS clients and services.

2.3.1 Compression

Efficient XML (EFX) was one of the formats the W3C XML Binary Characterization Working Group investigated during their work with requirements for a binary XML format. EFX was originally developed by Agile Delta and provides a very compact representation of XML information. It was later adopted by the W3C Efficient XML Interchange Working Group (EXI) as the basis for the specification of the efficient XML format, which is now standardized. We have experimented with compression and Web services, and found that overall EFX is the "winner" followed by GZIP as the second best [12]. A recent study [13] repeated the experiments, substituting Agile Delta's EFX with EXIficient, the open source version of Efficient XML. This study supports the original findings, i.e., that EFX compresses best followed by GZIP.

2.3.2 Replacing the transport protocol

On the Internet, Web services use the XML-based SOAP protocol over HTTP and TCP for information exchange. However, properties of these protocols make them unsuited for use in some disadvantaged grids. Our suggestion is that one could consider replacing HTTP/TCP with the Military Message Handling System (MMHS) implementing STANAG 4406. Experiments have shown that this is feasible [14].

2.3.3 Reducing information overhead

Maintaining information superiority, which is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same [15], means that proper information management is critical. Ensuring that only relevant information is transmitted over the network helps maintain information superiority, in that irrelevant information is not allowed to disrupt the information flow by overflowing the network. Content filtering can be used to alleviate network congestion by removing information that is not relevant to the user. Thus, it becomes important to identify the information that is indeed relevant, and transmit only that over the network.

In [16] we discussed several types of information filtering, and suggested that filtering should be performed in the origin system (or in intermediate proxies) in order to limit network use. We have experimented with a combination of geographical and frequency filtering. These techniques ensure that units always have the most recent information about units close to them, but get less frequent updates about units that are further away and thus outside their area of operations. This guarantees that only necessary and relevant information is sent over the network at any time.

An example of a content filtering edge proxy is the suggested Adaptation Framework foR web services prOvision (AFRO). This mediation service offers different levels of QoS to Web services, through application of context-aware service provisioning [17].

2.4 Service discovery

The term service discovery denotes the act of discovering services available for consumption. Service discovery and selection can be performed at two instances in time, design-time or run-time.

In the case of design-time discovery, the service endpoint is set once in either configuration file or WSDL, and it does not change during subsequent invocations unless an administrator changes the address at some later point, for example when deploying in a different network, etc.

Run-time service discovery means that in dynamic networks, we should be able to discover the current state of the network and find the current addresses of all available services. This means that while all the static metadata in the WSDL are valid the entire time, the address location of the service may change, and should be discoverable at run-time.

There are three standards related to service discovery, all by OASIS: Universal Description, Discovery and Integration (UDDI), electronic business using XML (ebXML), and WS-Dynamic Discovery (WS-Discovery). UDDI and ebXML are registries and support both design-time and run-time discovery. WS-Discovery is intended for more dynamic environments than the registries, and supports only run-time discovery. In the SOA baseline, UDDI has been chosen for the service discovery service, whereas ebXML has been chosen for the metadata registry service.

Registries were created for use in large, fixed infrastructure networks. They are not suitable for use in MANETs, due to the dynamic nature of such networks. MANETs, being characterized by mobile units and unstable links, are prone to network partitioning where not all nodes can communicate with each other all the time. In such networks, you can encounter problems with service liveness and service availability.

The *liveness problem* occurs when a service has been published in a registry, but the service has become unavailable. In this case, a client can still look up the service in the registry, but the service cannot be reached. No matter how many times the service discovery is performed — the result is still the same. This occurs because the standardized Web services registries require that you actively register and de-register services to keep them up-to-date.

The *availability problem* occurs when the registry is in a different network partition from that of the client. If this occurs, then the client will be unable to look up any services at all, since it cannot contact the registry. Thus, even if the service the client wants to use is actually present and available in the same network partition, there is no way of discovering and using it.

This means that in dynamic networks where partitions can occur, such as in tactical mobile networks, one should preferably use service discovery mechanisms that address these issues. Tactical mobile networks usually contain a few but highly mobile participating nodes. This means that it is feasible to use fully decentralized service discovery mechanisms in such networks. A fully decentralized mechanism addresses the availability problem by distributing the same information about services to all the nodes that it can reach. If the mechanism is coupled with a lease mechanism or just lets service advertisements time out from its cache, then it can also address the liveness problem in that there is no need to actively de-register unavailable services any more — the mechanism removes such stale information itself.

We have discussed the requirements and challenges of service discovery in different military networks [18], and concluded that due to the diversity of the networking technologies used in military networks, one single mechanism cannot be used in all networks. A toolkit of different mechanisms is needed, where the mechanism that is best suited is used in each network. By doing this, for example by using specially optimized solutions in disadvantaged grids [19, 20], we can solve the problem of service discovery in military networks. However, interoperability is a key concern, so there is also a need for pervasive service discovery across heterogeneous networks [21]. We investigated pervasive service discovery and concluded that using gateways for interoperability is the simplest and most cost-efficient means of achieving the needed protocol interoperability. The gateways must be placed in the connection points between heterogeneous networks (i.e., the so-called interoperability points that the NNEC feasibility study discusses).

2.5 Summary

There are some clear benefits to taking the "adapting Web services approach" to using SOA in disadvantaged grids. Using Web services eases integration with other systems, and allows using the same implementation of clients and services in the entire information infrastructure, thus reducing development and maintenance costs.

In order to employ Web services technology in disadvantaged grids, it needs to be adapted in order to handle low bandwidth and frequent connection disruptions. By implementing the adaptations in proxies, we can gain this flexibility while retaining the SOA benefits such as loose coupling and interoperability.

Standards are important in delivering interoperability in a heterogeneous federation of systems environment, but they are not sufficient to be used in disadvantaged grids without adaption. Ideally, the messaging infrastructure should be optimized for the consumers of services without the need to incorporate proprietary, ad hoc solutions. But, when optimizations are necessary, they should be implemented in gateways/proxies to ensure continued use of COTS clients and services.

In IST-118 we aim to leverage the knowledge gained from IST-090 in our work towards a tactical SOA profile.

3) NATO IST-118

IST-118 is a newly started NATO working group, which aims to provide concrete recommendations and guidelines when it comes to extending the SOA paradigm into the tactical domain. The group currently consists of domain experts from the NATO Communications and Information (NCI) Agency, Germany, the Netherlands, Norway and the United Kingdom. Other interested parties are encouraged to contribute to the group by contacting the group chairman, Peter-Paul Meiler (peter-paul.meiler@tno.nl).

3.1 Objectives and topics to be covered

The goal of IST-118 is to identify a set of use cases giving examples of the types of information that are exchanged at the tactical level, and use these to perform experiments targeting possible SOA improvements. Based on the results, the goal is to provide guidance (best practices) for making SOA applicable in battlefield disadvantaged grids, in the form of a Tactical SOA Profile.

The group aims to identify the types of information that are exchanged at the tactical level in the SOA environment. These will be used in testing and prototyping. Depending on the use cases identified we may consider "future" systems and services, as we do not limit our focus to current systems.

Based on the identified types of information and the available technology we will suggest a (set of) solution(s). We will employ formalized testing in a *synthetic environment*. Which framework to employ for this testing will be decided at a later meeting.

Experimentation will be subject to a rigorous test plan. The test plan will incorporate well defined scenarios with predefined parameters. For the communication networks the group will consider what techniques, throughputs and disruptions are relevant to the disadvantaged networks in the expected scenario.

The main focus is on identifying what we call *tactical SOA foundation services*. By this we mean which core enterprise services we need support for in the tactical domain. Examples can be the messaging service, publish/subscribe service, and service discovery service. In other words, we aim to investigate how services from the SOA baseline (see Figure 2) can be extended for use in tactical networks.

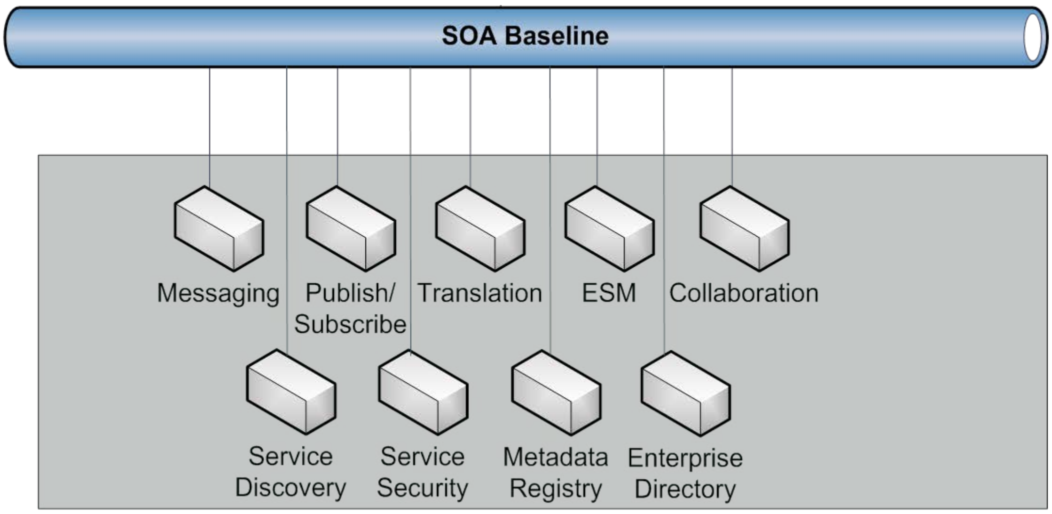

Figure 2: The CES (Basic SOA Infrastructure) Functionality (from [6])

The SOA baseline consists of the following subset of the core enterprise services [6]:

- Messaging: This service provides transport of information and forms a messaging infrastructure within the SOA.
- Publish/Subscribe: This service provides automated distribution of information based on user needs. It also minimizes traffic on the messaging infrastructure through the use of event driven notification of changing data.
- Translation: This service provides the automated means for the semantics of information to be translated from one structure to another.
- Service Discovery: This service provides a mechanism to discover and locate service instances.
- Service Security: The CES Security Services are a suite of services designed to enable Information Assurance. They provide a foundation to implement uniform, consistent, interoperable and effective service security.
- Metadata Registry: The purpose of this service is to provide a (conceptually) centralized source of technology-based representations of standards and specifications as implemented by different Communities of Interest (CoI) in order to improve visibility and enable interoperability.
- Enterprise Directory: This service provides a means for synchronization between directories or data repositories in NATO nations and NATO domains in order to harmonize and rationalize the information.
- Collaboration: In this initial SOA baseline, the Instant messaging service is included. This document recognizes that there are additional collaboration services and more services will be addressed in future versions.

- Enterprise Service Management (ESM): These services will provide the suite of operational processes, procedures and technical capabilities needed to ensure that NNEC services are up and running, accessible and available to users, protected and secure, and that they are operating and performing within agreed-upon parameters.

In IST-118 (a subset of) the SOA baseline will be subject to testing in disadvantaged grids.

3.2 Spiral approach to testing in IST-118

We have agreed to employ a spiral approach, in other words starting with one use case and repeating the process in succession as new use cases are added later.

3.2.1 Synthetic environment

We have agreed on a set of requirements regarding the synthetic environment:

- It must be capable of supporting all the testing that we want to perform (as defined in the test plans)
- It must be capable of connecting to real systems. In other words, it should be an emulator rather than a simulator
- The synthetic environment should preferably be as portable as possible

The group's approach will be to select one or more emulators, and, if several alternatives are available, decide which one to use based on an evaluation of measures of performance and measures of effectiveness of the given frameworks. At the next meeting we aim to determine what kind of input is needed to support our emulations, and find out what environmental parameters are interesting and should therefore be emulated (bandwidth, loss of connectivity, latency, response times, throughput, etc).

3.2.2 Spiral approach

We decided to use an incremental spiral approach to creating the tactical SOA profile. In each spiral we aim to test a set of use cases and core services, using the synthetic environment to provide a representable disadvantaged grid. Based on experiment series we aim to generate SOA recommendations, which collectively will form the basis of the tactical SOA profile.

The first item of the spiral is to define one or more use cases which identify processes, actors, and the relevant core service(s) to include. The synthetic environment will be employed to provide restrictions on throughput and create disruptions, enabling us to investigate Web services operation and QoS aspects relevant to the tactical domain.

Next, we need to create a test plan – a document detailing a systematic approach to testing. A plan should contain a detailed understanding of what the work flow of setting up and performing the test will be. Thus, it provides a means to perform multiple and repeatable tests for different use cases.

3.3 Significant milestones

The current IST-118 group has decided on the milestones in Table 1. Milestones 1 through 4 are discussed above.

Milestone 5, the demonstration event(s), will show national and industry solutions addressing SOA in tactical networks. The final demonstration event of IST-090 (co-located with MCC 2011) was a success (see [5] for details). Thus, we agreed to aim for such an event as the culmination of IST-118 as well.

The final milestone is the STO report containing the tactical SOA profile. This will specify which standards to use and how to use them in order to extend the existing CES standards / recommendations for the SOA baseline profile into the tactical domain.

NO.	MILESTONE	DATE
1	Use case(s) document produced (first version)	2013 Q3
2	Synthetic environment defined	2013 Q3
3	First spiral	2013 Q4
4	Other spirals	2014, 2015
5	Demonstration event(s)	2014(?), 2015
6	Final STO report produced	2015 Q4

Table 1: IST-118 milestones

4) Conclusion

In this paper we have presented the main findings of IST-090, which focused on SOA challenges for disadvantaged grids. Recommendations from that group include employing optimizations such as removing the dependency on end-to-end connections, addressing network heterogeneity, and reducing the network traffic overhead of Web services. The group suggested introducing proxies to implement these optimizations, in an attempt to provide a separation of concerns between proprietary enhancements and COTS services and clients. We investigated different approaches to reducing traffic overhead, such as data compression, replacing the transport protocol, and filtering information. Alternatives to Web services (e.g., DDS) were considered for use in certain sub-systems, but the main focus was on Web services as that technology has been identified by NATO as the key enabler for NNEC.

IST-118 is a recently started NATO STO group intended as a follow-on to IST-090. In the new group, the goal is to create what we call a Tactical SOA Profile, that is, to provide a profile for using (a subset of) the core enterprise services in tactical networks, with special focus on disadvantaged grids.

At the kick-off meeting we outlined how to proceed with work in the group. We discussed important items of work, notably the need to identify use cases and a synthetic environment for testing. We agreed on an incremental spiral approach to experimentation and testing, and identified significant milestones. Apart from experimentation, we discussed the need to disseminate results through academic publications in addition to the final STO report, and that we should aim to show some of our findings in a demonstration event. Such an event was held at the end of the IST-090 group, and we hope to create an equally successful event by the end of IST-118.

IST-118 aims to perform a series of experiments applying knowledge from IST-090 to (a subset of) the standards identified by the SOA baseline. The main goal and intended outcome of the work is the tactical SOA profile.

References

[1] F. Annunziata, B. Ardic, X. Denis, G. Fletcher, T. Hafsøe, I. Hernández Novo, N. Jansen, F. T. Johnsen, P.-P. Meiler, I. Owens, B. Sasioglu, J. Śliwa, J. Stavnstrup, and A. Tokuz. “IST-090 SOA challenges for disadvantaged grids,” 15th International Command and Control Research and Technology Symposium (ICCRTS), Santa Monica, CA, USA, July 2010.

[2] A. Gibb, H. Fassbender, M. Schmeing, J. Michalak, and J. E. Wieselthier. “Information management over disadvantaged grids,” Final report of the RTO Information Systems Technology Panel, Task Group IST-030 / RTG-012, RTO-TR-IST-030, 2007.

[3] I. Hernández Novo, P.-P. Meiler, L. Shaw Manero. “DDS technology demonstrations related to IST-090,” MCC 2011, 17-18 October 2011, Amsterdam, Netherlands.

[4] Christoph Barz and Norman Jansen. “Towards a Middleware for Tactical Military Networks – Interim Solutions for Improving Communication for Legacy Systems,” MCC 2011, 17-18 October 2011, Amsterdam, Netherlands.

[5] Frank T. Johnsen, Trude H. Bloebaum, Léon Schenkels, Rui Fiske, Marc van Zelm, Vincenzo de Sortis, Aad van der Zanden, Joanna Śliwa, and Przemysław Caban. “SOA over disadvantaged grids experiment and demonstrator,” MCC 2012, Gdańsk, Poland, 8-9 October, 2012

[6] Consultation, Command and Control Board (C3B). “CORE ENTERPRISE SERVICES STANDARDS RECOMMENDATIONS: THE SOA BASELINE PROFILE VERSION 1.7,” Enclosure 1 to AC/322-N(2011)0205, NATO Unclassified releasable to EAPC/PFP, 11 November 2011

[7] NATO Network Enabled Feasibility Study Volume II: Detailed Report Covering a Strategy and Roadmap for Realizing an NNEC Networking and Information Infrastructure (NII), version 2.0, 2005

[8] Przemysław Caban, Joanna Śliwa. “Dedicated WS-DDS Interface for Sharing Information Between Civil and Military Domains”, MCC 2011, 17-18 October 2011, Amsterdam, Netherlands.

[9] M. Rabinovich and O. Spatscheck. Web caching and replication. Addison Wesley, 2002.

[10] “Robust Web Services in Heterogeneous Military Networks”, Ketil Lund, Espen Skjervold, Frank T. Johnsen, Trude Hafsøe, and Anders Eggen, IEEE Communications Magazine, Special Issue on Military communications, October 2010.

[11] F.T. Johnsen and T. Hafsøe, “Experiments with Web services at Combined Endeavor”, 15th International Command and Control Research and Technology Symposium (ICCRTS), Santa Monica, CA, USA, June 2010.

[12] Frank T. Johnsen and Trude Hafsøe. "Using NFFI Web Services on the tactical level: An evaluation of compression techniques", 13th International Command and Control Research and Technology Symposium (ICCRTS), Seattle, WA, USA, June 2008.

[13] T. Podlasek, J. Śliwa, and M. Amanowicz. “Efficiency of compression techniques in SOAP.” Military Communications and Information Systems Conference (MCC), Wroclaw, Poland, September 2010.

[14] 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.” NATO IST-083 Symposium on Military Communications with a special focus on Tactical Communications for Network Centric Operations, Prague, Czech republic, April 2008.

[15] J. E. Miller and J. Dussault. “Accessing and sharing: Facets of addressing information overload.” 11th International Command and Control Research and Technology Symposium (ICCRTS), Cambridge, UK, 2006.

[16] T. Hafsøe and F. T. Johnsen. Reducing network load through intelligent content filtering. 13th International Command and Control Research and Technology Symposium (ICCRTS), Seattle, WA, USA, June 2008.

[17] Śliwa J., Gleba K., Amanowicz M., “Adaptation Framework foR web services prOvision in tactical environment”, MCC 2010: Military Communications and Information Systems Conference, Wrocław, Poland

[18] “Web Services and Service Discovery in Military Networks”, Frank T. Johnsen, Trude Hafsøe, Magnus Skjegstad, 14th International Command and Control Research and Technology Symposium (ICCRTS), Washington DC, USA, June 2009.

[19] “Adapting WS-Discovery for use in tactical networks”, Frank T. Johnsen and Trude Hafsøe, 16th ICCRTS, Québec City, Québec, Canada, June 2011.

[20] “An Evaluation of Web Services Discovery Protocols for the Network-Centric Battlefield”, Magnus Skjegstad, Frank T. Johnsen, Trude Hafsøe, MCC 2011, Amsterdam, Netherlands, October 2011.

[21] “Pervasive Service Discovery across Heterogeneous Tactical Networks”, Frank T. Johnsen, Joakim Flathagen, Trude Hafsøe, IEEE MILCOM, Boston, MA, USA, October 2009.