IST-118 SOA recommendations for Disadvantaged Grids: Tactical SOA Profile, Metrics and the Demonstrator Development Spiral.

Point of Contact

Meiler, Peter-Paul
Netherlands Organisation for Applied Scientific Research TNO
P.O. Box 96864, 2509 JG the Hague
THE NETHERLANDS

peter-paul.meiler@tno.nl

Authors

Bloebaum, Trude Hafsoe
Norwegian Defence Research Establishment (FFI),
NORWAY

Trude-Hafsoe.Bloebaum@ffi.no

Johnsen, Frank-Trethan
Norwegian Defence Research Establishment (FFI),
NORWAY

Frank-Trethan.Johnsen@ffi.no

Jansen, Norman
Fraunhofer FKIE,
GERMANY

norman.jansen@fkie.fraunhofer.de

Meiler, Peter-Paul
Netherlands Organisation for Applied Scientific Research TNO,
THE NETHERLANDS

peter-paul.meiler@tno.nl

Owens, Ian
Cranfield Defence and Security,
UNITED KINGDOM

i.owens@cranfield.ac.uk

ABSTRACT

The Service Oriented Architecture (SOA) paradigm has been chosen by the NATO C3 Board (NC3B) as the method to achieve interoperability at the information infrastructure level. The SOA paradigm can enable agile C2 functionality because it provides flexibility and loose coupling. Therefore 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, are a part of this development, at least for use in fixed infrastructure networks as they are currently available at the higher levels of command such as (deployed) headquarters. But they are not yet deployed at the tactical levels.

NATO 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.).

This paper covers the results of IST-090 and outlines the program of work for IST-118. The goal of IST-118 is to create a recommendation for a tactical profile for using SOA in disadvantaged grids. The paper focuses on the following topics that are of specific relevance for this symposium: Metrics, Systems architecting approaches and Systems architecture assessment.

1 INTRODUCTION

The Service Oriented Architecture (SOA) approach has been chosen by 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 civilian 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 battle space.

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] and [2]. Disadvantaged grids are characterized by low bandwidth, variable throughput, unreliable connectivity, and energy constraints imposed by the wireless communications grid that links the nodes [3].

The results of IST-090 created an awareness of the challenges related to extending a SOA to tactical networks and provided some possible solutions. These solutions have an impact on the communication and information architecture. 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 [4], and in the final two IST-090 demonstrations by DEU [5] and NC3A, NOR and POL [6], both at the Military Communications and Information Systems Conference (MCC) in 2011.

The SOA concept is now well known within NATO, and, partly due to the work of predecessor IST groups, it is being used in portions of the Afghan Mission Network (AMN).

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 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 documents provide best practices for how to implement interoperable Web service based systems. NATO has, through the Core Enterprise Services Working Group, defined a number of core services that are needed in order to build a NATO-wide service-oriented system-of-systems. They have published a SOA Baseline [7] 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 provides. 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 OBJECTIVES AND TOPICS TO BE COVERED

IST-118 will 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 on battlefield disadvantaged grids, in the form of a Tactical SOA Profile.

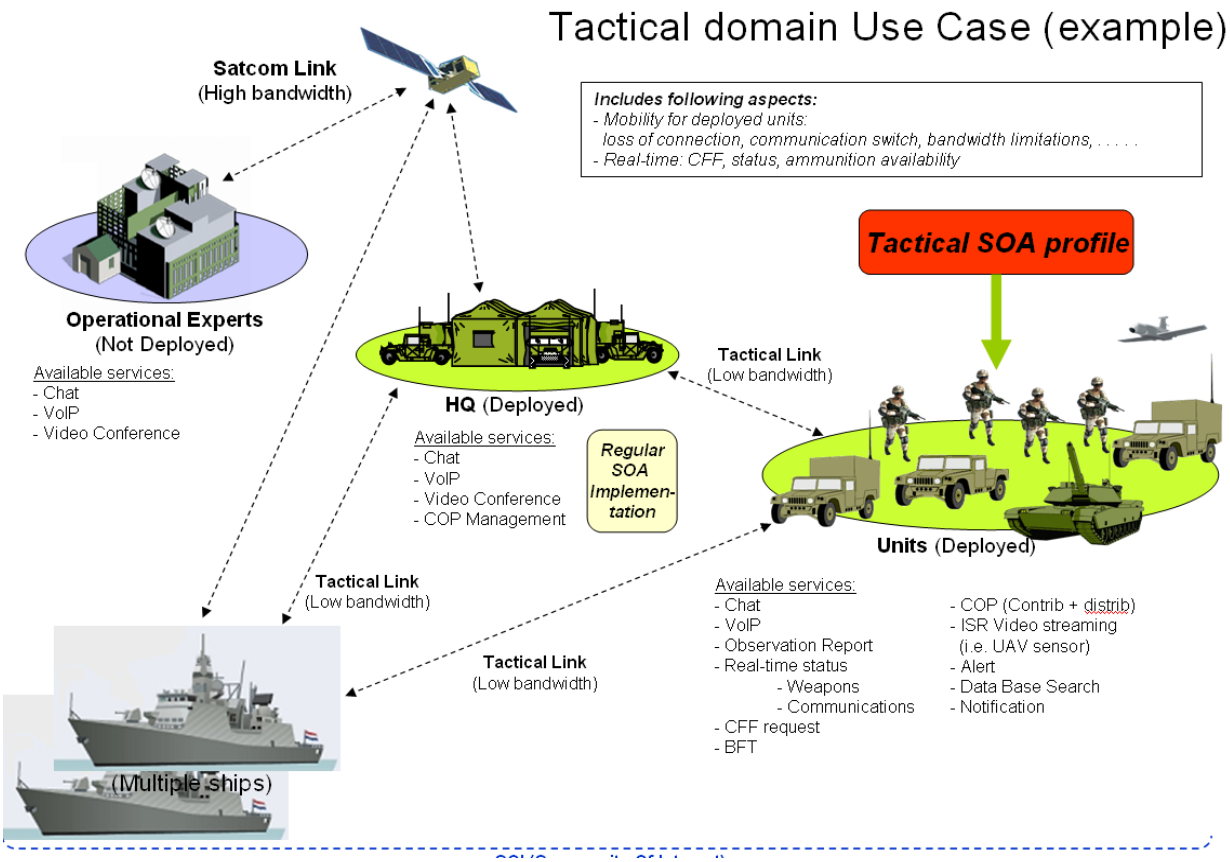

Figure 1: IST-118 Basic Use Case

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 propose a (set of) solution(s). We will employ formalized testing in a synthetic environment. Which specific framework to employ for this testing must still be determined. Also the QoS parameters (metrics) to be used for testing will be determined.

Experimentation will be subject to a rigorous test plan. The test plan will incorporate well defined scenarios with predefined parameters. The test plan will incorporate a spiral development cycle. 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 can be extended for use in tactical networks. The SOA baseline itself consists of the following subset of the core enterprise services [7]: Messaging, Publish/Subscribe, Translation, Service Discovery, Service Security, Metadata Registry, Enterprise Directory, Collaboration and Enterprise Service Management (ESM).

3 FOUNDATION: THE RESULTS AND CONCLUSIONS FROM IST-090

IST-118 builds on the results and conclusions of IST-090. These results and conclusions are succinctly delineated below:

- IST-090 brought together the knowledge and experience of the member nations to better understand the SOA challenges and problems of deploying SOA on disadvantaged networks;
- Tests were carried out among IST-090 participants. A technology demonstration with the focus on DDS was held in Madrid 2010 and several demonstrations of actually deploying SOA on disadvantaged networks were provided at MCC 2011;
- IST-090 identified advantages and disadvantages of the used solutions;
- IST-090 identified limitations for the utilization of specific solutions in disadvantaged networks;
- IST-090 gained experience with SOA implementation for a tactical disadvantaged environment (in experimental stage);
- IST-090 provided directions for further development in terms of SOA for disadvantaged grids.

Figure 2 presents a more explicit overview of the optimizations that we considered in IST-090.

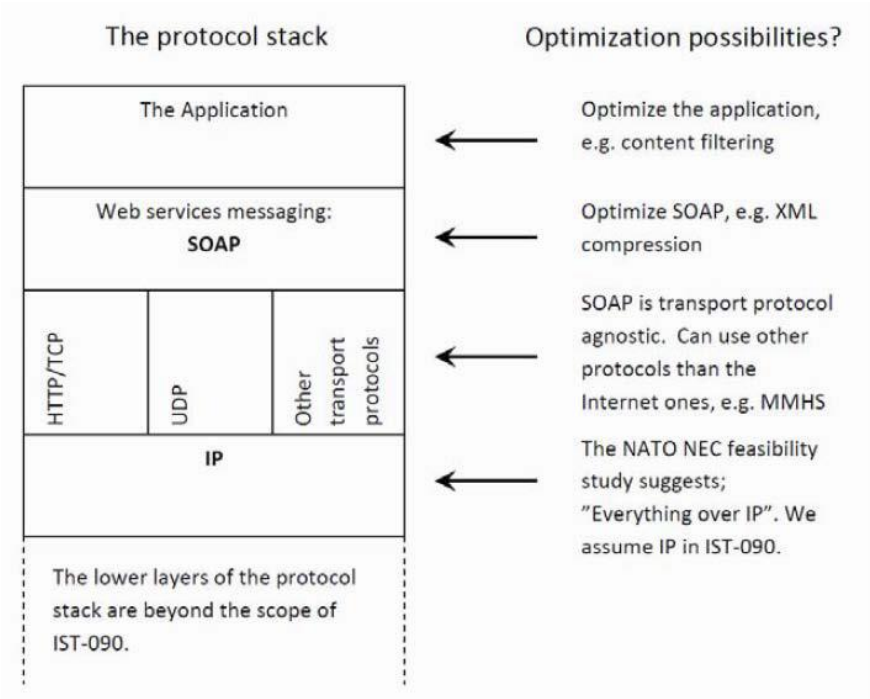

Figure 2: Optimizing the Web services stack (from [1])

IST-090 has identified three main 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. Hide 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 build-up 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
   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.

Points 1 and 2 above can have a real impact on the architecture of a SOA that is deployed on a (combination of) disadvantaged grid(s). Furthermore we 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.

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. But, in order to employ Web services technology in disadvantaged grids, it needs to be adapted to handle the low bandwidth availability 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.

The SOA implementation should be robust. Therefore, the messaging infrastructure should be optimized for the consumers of services without the need to incorporate proprietary, ad hoc solutions. When specific optimizations are necessary, they should be implemented in gateways/proxies to ensure continued use of COTS clients and services.

4 TACTICAL SOA PROFILE CONSIDERATIONS

Current SOA implementations tend to create increased demand on network resources, while proposed NATO standards (static environment) [7] are not necessarily suitable and not extensively tested for disadvantaged grids. In general, a profile provides a standard way to focus a set of models towards specific architectural styles, applications and environments [8]. Our proposed tactical SOA profile will specify which standards to use and how to use them in order to extend the existing CES standards / recommendations from the SOA baseline profile into the tactical domain. We need a Tactical SOA Profile because:

- It specifies which standards to use;
- It specifies how to use the standards to extend existing CES [7] standards / recommendations to the tactical domain;

- It provides guidance (best practices) to make SOA applicable on battlefield disadvantaged grids. An example (at a high level) of how such best practices may be elaborated is shown in the table below.

Table 1 Example of Best Practices

Network Constraints Problems	***What to do***		
Intermittent Connectivity /link instability	Use Caching mechanisms	Use Data Replication	Use a register of Services (not centralized)
High latency and low-bandwidth	Reduce packets size	Reduce the network traffic	Use Information Filtering
High error rates	Use Reliability mechanisms	Redundancy	

5 ARCHITECTURAL APPROACH AND METRICS

Often, using an architectural approach implies (just) using the NATO Architecture Framework (NAF) or DoDAF. This approach is very helpful when designing an actual product that must be delivered. IST-118 is, however, not in the business of developing a system as a product. But we do want to work methodologically. So we will use the NAF architecture as far as applicable. For our purposes this implies that we may use the NAV, NOV, NSV, NTV and the Services views. The output of IST-118 could eventually evolve to a Technical Standard at the NTV level.

Apart from applying NAF where appropriate, the main innovation in the architectural approach of IST-118 consists of delineating the different dimensions of SOA at the tactical level and of applying a Spiral approach to testing. Each step in the spiral will investigate the different dimensions as they are represented in a new and/or more complicated Use Case then the step before. Each investigation of a Use Case will provide input to the Tactical SOA Profile.

We have considered the following dimensions: Network, Resources, Information Assurance and User Interface. These four dimensions could further be quantified using a set of attributes and a range of possible values for each attribute. This results in a set of Metrics that we can use to evaluate the Tactical SOA profiles as they are applied in each Use Case. For practical reasons, we mainly focus on the Network dimensions for the actual IST-118 work.

Table 2: The four Dimensions that characterize the behaviour of a Tactical SOA implementation

Dimensions	**Attributes**								
Network(*)	connectivity	bandwidth	latency						
Resource	processing capacity	storage capacity	power	total system space	total system weight				
Information Assurance	fixed network topologies	network defences	host defences	perimeter defences	policies & procedures	data defence			
User Interface	content	standard user interface	system training	receptiveness	decision time	lighting	envi ron ment	dis play	input/ output

(*) both latency and bandwidth of the network define the throughput of the network.

The network dimension is characterized by the attributes:

- Connectivity
  Intermittent connectivity causes loss of data; the packets are dropped if they can't be sent, and they should be retransmitted.
- Bandwidth
  Bandwidth, typically measured in bits, kilobits, or megabits per second, is the rate at which data flows over the network. This is a measure of throughput (amount per second) rather than speed (distance travelled per second).
- Latency
  Latency, usually measured in milliseconds, is the time that elapses between a request for information and its arrival. A high latency can degrade the performance of even the largest capacity network to a tremendous degree. Excess latency gives a network a low-speed feel.

6 SPIRAL APPROACH TO TESTING

In each spiral (Figure 3) we aim to test a set of use cases and core services, using the synthetic environment to provide a representative disadvantaged grid. Based on the experiment series we aim to generate SOA recommendations (best practices), 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. This is how we perform architecture assessment.

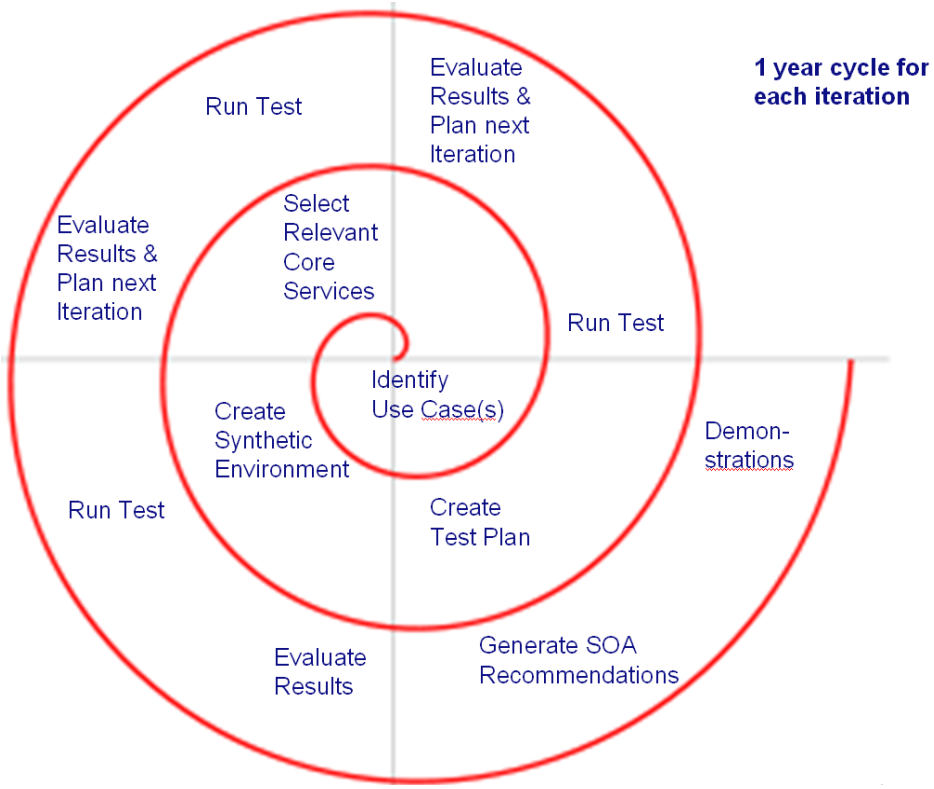

Figure 3: Spiral approach to testing

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.

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. 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, et cetera).

We will employ a test plan for each spiral. A test plan is a document detailing a systematic approach to testing. The 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.

The test plan:

- Is a document detailing a systematic approach to testing;
- Contains a detailed understanding of what the work flow of setting up the test and of performing the test will be;
- Describes a way to perform multiple and repeatable tests for different use cases;
- Makes sure that the test results of each increment can be compared.

In more detail, the test plan contains:

- Selected use Case:
  - Description (at the technical level) of the selected use case;
  - Description of how the services work together;
  - Mapping of the core services to the use case;
  - Identification and description of the types of information that are exchanged (IER).
- Description of the solution to be tested;
- System configuration. What are the parameters (how do we set-up the network), methods (use of emulated framework, etcetera);
- Description of what and how should be recorded during a test and how it is put in the test results (test report).

There is one overall plan (template) per use case. It can be re-used and/or updated for each increment.

The current IST-118 group has decided on the milestones in Table 3 below. Milestones 1 through 4 are discussed above. The final demonstration event of IST-090 (co-located with MCC 2011) was a success (see [6] for details). Therefore we agreed to aim for a similar event as the culmination of IST-118 as well. Milestone 5, the demonstration event(s), will show national and industry solutions addressing SOA in tactical networks.

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.

Table 3: IST-118 Milestones

N°	MILESTONE	YEAR
1	Use Case(s) document produced (first version)	2013
2	Synthetic environment defined	2013
3	First spiral	2013
4	Other spirals	2014, 2015
5	Demonstration event	2014 ?, 2015
6	Final RTO report produced	2015

7 CONCLUSIONS

IST-118 is a newly started NATO working group, which aims to provide a Tactical SOA Profile: concrete recommendations and guidelines when it comes to extending the SOA paradigm into the tactical domain, with special focus on disadvantaged grids. This was also promoted at the Interoperable Open Architecture Conference in October 2012 [9]. 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). We will also consider integrating the IST-118 research with other ongoing NATO-CSO research as well as research outside of NATO, as much as possible.

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. 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, hiding network heterogeneity, and reducing the network traffic overhead of Web services.

We outlined important items of our 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.

8 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. Sliwa, J. Stavnstrup, and A. Tokuz. “IST-090 SOA challenges for disadvantaged grids,” 15th International Command and Control Research and Technology Symposium (ICCRTS), Los Angeles, CA, USA, July 2010.

[2] Annunziata, Francesca, Ardic, Burcu, Barz, Christoph, Fletcher, Graham, Hafsøe, Trude, Hernández Novo, Ignacio, Jansen, Norman, Johnsen, Frank Trethan, Marco-Mompel, Daniel, Martin, Jonas, Meiler, Peter-Paul, Owens, Ian, Sasioglu, Betül, Schenkels, Leon, Sliwa, Joanna, Stavnstrup, Jens, Tokuz, Akif. "An overview of the research and experimentation of IST-090: SOA over Disadvantaged Grids", MCC 2011, Amsterdam, Netherlands.

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.

[8] Michael Rosen. "MDA, SOA and Technology Convergence", MDA (Model Driven Architecture) Journal, December 2003.

[9] P.P. Meiler and the IST-118 team. "IST-118 SOA recommendations for disadvantaged grids in the tactical domain", Interoperable Open Architecture Conference, 30 - 31 October 2012, London, GBR. http://www.iqpc.com.