Chapter 2 – APPLICATION OF SOA TO SUPPORT NEC

This chapter describes how SOA and the associated technology can be applied to NEC. NATO has adopted the principle of Network Enabled Capabilities (NEC) as a major guideline for future development work. Among the most important core functionalities within NEC is dynamic sharing of information. Nations must be willing to share information and the solutions must be available that makes dynamic information sharing possible.

Service Oriented Architectures (SOA) is a concept that enables resources to be provided and consumed as services. The services are published in a service registry, which announces their availability and indicates where they can be invoked. Web Services are promising technologies for implementing SOA allowing for dynamic information sharing between military units. Among the many interesting features of Web Services are dynamic discovery of services and information exchange using event driven models like publish/subscribe. Dynamic security solutions and bandwidth constraints in tactical networks are some great challenges that have to be solved in order to fully deploy a Service Oriented Architecture supporting NATO NEC.

2.1 NATO NEC FEASIBILITY STUDY

If we look at today's military solutions for information exchange, the information flow is typically defined by a set pattern from sender to recipient. It is pre-planned and preconfigured, and changes normally require manual assistance. The solutions used are often stove piped, tailored for certain applications within one military service and with no interoperability with other types of systems. Another problem is the limited exchange of information between security domains. If we look at the NATO NEC ambitions of seamless information exchange between units, there is certainly a requirement for more flexible and dynamic concepts of information sharing.

The NATO NEC Feasibility Study (NNEC FS) [4] is an 18 month study funded by 12 nations organized within the context of NC3B, and conducted by the NC3A. The aim of the study was to develop the scope and vision for NATO NEC and to establish the necessary context for developing the C3 aspects of NEC. The document focuses on a strategy and roadmap for identifying and proposing specific courses of action to deliver NEC CIS infrastructure capabilities including interoperability between NATO, NATO nations, partnership countries and potential coalition members. In the study NEC is defined as follows: "Network Enabled Capability (NEC) involves the seamless linking together of sensors, decision makers, and weapon systems, as well as multinational military, appropriately linked with governmental and non-governmental agencies in a collaborative, planning, assessment and execution environment. The NEC must provide for the timely exchange of secure information, utilizing communication networks which are seamlessly interconnected, interoperable and robust, and which will support the timely collection, fusion, analysis and sharing of information."

The NNEC FS has been well received in NATO and nations and the recommendations chapter of the document has been endorsed by the NATO C3 Board. This endorsement will have an impact on future work of the working groups under the NATO RTO and NATO C3Board in that their work will have to be in line with the recommendations of the NNEC Feasibility Study. One of the recommendations is "to utilize a component based 'Service Oriented Architecture' (SOA) approach in implementing the NII (Networking and Information Infrastructure)". The work of this RTG is therefore in line with the directions of the NATO C3 Board.

2.2 USE OF SOA TO SUPPORT NEC

In addition to the current concept of "need to know", NEC requires the new concept of "need to share". The aim of NEC is to increase mission effectiveness by networking military entities, enhancing the sharing of information and situation awareness. The key prerequisite of shared situation awareness is increased access to and sharing of information. The information infrastructure has an important role as an enabler, organizer and provider of information access and information sharing. By using SOA as a foundation for the Information Infrastructure, military resources may be made available as services that may be published and utilized over a communication infrastructure. The service itself is defined using a well-defined interface that exposes the functionality and hides the underlying implementation details. Services may be aggregated, by either the service provider or service consumer, to create more advanced services as further described at the beginning of Chapter 3 SERVICE ORIENTED ARCHITECTURE TECHNOLOGIES USED. This modularization makes dynamic reconfiguration of functionality easier. It opens up the possibilities of ad-hoc organizations of units without requiring much administrative overhead. The Services are characterized by metadata for easier discovery and published in the network.

Another aspect of SOA is the loose coupling of entities that allows for the dynamic and flexibility required in NEC. In a SOA, Consumers do not need to know in advance where the Service Providers are located (only where the Service Registry is). The Service Providers do not need to know in advance where the Consumers are located (only where the Service Registry is). And the Service Registry does not need to know in advance where neither the Consumers nor Providers are located. This makes ad-hoc organization of entities easier since the requirement for preplanning is minimal.

The concept of publish/subscribe as further explained in Chapter 3 SERVICE ORIENTED ARCHITECTURE TECHNOLOGIES USED has its strength in more efficient information exchange, avoiding information overflow. Simply speaking, publish/subscribe means that you will only receive the information that you have subscribed to. This concept utilizes a combination of push and pull. As opposed to a general "push" mechanism there are benefits in that you may select the information sent to you. Also, pure "pull" principles are not able to notify listeners when events occur.

Even if new and better technologies come along there will always be legacy systems in which nations have invested a lot of money and which have a defined calculated lifetime. These systems need to be integrated in a way that makes them an integrated part of SOA. Integrating systems in an SOA requires (amongst several things) the use of (or mapping to) a common data model and enabling the legacy systems to use SOA publishing and data exchange. As stated in the SOA reference model [5] "A SOA service brings together needs and capabilities, but the provider of the underlying capability may not be the same entity that provides the service which accesses that capability". As an example, when integrating a legacy system in the SOA, a bridge may be used to map the functionality of the legacy system the to the SOA technology used. The legacy system may be managed by different people than the people responsible for the SOA service management. Because administration of services can be done independently of the capability, the integration of functionality over heterogeneous technologies can be made easier.

The benefits of using SOA to support NEC may be summarized as follows:

- Military resources are made available as services over a communication network;
- Efficient discovery of and subscription to as well as downloading of relevant information;
- Faster deployment of new technology and functionality;
- Dynamic reconfiguration of functionality within a relatively short timeframe;
- Integration of functionality over different networks and heterogeneous technologies;
- Minimal pre-planning required – loose coupling of systems; and
- Migration – Legacy systems may be integrated with the new technology.

2.3 FLEXIBLE SECURITY MECHANISMS

The "need to share" concept of SOA requires changes not only related to technical solutions, but maybe even more at the organizational level. The concept of sharing information with others in such a flexible manner may be perceived as loosing control compared to the preplanned and preconfigured solutions. When the consumer in addition may be someone that you do not know in advance, this becomes a challenge. The willingness to share information requires that the provider can be sure that the information is protected all the way during transport and also when received by the consumer.

The increased information sharing in SOA may lead to increased vulnerability if security is not properly integrated. The situation of today is that separate networks protect information of different classification using physical, cryptographic and administrative separation. Introduction of security mechanisms which allow for dynamic and seamless exchange of information between units will be a challenge in NEC. IP level security will give confidentiality between systems, but will not prevent unauthorized access within the systems or LANs. Computer Network Attacks (CNA) will focus on attacks behind the firewalls (crypto devices) within the LANs/Systems. Therefore, end-to-end security services are required in order to secure the information inside the NEC systems and LANs, and to make sure the security is not broken in proxies or servers.

Security is a challenge with respect to NEC, making seamless sharing of information a bit more difficult. In our experiment we have focused on end-to-end security, which is also highlighted as the long term goal in the NATO NEC Feasibility Study. The use of end-to-end security solutions does not exclude additional use of traditional network and transport level security. To obtain end-to-end security we have been experimenting with XML and Web Services security solutions with the addition of XML Security Labels and a Public Key Infrastructure. Even though we have shown that the technology of today is improving, there is a way to go before trusted implementations are available that may be used to protect information of higher classifications like NATO CONFIDENTIAL or higher. More work needs to be conducted in this area.

2.4 DISADVANTAGED GRIDS CHALLENGES

Besides security, bandwidth restrictions at the tactical level are a limitation when it comes to fully deploying NEC principles. Those restrictions will in most cases remain, and as a means of reducing network traffic, the concept of publish/subscribe may be valuable for a consumer to be able to restrict the information being delivered. Other measures to reduce the use of bandwidth could be:

- More efficient protocol solutions (for example, the use of multicast);
- Compression;
- XML schema recoding;
- Data Model recoding; and
- Use of Proxies and cashing techniques.

This Task Group has only been evaluating some compression techniques, which are described in Chapter 8 of the Demonstrator Specification (see Annex A).

More work need to be conducted in this area.