Experiment Report – SOA Pilot 2011

Rolf Rasmussen and Bjørn Jervell Hansen

Norwegian Defence Research Establishment (FFI)

27 February 2012

FFI-rapport 2011/02407

1176

P: ISBN 978-82-464-2076-9
E: ISBN 978-82-464-2077-6

Keywords

Nettverksbasert forsvar

Tjenesteorientert arkitektur

Kjernetjenester

Approved by

Anders Eggen Director

English summary

The SOA Pilot is an experimental demonstrator developed by FFI in cooperation with NC3A and resources from Norwegian Defence. This report documents the pilot as it was presented in June 2011.

The purpose was to show how service-orientation and use of a shared SOA infrastructure can add operational value. Several operational military systems were included in the pilot, which increased the technical experience gained.

Using a coalition operation scenario as backdrop, a storyline was created and used to present technology use cases giving operational value. A subset of NATO Core Enterprise Services was implemented in the pilot. Service discovery services and publish/subscribe services were given special focus. A designated viewer was developed to visualize effects of these core services.

A list of nine key technology points made in the pilot presentation is identified and briefly described in a separate section of the report. The reader is referred to more detailed information given in other publications with a more technical focus.

Experience gained and other reflections and feedback based on the pilot were discussed with the audience directly after the presentation. Highlights from that session are referred in this report. The SOA Pilot was well received and considered as an important initiative, contributing to the development towards Network-based Defence. FFI recommends further experimentation work along the lines of the SOA Pilot, using NATO Core Enterprise Services as the preferred technical platform.

Sammendrag

SOA-piloten er en eksperimentell demonstrator utviklet av FFI i samarbeid med NC3A og ressurser fra Forsvaret. Denne rapporten dokumenterer piloten slik den ble presentert i juni 2011.

Hensikten var å vise hvordan tjenesteorientering (SOA) og bruk av en felles SOA infrastruktur kan bidra til operativ nytte. Flere eksisterende militære systemer ble inkludert i piloten, noe som økte de tekniske erfaringene i betydelig grad.

Med utgangspunkt i et scenario sentrert rundt en koalisjonsoperasjon ble det utviklet et hendelsesforløp med situasjoner som viste bruk av teknologi som ga operativ nytte. Utvalgte kjernetjenester fra NATO ble implementert i piloten, blant disse fikk områdene service discovery og publish/subscribe størst synlighet. En egen visningsmodul (viewer) ble utviklet for å synliggjøre effekten av disse kjernetjenestene.

En liste med ni teknologi-hovedpunkter fra pilot-presentasjoner er tatt frem og omtalt kort i et eget kapittel i rapporten. Leseren henvises til mer detaljert informasjon som finnes i andre publikasjoner med mer teknisk preg.

Erfaringene fra utviklingsarbeidet samt andre refleksjoner og tilbakemeldinger knyttet til piloten, ble diskutert med publikum i en egen sesjon direkte etter presentasjonen. Hovedpunktene fra dette er referert i et eget kapittel i rapporten. SOA-piloten ble godt mottatt, og ble vurdert som et viktig initiativ som bidrar til NbF-utviklingen i Forsvaret. FFI anbefaler videre eksperimentarbeid i forlengelsen av SOA-piloten. NATOs kjernetjenester er den foretrukne tekniske plattformen for dette.

Contents

1 Introduction

The experimental demonstrator ”SOA Pilot”, developed by FFI in cooperation with Norwegian Defence project resources and NATO C3 Agency (NC3A), was presented to the Norwegian Armed Forces in the FFI Batte Lab June 15th and 16th 2011.

The purpose of the SOA Pilot was to gain technical experience with service orientation, and show the audience examples of how the technology can be applied to add operational value. A demonstrator was set up with instances of well-known operational systems, and a shared infrastructure based on service-oriented architecture (SOA) was to allow for flexible information sharing within the demonstrator. The infrastructure was based on the principles of NATO Core Enterprise Services (CES) [1].

This report documents the background, preparations and content of the presented demonstrator, focusing on operational value and identification of enabling technologies. The reflections, recommendations and conclusions that can be made based on the SOA Pilot, are also stated. For further details, the reader is referred to the following publications:

- Technical details regarding SOA and the web service implementations made by FFI for the SOA Pilot are described in [2]
- The use of semantic technologies within the SOA Pilot is described in [3]
- The use of XML confidentiality labels for cross-domain information exchange is described in [4]
- A prototype of a multi-level workstation based on Multiple Independent Levels of Security (MILS) is described in [5]

These reports will complete the technical description given here of the SOA Pilot demonstrator.

2 Background

The FFI-project 1176 (Service-orientation and semantic interoperability in the Information Infrastructure) has among its objectives to explore technologies for SOA on various operational levels. A key challenge is flexible exchange of information between heterogeneous systems. The project has also participated in the work within NATO on Core Enterprise Services, that will be an important building block for future SOA development in NATO. The project also covers research on semantic technologies and end-to-end security solutions for SOA.

A Norwegian Defence procurement project with a mission to prepare “Service-orientation of Decision Support” needed input to the preliminary phase of the project in order to set directions for the upcoming work on service orientation and create further specifications for the project. The idea of performing an experiment, using the recent SOA standards and guidelines from research and combining them with actual instances of military information systems, was assumed to be a good way of creating the first level of necessary experience for further work.

From August 2010 a joint effort was established in order to create the SOA Pilot. The goal was for FFI to implement an experimental SOA infrastructure, interconnecting a significant number of currently operational systems. The infrastructure was to have a national and an international part, with flexible information flows in both directions. NC3A had interests in experimenting with their proposed SOA infrastructure solutions, and they agreed to contribute as responsible for the international part of the infrastructure.

The SOA infrastructure was built upon standards and recommendations from the NATO Core Enterprise Services. These standards and recommendations were emerging at the time of the pilot, but has since then been approved by NATO C3 Board [1].

The technical setup of infrastructure components and application systems was done in the laboratories of FFI and NC3A, connecting the labs via secure internet links. As a means to show the operational value and military effects of the flexibility provided by the technology involved, a scenario and a sequence of operational events was defined. For the demonstration, the scenario was the basis for a storyline, giving the audience realistic examples of how the use of SOA technologies can add military value to an operation.

3 Scenario

The scenario for the SOA Pilot was built around an expeditionary operation to a conflict with an international coalition involved to protect civilians and initiate a peace process. Figure 3.1 is an illustration taken from the starting point of our work to define the scenario.

Figure 3.1 Example illustration from the initial scenario work

The operation involves use of Tactical Units consisting of several Ground Teams under a Tactical Level Command. Naval and air forces are also involved in the operation.

3.1 Storyline

The situation presented in the SOA Pilot takes place within this coalition operation scenario. The ground teams of two Tactical Units, reporting to a Tactical Command HQ, are the main players on the ground. Naval and air forces, in Figure 3.2 represented as Maritime Elements and a Fighter, are standby. There is a reachback possibility from coalition units back to their respective national HQs.

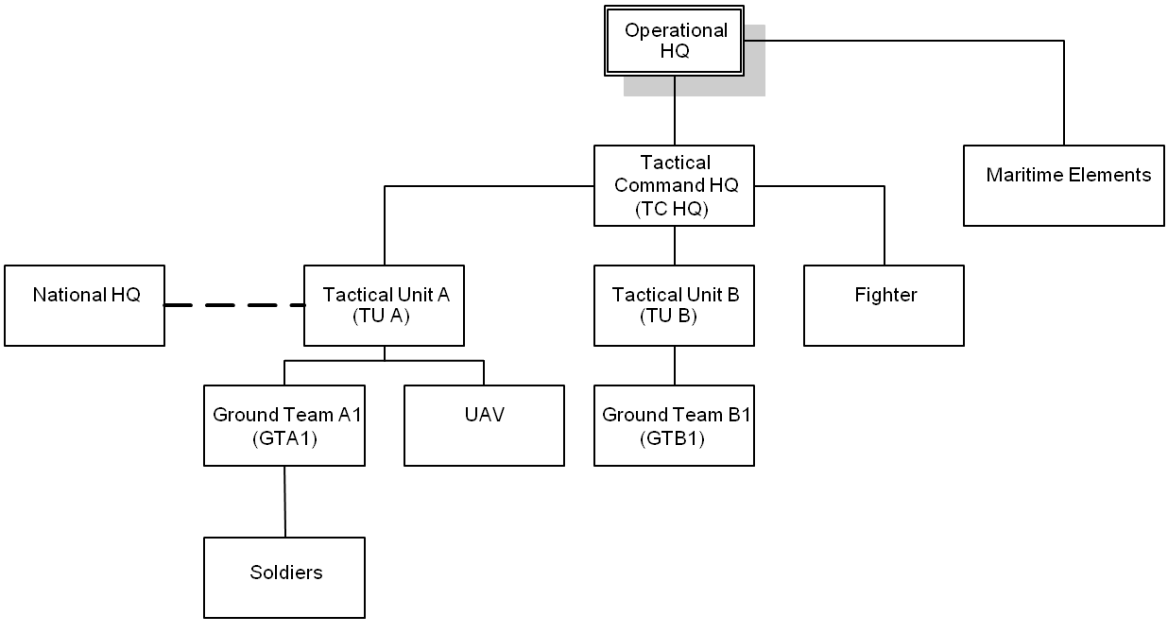

Figure 3.2 Hierarchical organisation of the military units involved in the scenario

Several assumptions with regard to the scenario and technical architectures were made. That was done to simplify the conditions in order to illustrate the benefits of SOA. An example of such an assumption was radio connectivity between and within all participating coalition forces.

To allow for authentic terrain movements within the limits of the involved radio equipment, the story was geographically located to the surroundings of FFI. Figure 3.3 shows the initial situation setup.

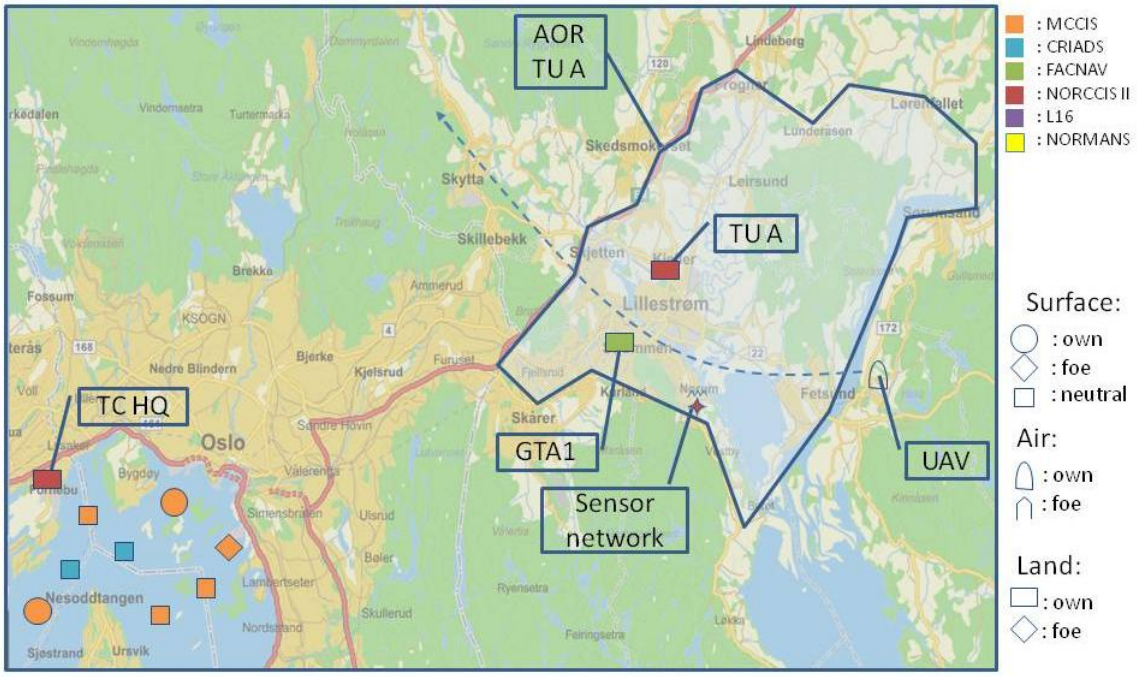

Figure 3.3 Initial setup of the operation area. Position colour indicates reporting system.

In brief, the illustrating story for the SOA Pilot goes as follows:

1. Initial force setup T1, T2
2. Ground Team A1 (GTA1) is patrolling the Area of Responsibility (AOR) of Tactical Unit A (TU A)
3. UAV picture shows potential hostile activity (image comparison via national reachback) T3
4. GTA1 is tasked to investigate the pictured area
5. Incoming incident reports trigger a threat detection warning T4
6. TU A requests reinforcements to GTA1 T5
7. A ground team GTB1 from Tactical Unit B is tasked to move in and provide reinforcement
8. GTB1 (entering from the lower right corner of the map in Figure 3.3) triggers a sensor network on their way towards GTA1 T6
9. GTA1 soldiers dismount from their vehicle for close inspection of the designated area, which results in a request for Close Air Support (CAS) T7
10. A fighter aircraft launches weapons on target
11. Damage assessment is performed by inspecting independent images T8
12. User reports results into the coalition system NITB T9

Codes T1 to T9 refers to technology points that will be introduced in section 5.

With this storyline as backdrop, the SOA Pilot focused towards showing potential operational value of the flexible sharing and exchange of information provided by the SOA infrastructure and the implemented services.

Important premises that are used in the presentation:

- Positions are shared and displayed on the map of a viewer (assumed present on all units), see section 4.1.1.4
- Users have a flexible mechanism for subscribing to the relevant information sources
- Information sources are discovered and made accessible for subscription
- Coalition forces will in general operate in a common security domain on a Mission Secret classification. There are exceptions, however, and technical solutions to handle different security levels were presented.

3.2 Operational value

During the presentation of the SOA Pilot, several value-adding aspects were brought into focus:

- Any military unit can see all services that are currently available for use, due to an automatic discovery mechanism
- Any military unit can subscribe to information from any available service (e.g. ensure continuous flow of updates of positions and incoming events from selected sources)
- Current mission images can be compared to reachback images that exist at a different classification level
- Large volumes of information are continuously being automatically analysed and warnings are triggered
- Textual messages can be exchanged within the coalition
- Connectivity to the shared infrastructure may exist from even the lowest levels of network capacity (disadvantaged grids)
- Automatic filtering of classified information between different security domains (preventing information leakage when soldiers dismount)
- Flexible information exchange enabled by pervasive connectivity (e.g rapid availability of battle damage images from various sources)
- User is allowed secure access to a coalition service based on local authentication and federated identity management

Section 5 will look more detailed into the technical foundation for these elements, and present the enabling technology for each of these aspects.

4 The SOA Pilot

4.1 Systems and contributors involved

This section describes the contributing partners and the systems involved in the SOA Pilot, including modules developed to serve a specific purpose. Some other important contributions are also mentioned. Descriptions are given for each of the participating organizations: FFI, NC3A and the Norwegian Defence.

4.1.1 FFI

FFI was the host of the SOA Pilot, having the largest part of the demonstrator, including all national systems involved, installed in the project lab. A team of FFI researchers participated in the planning phase and did substantial programming for the demonstrator.

4.1.1.1 Infrastructure technology

The FFI part of the SOA infrastructure consisted at the physical level of a local area network connected to the radio networks. Web services were used as the service realization mechanism. The most important elements at the service level were implementations of service discovery and publish/subscribe based on OASIS standards, as recommended by the NATO CES. More details about the FFI infrastructure implementation can be found in [2].

4.1.1.2 Web service adapters

In order to service-enable legacy systems, web service adapters were used to interface the services of each participating system to the infrastructure. Logically, the adapter can be described as two interacting components: A generic part that interfaces the infrastructure, and a system specific part that has to be tailored to meet the properties of the system in question.

Service enabling of systems using web service technology is described in [2].

4.1.1.3 National systems

An important premise to make the SOA Pilot a realistic experience, was the involvement of operational systems. From the technical point of view it was important to gain experience with legacy systems in the context of service-orientation.

In hindsight, the main message is not which of the individual systems that ended up being included in the demonstrator, but the fact that there were a significant number of them. Table 4.1 shows a list of the systems with a brief description for each.

System	Short description
CSD	The Coalition Shared Database (CSD) is a system from the multinational project MAJIIC (**M**ulti-sensor **A**erospace-Ground **J**oint **I**ntelligence Surveillance and Reconnaissance **I**nteroperability **C**oalition). Its purpose is to collect various types of intelligence information in a searchable solution based on replication of metadata between servers. Content may be information requirements, collection and exploitation plans, still imagery, motion imagery, exploitation products and other relevant data that is generated and used by ISTAR collection assets and exploitation systems.
NORCCIS II	NORCCIS II is a national C2 system, developed by the Norwegian Defence, that supports planning and execution of joint (air, land and naval) operations at the strategic, operational and tactical level. The most important common service is the common operational picture, which supports the development of a shared situational awareness between military decision makers concerning the disposition and status of all known actors in the battlespace.
CRIADS	Coastal Radar Integration and Display System (CRIADS) provides control and monitoring facilities for sensors such as AIS, coastal radars, radio direction finders, ESM equipment, and interfaces to tactical links. It has the capability to merge the data inputs into a maritime picture.
MCCIS	Maritime Command and Control Information System (MCCIS) has been developed and maintained for members of NATO. MCCIS contribute a high quality Recognized Maritime Picture (RMP) to NATO's situational awareness and the Common Operational Picture (COP). MCCIS has a substantial Joint capability in providing a near real-time COP to the commander.
TDL	The Tactical Data Link (TDL) Link 16 has been developed to meet the information exchange requirements of all tactical units, supporting the exchange of surveillance data, electronic warfare data, mission tasking, weapons assignments and control data. The Link 16 message standard uses J-series messages and completely meets the requirements for C2 functionality and aircraft control. In addition, Link 16 has been selected by the US and NATO as the main tactical data link for theatre missile defence. In the execution of the SOA Pilot, this system was represented by simulated input.

System	Short description
FACNAV	FACNAV (aka MARIA BMS) is an application originally developed to support Forward Air Controllers (FAC) and Forward Observers (FO). The application is designed to operate effectively on computers with touch sensitive screens (e.g. a tablet PC), but works also on standard computers. The main objective for the application is to support tactical navigation and offer automatic information exchange (enabling blue force tracking) and Forward Air Control (FAC) operations to ensure • Force security • Accurate delivery of weapons on target • Minimized third party collateral damage
NORMANS	NORwegian Modular Arctic Network Soldier (NORMANS) is a concept for soldier situational awareness, with blue force tracking, navigation, target hand-off, and text messaging. The concept consists of two classes of equipment: • NORMANS Light, designed for the individual team members in a dismounted squad • NORMANS Advanced, tailored to the needs of the squad leader In the execution of the SOA Pilot, this system was represented by simulated input.
Sensornet	The sensor network is an experimental setup by the FFI project SASS (Situational Awareness Sensor Systems), built using TelosB sensing nodes. The nodes are equipped with sensors for sound, light, temperature, humidity, ultrasound, and passive infrared in order to detect and report on the presence of objects in the vicinity.
GEO/METOC	GEO/METOC is a set of core services and applications for the storage, processing and dissemination of geographical (GEO), meteorological and oceanographic (METOC) data.

Table 4.1 National systems included in the SOA Pilot

4.1.1.4 The Viewer

The Viewer was developed by FFI for the SOA Pilot. It runs on any computer that supports the required Java libraries (see technical description in [2]). It was designed to meet the requirements for an application showing the user

- A map, on which positions and other symbols can be displayed
- Services available for subscription
- Incidents, implemented here as a sequential scrolling log of incoming messages
- Chat functionality

A screenshot from the Viewer is shown in Figure 4.1.

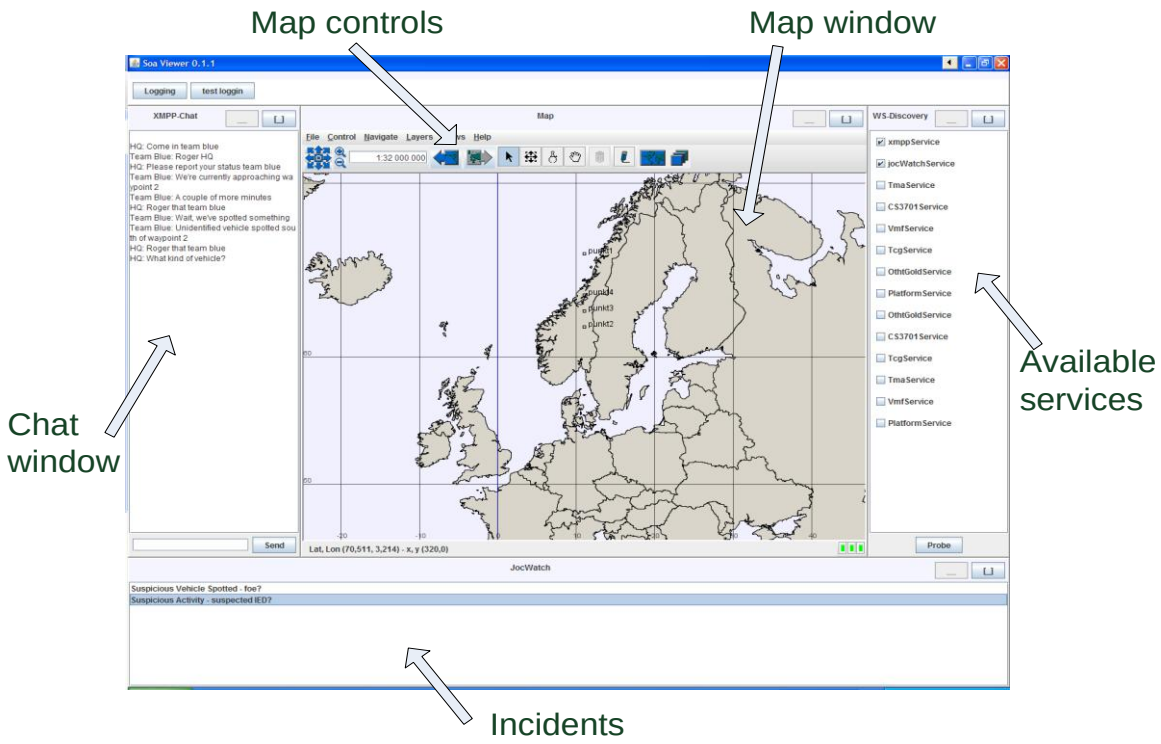

Figure 4.1 Information from any system was displayed in the Viewer

The Viewer itself can also be subscribed to as a service, as it can be set up to forward all incoming messages. For test and demonstration purposes, this offers an elegant way of accumulating information flows in an experiment setting.

4.1.2 NC3A

Core Enterprise Services (CES) have been on the NC3A agenda for several years. Seeing the SOA Pilot as an opportunity to experiment with different implementations of infrastructures based on the CES recommendations [1], they were an important technical partner. Additionally, the point of including international (NATO) systems made the SOA Pilot resemble a real-life coalition operation in a much better way.

4.1.2.1 Infrastructure technology

The physical link between FFI and NC3A labs was a Virtual Private Network (VPN) tunnel via the Internet. NC3A had their own implementation of publish/subscribe according to the WS-Notification standard and a service discovery solution, both in line with the recommendations of [1].

4.1.2.2 NATO systems

The systems brought into the SOA Pilot by NC3A, are shown in Table 4.1.

System	Short description
NATO Track Source	Tracks from participating coalition forces were simulated. The track format was NATO Vector Graphics (NVG).
JOCWatch	JOCWatch has become a well-known system from coalition operations, collecting incident reports and distributing them. The incident reports used in the SOA Pilot were collected from a test version of the US PASS system.
BRITE	A system from NATO's application suite BRITE (Baseline for Rapid Iterative Transformational Experimentation) was used on the NC3A side as their alternative to the FFI Viewer.
NITB	NATO Intelligence Tool Box was used to demonstrate federated identity when uploading images for damage assessment.

Table 4.2 International systems included

Again, the important message is not necessarily which systems that were included, but having some of them there, showing the international part of the coalition.

4.1.3 Input from the Norwegian Defence organisation

An essential part of the SOA Pilot preparation process was to gain insight from military officers and operational users, in order to understand how the technological flexibility should be converted into potential benefit on the user level. A two day workshop in February 2011 involving operational officers, technical personnel and researchers from FFI and NC3A, was important for the common understanding of the pilot work. Besides an extensive and very valuable sharing and combining of technical and user-related issues, the workshop resulted in the requirements for the Viewer (section 4.1.1.4) with the four essential elements map, services, incidents and chat.

The project coordinator for the defence project was the primary point of contact into the Norwegian Defence organization. He defined most of the scenario-based storyboard that was essential in presenting the SOA Pilot, and he was a key player in selecting operational systems to be included. He also arranged personal contacts and provided information necessary to make the experimental versions of the systems useful in the pilot. These contributions were critically important in the creation of a successful SOA Pilot presentation.

4.2 The demonstrator

This section describes the demonstrator that was used in the SOA Pilot.

4.2.1 System overview

The high-level technical description of the SOA Pilot has been summarized in the diagram in Figure 4.2

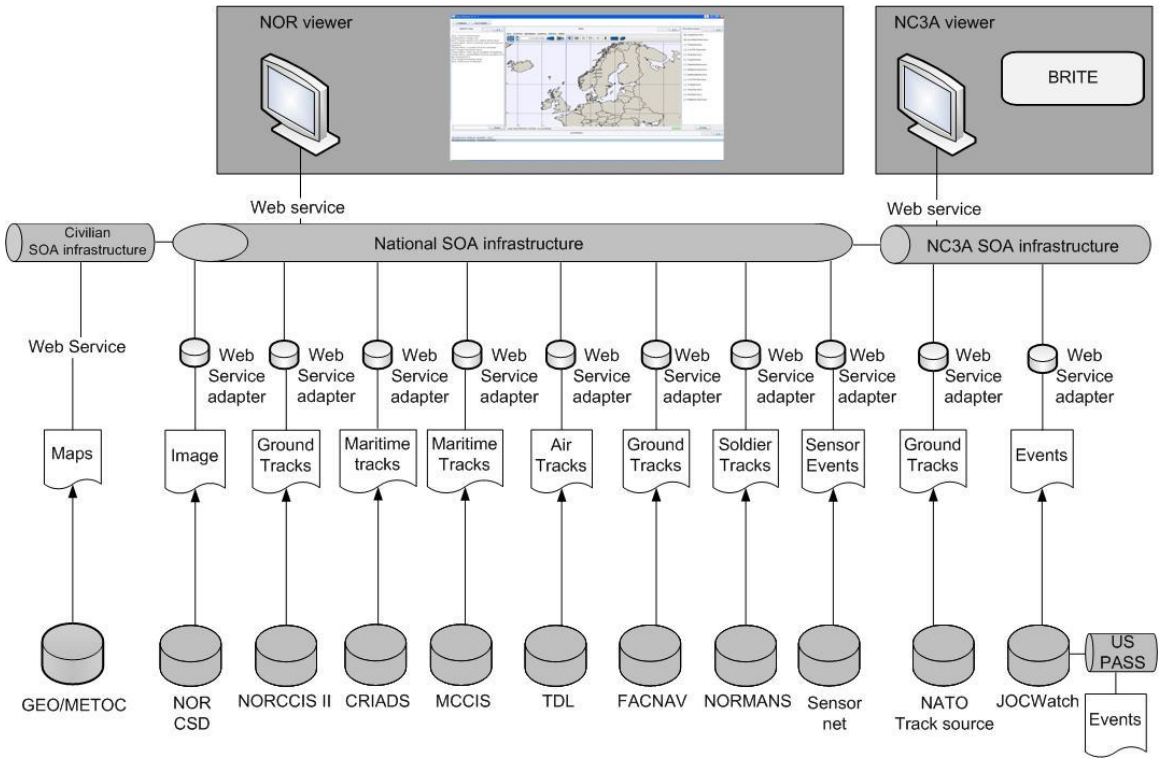

Figure 4.2 SOA Pilot system overview

Each of the systems pictured in the lower end of the diagram, is briefly described in section 4.1. The essence of the SOA Pilot is that all these systems deliver information, in the technical arrangement of a web service, into an infrastructure connecting all elements.

The infrastructure is pictured as an interconnection of the three physical parts. The largest part was located at FFI (National SOA Infrastructure), containing core services like discovery and publish/subscribe to be explained later. NC3A had their implementation of a similar infrastructure, while the civilian internet was used to connect to the official map service.

The top level of the diagram depicts the viewer level, with two independent implementations. At this level selected information from the complete system was shown.

4.2.2 Physical architecture

Figure 4.3 shows the actual technical setup of elements connecting into the FFI LAN. Two of the radio networks were physically equipped, while two were simulated. Systems referred in the figure are described in section 4.1, while the security mechanisms MILS and Guard will be described in sections 5.3 and 5.7.

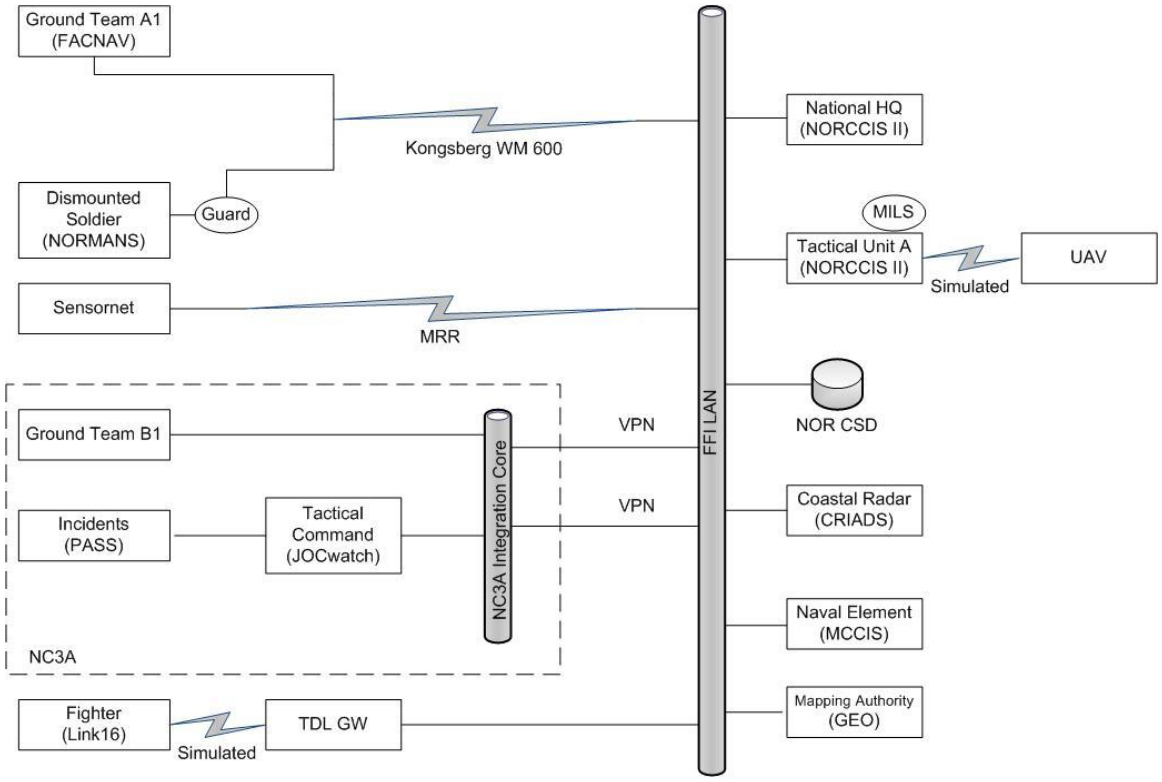

Figure 4.3 SOA Pilot network diagram

4.2.3 Services

The previously described system landscape and physical network refers to tangible elements. The elements that are key to SOA – the services – are not so easily visualized. This section is about the services that were used in the SOA Pilot.

It is useful to distinguish between

- **functional services**, e.g. issuing position reports and incidents, and
- **core services**, which can be thought of as reusable parts of the infrastructure that are there for everyone to use – examples are discovery and publish/subscribe

The majority of the information flows in the SOA Pilot were created by incident reports and positions reported on the NFFI (Nato Friendly Force Identification) format. Incident and position reporting were the two main functional services in the pilot. Instances of one or both of these services were implemented by each system involved, and information was exchanged when services were invoked.

The demonstrator also made use of several core services. The most important one in this context is publish/subscribe, which allows information consumers to create a subscription at the producer side, and then getting notified with an actual flow of information for every event that is covered by the subscription. Other core services are listed in section 5.8. Core services and the recommended standards for NATO are described in [1].

5 Key technology points

Keeping in mind that the presented storyline (section 3.1) was created in order to show how infrastructure and core technical solutions can add operational value, this section points to the technical demonstration elements of the SOA Pilot.

In section 3.2 there is a list of value-added operational situations from the SOA Pilot. For each of these elements there is an underlying technical key point. Table 5.1 indicates which enabling technology each situation is based upon.

Operational situation	**Value-adding technology**
Any military unit can see all services that are currently available for use	Service discovery (T1)
Any military unit can subscribe to information from any available service	Publish/subscribe (T2)
Current mission images can be compared to reachback images at a different classification level	Multilevel security (T3)
Large volumes of information are continuously being automatically analysed and warnings are triggered	Threat detection (T4)
Textual messages can be exchanged within the coalition	Chat services (T5)
Connectivity to the infrastructure may exist from even the lowest levels of network capacity	Disadvantaged grids (T6)
Automatic filtering of classified information (preventing information leakage when soldiers dismount)	Cross domain information exchange (T7)
Flexible information exchange enabled by pervasive connectivity (battle damage images from various sources)	SOA infrastructure (T8)
User is allowed secure access to a coalition service based on local authentication and federated identity management	Role-based access (T9)

Table 5.1 Presented operational value point and its corresponding enabling technology

Codes T1 to T9 are also shown in the storyline in section 3.1, where the technology points were assigned to the step in the pilot presentation where the respective point was made.

In the following subsections each technology point will be briefly described. The sequence is according to the presented storyline, and is not to be interpreted as a priority or scale of importance.

5.1 Service Discovery

An important operational value focused in the SOA Pilot was the ability to see and choose information from all services that were currently available. The underlying core service enabling this is service discovery.

Discovery of services is in principle performed by lookup in a registry where instances of all services are defined. This can be done at design-time, implying a static choice programmed into the application, or at run-time, which gives a lot more flexibility. Standards and recommendations exist, see [1].

The registry approach, however, suffers from liveness and availability problems in dynamic environments. For the SOA Pilot it was decided also to use a non-registry solution for service discovery, emphasizing the need for dynamicity that was exemplified in the operational situation created. All details of how the web service standard WS-Discovery was used to enable the choice of available services depicted in Figure 5.1, is described in [2].

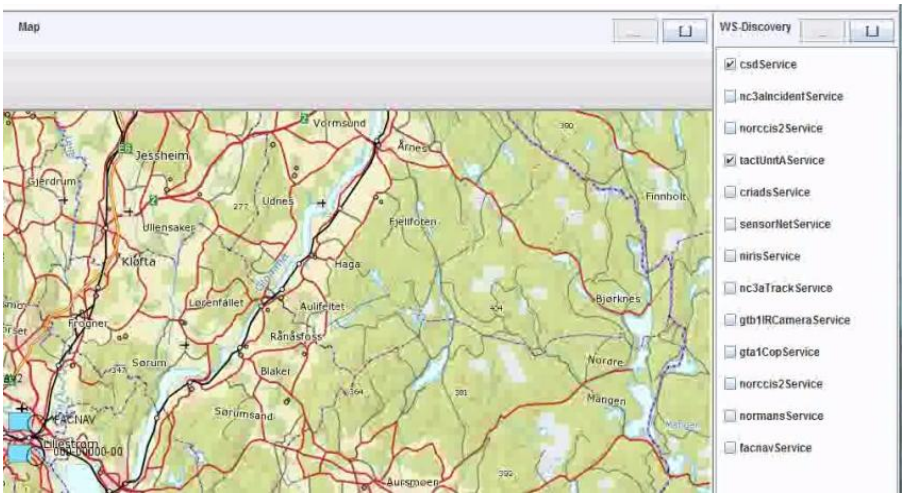

Figure 5.1 Part of the Viewer showing available services

5.2 Publish/Subscribe

Publish/subscribe is a communication pattern for event-driven, asynchronous communication. As opposed to a polling mechanism based on traditional request/response, it saves the client from continuously asking for news as shown in Figure 5.2. Compared to a general push mechanism the benefit is in that you may select what information you want to receive. The pattern minimises traffic on the messaging infrastructure through the use of event-driven notification of changing data, and is particularly well suited in situations where information is produced at irregular intervals.

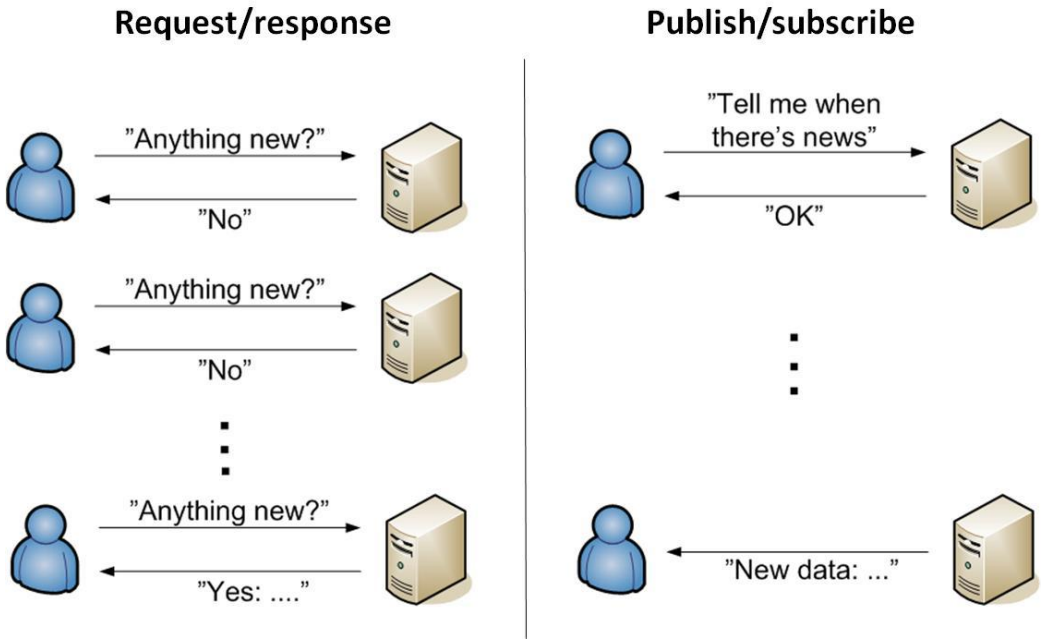

Figure 5.2 Interaction patterns request/response and publish/subscribe

The recommended standard [1] for publish/subscribe as a core service, is WS-Notification. In the SOA pilot a freely available university implementation was used, proving the concept and providing technical lessons learned. Technical details are given in [2].

FFI has since then developed its own implementation of WS-Notification, and will continue focusing on publish/subscribe as an important interaction pattern in future experiments.

5.3 Multilevel Security

FFI has implemented a basic proof-of-concept prototype of a potentially certifiable workstation for handling multiple security classifications. It was demonstrated as part of the SOA Pilot, solving the problem of comparing recent images from the Mission security domain to older images made available on the National security domain. Figure 5.3 shows the Mission window filled with the recent image to be investigated, presented on the desktop labeled National while the user is locating the same position in a reachback image.

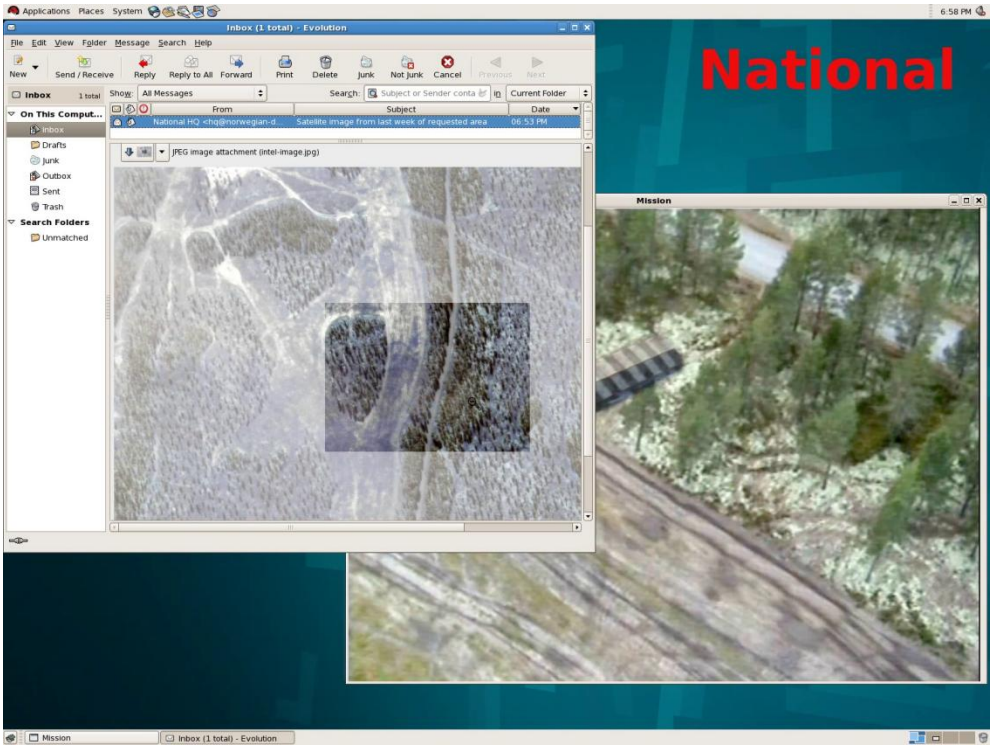

Figure 5.3 Screenshot: Comparing images from different security domains.

The prototype is based on the use of a MILS (Multiple Independent Layers of Security) separation kernel. An important premise is having a secure way to share the keyboard, mouse, and screen between partitions, preventing data flow between classification levels. Figure 5.4 illustrated the principles of the design. More details are given in [5].

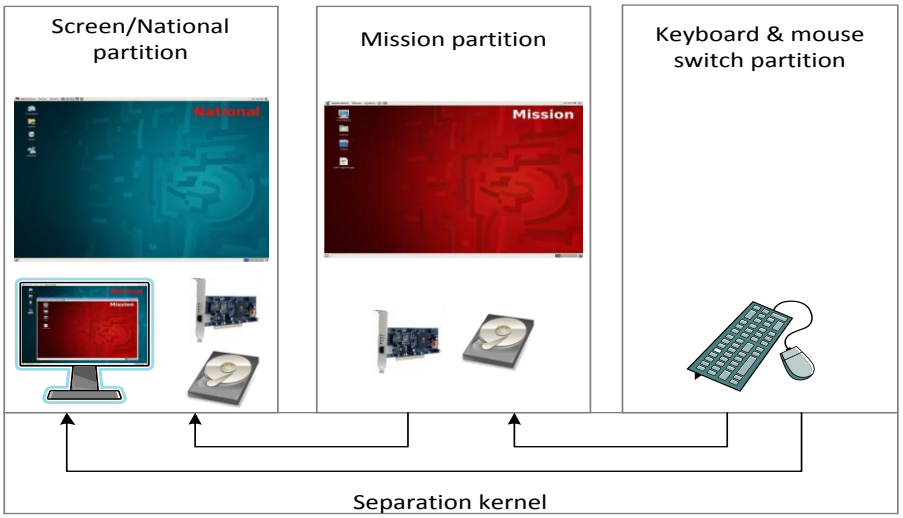

Figure 5.4 MILS configuration used in the SOA Pilot

5.4 Threat Detection using Semantic Technologies

When conducting a coalition operation like the one outlined in Section 3, one of the big challenges is handling the large amount of information that is being shared. As an example in this case, the amount of events received at TU A HQ through its subscription to information from JOCWatch is too large for an operator to manage and align with information from other information sources.

Semantic technologies is a family of information technologies that utilise formal models (ontologies) in order to capture the meaning of the information. Through the ontologies, the meaning is captured in a way that computers can manage and process, and this makes it possible to build systems that can both integrate information from unanticipated information sources and also infer the existence of hidden information on the bases of the integrated information and the meaning captured in the ontologies.

In the context of the pilot, the key to utilise semantic technologies was an ontology that formally captured the notion of how a military unit can pose a threat to another military unit. A multi-agent system based on semantic technologies could then integrate information from several sources, and, on the basis of the integrated information and the threat ontology, infer that there was a possible threat to own unit GTA1.

Figure 5.5 shows a screenshot providing information to the decision maker regarding what information sources the warning was based on and an explaining why this information indicated a possible threat.

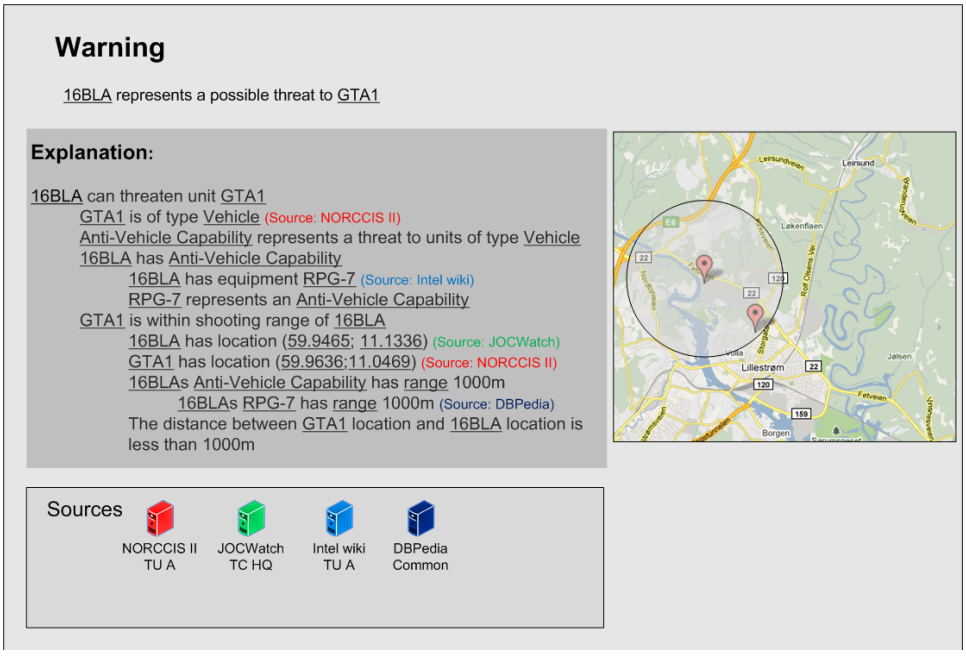

Figure 5.5 The explanation of the warning provided to the TU A commander

More technical details about how this was implemented for the SOA Pilot can be found in [2].

5.5 Chat services

The ability to exchange textual messages, i.e. to chat, is considered important from an operational point of view. Chat functionality has become accepted as a basic requirement, and is gradually being fielded as a part of modern military systems.

For the SOA Pilot, chat was a functional requirement to the Viewer, ref section 4.1.1.4. Chat is also an essential part of the information sharing capabilities of the core collaboration services as described in [1]. The recommended standard XMPP (Extensible Messaging and Presence Protocol) was used in the implementation.

5.6 Disadvantaged Grids

As a means to extend information service availability towards the tactical level, and ultimately all the way down to each soldier, substantial research efforts have been directed to the area of disadvantaged grids. The term implies communication networks (grids) that perform poorly on one or more of properties like bandwidth, latency and reliability. Traditional radio networks typically suffer from such disadvantage.

In the pilot there was a scene where the network of sensors (Sensornet) triggered an event when GTB1 passed through the area under surveillance. From the network diagram in Figure 4.3 we see that the connectivity to Sensornet was set up via the MRR radio, which delivers poor quality IP connectivity.

The point of including disadvantaged grids in this setting, is to illustrate the technical possibility of extending IP connectivity and web service functionality down to low network quality levels.

5.7 Cross Domain Information Exchange

When soldiers of GTA1 dismounted from their vehicle, they entered a less restricted security domain. The operational reasoning for this was to reduce the consequences of eventual loss of equipment while dismounted. This situation imposes the need for information exchange across security domain boundaries, preventing information leakage from high to low.

This cross domain information exchange was handled by an XML/SOAP guard. The premises for the guard are that there is metadata describing the protection needs for each data object. These descriptions are securely bound to the object as a confidentiality label, and the guard can execute the release of each object according to its label. More about the guard implementation can be found in [4]

In the SOA Pilot example, positions within the ground team had a lower classification than the Mission Secret used throughout the coalition. When dismounted it was shown that the soldiers did not have access to Mission Secret, and only blue dots within the team remained in their Viewer, while soldier positions were available to the coalition.

5.8 SOA Infrastructure

In damage assessment, the SOA Pilot presentation made a crucial point of having a set of independent images available a very short time after weapons were launched. The enabling technology was meant to be perceived as the SOA infrastructure, combining network connectivity and a set of interoperable services into the resources needed for flexible information exchange.

The SOA infrastructure is often described as a set of core services. In [1], the Baseline SOA infrastructure is described like in Figure 5.6 with implementations from the following nine core services:

- Messaging
- Publish/subscribe
- Translation
- Enterprise Service Management (ESM)
- Collaboration
- Service discovery
- Service security
- Metadata registry
- Enterprise directory

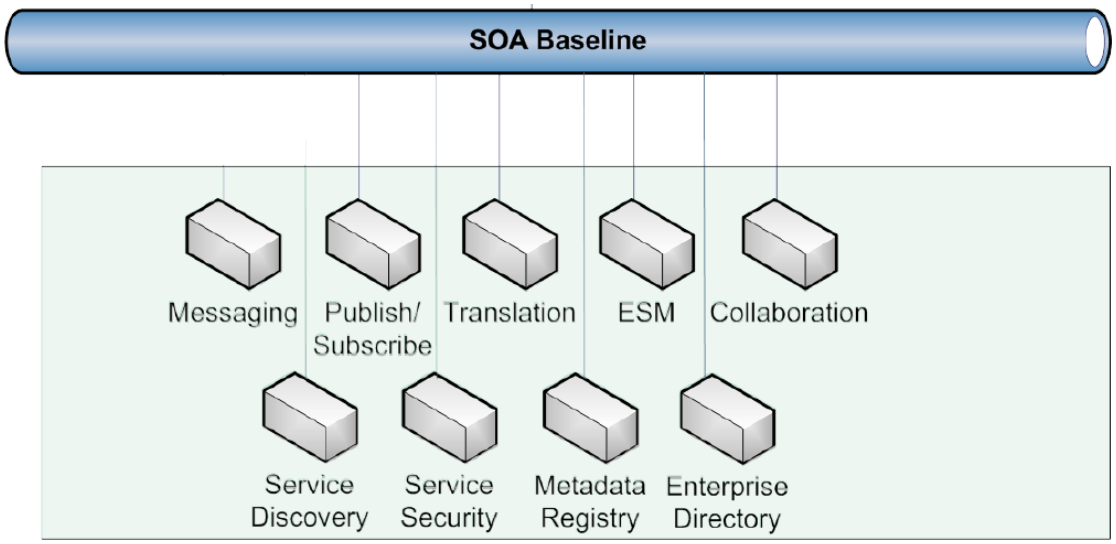

Figure 5.6 Core Enterprise Services - Basic SOA Infrastructure (figure from [1])

Compared to the 14 services listed in the initial CES framework, this leaves out the following five as not being part of the baseline: Information discovery, application, storage, composition and transaction. These five are still lacking recommended standards for implementation as given in [1].

The SOA Pilot was a showcase for a shared SOA infrastructure where legacy systems were included. It intended to show the operational value of flexible information exchange, aiming to have information available to everyone who needs it.

5.9 Role Based Access

The final scene of the SOA Pilot was a demonstration of how federated identity can be used within a coalition. More specifically, it was shown how a federated identity solution based on open standards was used to enable Norwegian access a coalition service provided by NATO.

Figure 5.7 shows the following process:

1) Norwegian client accesses NITB (NATO Intelligence Tool Box) logon
2) Request is redirected to NATO Identity Provider (IdP), asking for security token (yellow line)
3) NATO IdP redirects to Norwegian IdP which authenticates via Norwegian domain controller
4) Request returns back to NITB via NATO IdP, with valid token
5) Client uploads image to NITB. Key here is the trust between the two identity providers

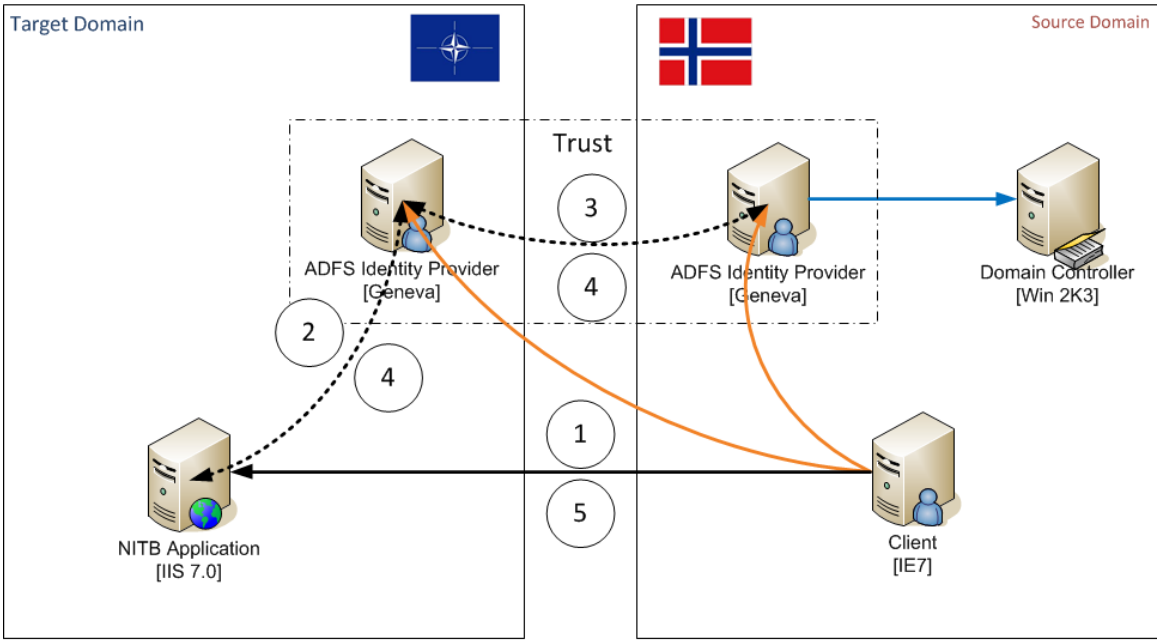

Figure 5.7 Accessing NITB using federated identity (slide from NC3A)

Using such a solution, a user can be granted specific access to a service based on his/her attributes or roles. An advantage of this is that the service itself does not need to have prior knowledge of each potential user.

6 Reflections

After the SOA Pilot presentation there was an interactive discussion session with the audience, focusing on the experience gained from the development work. These are the main points from that discussion.

The numerous practical implications of creating a demonstrator like the SOA Pilot were briefly mentioned. The skills needed to set up and use legacy systems, limitations in physical radio coverage, and the problem of making all the experimental implementations run successfully at the same time, are some of the practical problems that were dealt with. Also, lack of available alternative implementations following the WS-notification standard was a challenge. To avoid the risk of technical errors destroying the effect of the official presentation, it was decided to present video capture of previously recorded computer screens instead of a live demo during presentation.

Although presented in an operational setting, the experience gained from the SOA Pilot was on the technical level. The elements of the demonstrator was referred to the NNEC framework as shown in Figure 6.1, and shortcomings in the area of Service Management & Control were mentioned as a lesson learned. Service access control and authorization mechanisms, as well as sharing of data structures, interface descriptions and other metadata, are important areas that need to be addressed.

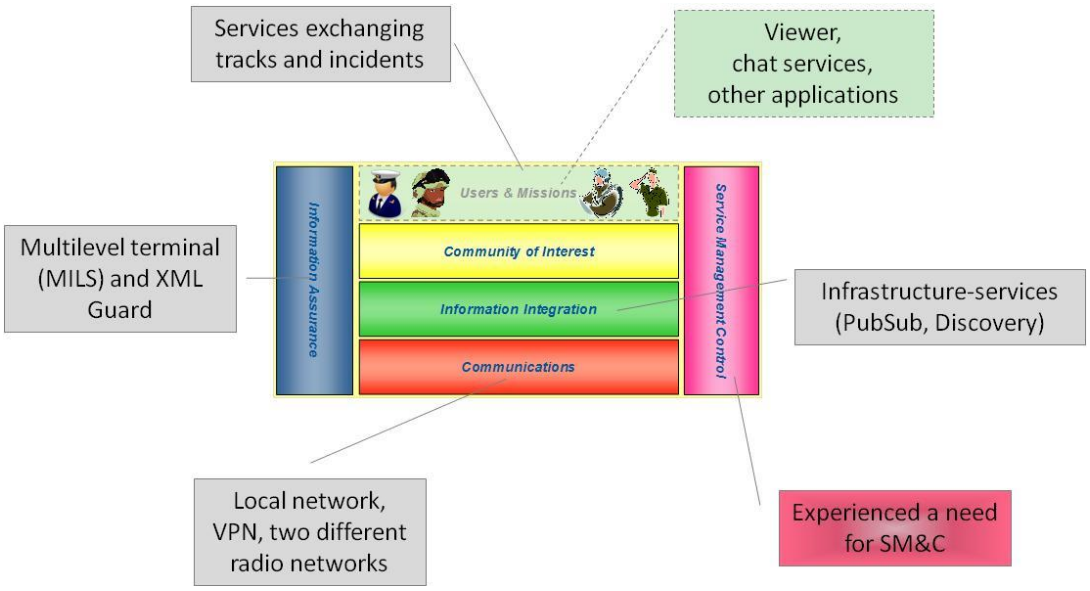

Figure 6.1 Reference to the NNEC framework

The SOA Pilot focused on service enabling using web services. Information was primarily exchanged using publish/subscribe, and there were only a few functional services reporting tracks and incidents. This implies that the pilot covers only a small part of the service orientation universe, but was nevertheless an important exercise in trying out important new standards and recommendations.

The information flows in the demonstrator were mainly one-way. The viewers were the only information consumers. It was stated that the efforts needed to make a legacy system act as a service consumer, would normally be substantially bigger than what it takes to service-enable an output functionality from the same system. In general, services that consume information are best created by the system vendor or someone who knows the system from inside.

Composability of services was briefly discussed, pointing to the potential benefits of reusing modular services, orchestrating them into more complex functionality. In future systems, offering a combination of consuming and information exporting services, one can imagine easy-to-use orchestration tools creating powerful composite services.

It was discussed whether service-orientation would lead to increasing importance of a system integrator role, as opposed to the traditional system owners. With an infrastructure of core services being built across and in between the functional areas of the classic systems, this may become an important issue over time.

One of the main messages from the presentation was that a shared SOA infrastructure enables flexible information exchange. It was pointed out that the technical ability of exchanging all available information between all parties will result in information overflow if not properly managed. Circular flows of information must also be avoided. It was mentioned that reusable correlation services could be very beneficial.

It is important to consider how to make proper use of new technical possibilities. Technology enables new ways to operate, thus implying changes to future user requirements. The user needs of tomorrow are generated by technology enablement of today. For optimal effect, iterations between bottom-up (enablement) and top-down (focusing on user needs) are recommended over time.

Finally, the different valuable aspects of an effort like the SOA Pilot was pointed out: Developers gain hands-on technical experience, in this case also involving existing legacy systems. The audience is given realistic examples of how the enabling technology can be used to create value for the operational user. Researchers also were thankful for the opportunity to learn more about the situation of the users.

7 Recommendations and conclusions

The SOA Pilot aimed to demonstrate some of the benefits of using a service-oriented architecture. A number of existing military operational systems were service-enabled and connected in a shared SOA infrastructure, making the systems share information using services.

In retrospect it is easy to conclude that the SOA Pilot was a successful initiative. It was a great learning experience, it proved the viability of the technical standards that were used, and

hopefully it increased the awareness among the audience of what can be made possible by the use of these technologies.

From FFI we strongly believe in continuing this path of experimentation. Results so far show no reason why the technical principles and solutions exemplified by the SOA Pilot should fail as building blocks of the future. There are obvious discussion points when it comes to “how fast” and “how much”, but the direction seems to be given, and further exploration should not be unnecessarily postponed. Skills need to be developed. We recommend for the information systems development organization of the Norwegian Defence to start implementing SOA and core services where applicable.

A primary recommendation for further research is to look for a system or ongoing development effort that would benefit from applying some of the principles from the SOA Pilot, and make a joint effort. Using technical skills from research in gaining experience in development as well as experimental use of a SOA infrastructure, will hopefully create results in line with what we achieved from the SOA Pilot.

Publish/subscribe is very promising, and should be pursued. As an interaction pattern, it needs a number of enabled communication partners before it gets interesting. Early adoption into some of our operational systems could prove very valuable in the long run.

Other baseline core services are also ready for implementation according to NATO recommended standards. They constitute an excellent foundation for future experimentation efforts.

As a conclusion is seems fair to state that the SOA Pilot was considered an important contribution to technical experience and transfer of knowledge about how service orientation can play an important role in the process towards Network-based Defence.

References

[1] ” Core Enterprise Services Standards Recommendations - The SOA Baseline Profile version 1.7”, dated 11.11.2011

[2] K. Lund et al, ”SOA Pilot 2011: Service infrastructure”, FFI-report 2011/02235

[3] J. Halvorsen, B. J. Hansen, “Integrating Military Systems using Semantic Web Technologies and Lightweight Agents”, FFI-notat 2011/01851

[4] R. Haakseth, “SOA Pilot 2011: Demonstrating secure exchange of information between security domains, FFI-report 2012/00117

[5] N. A. Nordbotten, T. Gjertsen, “Towards a certifiable MILS based workstation”, FFI-report 2012/00049

Abbreviations

AIS	Automatic Identification System for ships, introduced by the UN's International Maritime Organisation (IMO)
BMS	Battlefield Management System
BRITE	Baseline for Rapid Iterative Transformational Experimentation
C2	Command and Control
C3	Consultation, Command and Control
CES	Core Enterprise Services
COP	Common Operational Picture
CRIADS	Coastal Radar Integration and Display System
CSD	Coalition Shared Database (aka Coalition Shared Data server)
ESM	Electronic Support Measures (alternative meaning: Enterprise Service Management)
FAC	Forward Air Controller
HQ	Headquarter
JOC	Joint Operation Center
MAJIIC	Multi-sensor Aerospace-Ground Joint Intelligence Surveillance and Reconnaissance Interoperability Coalition
MCCIS	Maritime Command and Control Information System
METOC	Meteorology and Oceonography
MILS	Multiple Independent Levels of Security
NC3A	Nato C3 Agency
NC3B	Nato C3 Board
NITB	NATO Intelligence Tool Box
NNEC	Nato Network Enabled Capability
NORCCIS	Norwegian C2 Information System
NORMANS	NORwegian Modular Arctic Network Soldier
RMP	Recognized Maritime Picture
SOA	Service-Oriented Architecture
TDL	Tactical Data Link
UAV	Unmanned Aerial Vehicle
VPN	Virtual Private Network
XML	Extensible Markup Language