FFI-RAPPORT

16/02314

Core services

recommendations and trends

—

Trude H. Bloebaum
Frank T. Johnsen
Ketil Lund
Marianne R. Brannsten

Core services
recommendations and trends

Trude H. Bloebaum
Frank T. Johnsen
Ketil Lund
Marianne R. Brannsten

Norwegian Defence Research Establishment (FFI) 20.12.2016

Keywords

Tjenesteorientert arkitektur
Kjernetjenester
Informasjonsinfrastruktur

FFI-rapport

FFI-RAPPORT 16/02484

Project number

1277

ISBN

P: 978-82-464-2874-1
E: 978-82-464-2875-8

Approved by

Bjørn Jervell Hansen, *Research Manager*
Anders Eggen, a*vdelingssjef/Director*

Summary

This report provides an overview of results and recommendations within the area of service-oriented architecture (SOA) from FFI project 1277 Information and integration services in the information infrastructure. The project consists of two parts, one focusing on semantic technologies and one focusing on SOA. The results from the work on semantic technologies are presented in a separate report.

The main objective of the project was to support the Norwegian Armed Forces in its work on developing network-based defence (NBD), by investigating technological solutions that can contribute to the development of a common information infrastructure (INI). As SOA is key to the development of INI and NBD, the project has contributed to further testing and improvement of core services, with the work done within NATO as a starting point.

The research activities within the SOA areas have mainly been performed as collaborative research, often within the context of external research activities involving groups from other nations and/or organizations.

The report provides an overview of the main findings within our research areas. We give a short description of the different arenas of cooperation we have worked within, as well as results and recommendations from what is our main focus, namely core services in the information infrastructure. This part is more technically oriented. For further details, we refer to the appendices, as well as the other publications from the project.

Sammendrag

Dette dokumentet gir en oversikt over arbeidet som er gjort innen tjenesteorientert arkitektur (SOA) i FFI-prosjekt 1277 Informasjons- og integrasjonstjenester i INI. Prosjektet er todelt, med en del som har sett på SOA og en som har fokusert på semantiske teknologier. Resultatene fra sistnevnte del er presentert i en egen rapport.

Det overordnede formålet med prosjekt 1277 har vært å støtte Forsvarets arbeid med å utvikle Nettverksbasert Forsvar (NbF) gjennom å utforske teknologiske løsninger som bidrar til utviklingen av en felles informasjonsinfrastruktur. Innenfor området SOA skulle prosjektet bidra til videre utprøving og foredling av kjernetjenester, med utgangspunkt i arbeidet som gjøres innenfor dette feltet i NATO. Løsninger som ble sett på i den sammenheng vil vurderes for bruk også i en nasjonal SOA-infrastruktur.

Mye av forskningsarbeidet i prosjektet er gjennomført gjennom deltakelse i nasjonale og internasjonale fora, hvor vi har samarbeidet med andre forskningsgrupper.

Rapporten gir en oversikt over hovedfunnene innen vår forskningsområder. Den gir en kort beskrivelse av de ulike samarbeidsarenaene vi har hatt aktiviteter på, samt resultater og anbefalinger innenfor det som er vårt sentrale fokus, nemlig kjernetjenester i informasjonsinfrastrukturen. Denne sistnevnte delen er noe mer teknisk rettet. For lesere som ønsker ytterligere detaljer henviser vi til vedleggene samt øvrige publikasjoner fra prosjektet.

Content

1 Introduction

This report provides an overview of results and recommendations within the area of service-oriented architecture (SOA) from FFI project 1277 – *Information- and integration services in the information infrastructure*. The project consists of two parts, one focusing on semantic technologies, and one focusing on SOA, and it started in March 2013 and ran until December 2016. The research activities within the SOA area has mainly been performed as collaborative research, often within the context of external research activities involving groups from other nations and/or organizations.

The main objective of the project was to support the Norwegian Armed Forces in its work on developing network-based defence (NBD), by investigating technological solutions that can contribute to the development of a common information infrastructure (INI). SOA is key to the development of INI and NBD, and it has therefore been an important goal for the project to ensure that FFI maintains a high level of competence in this area. In addition, the project has contributed to further testing and improvement of core services, with the work done within NATO as a starting point.

In particular, SOA has been chosen by the NATO C3 Board as the method to achieve interoperability at the information infrastructure level. However, the current technologies used to implement SOA (e.g. Web Services, which is our focus) were not specifically designed to handle the conditions found when working with tactical networks. This fact remains a major impediment to achieving interoperability among the nations in the battle space.

The purpose of this report is to present the results from the SOA part of the project, as well as to point to the publications produced by the project within this area.

The remainder of this report is organized as follows: In Chapter 2 we present the different activities that the SOA part of the project has been involved in. Next, in Chapter 3 we present the main results and recommendations that have come out of our research. We have chosen to structure this section according to the different core services that we have looked into, with one subsection for each core services. In Chapter 4 we present what we consider to be the most important trends at the moment, giving recommendations on where research efforts should be focused in the coming years. We then conclude in Chapter 5.

Appendix A provides a more detailed presentation of the demonstration and experiment performed within the NATO IST-118 group (SOA Recommendations for Disadvantaged Grids in the Tactical Domain), while Appendix B presents more details from the LINE experiment performed at FFI in November 2015. Appendix C contains a list of all publications from the project.

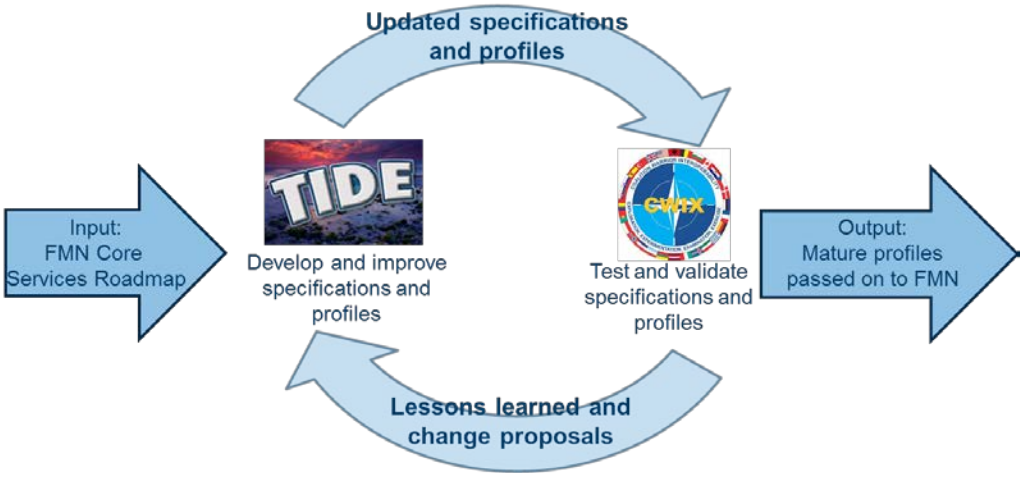
2 Activities

In the project, we have been working on a quite large number of different activities, but they all contribute to the research on our main topics, namely interoperable core services and core services in tactical networks. This chapter presents the different activities and arenas that the SOA part of project 1277 has been involved in, both nationally and internationally.

2.1 CWIX and TIDE

The Information and Integration Services research program at FFI has participated in testing events at the Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX) for a number of years, primarily in order to support the work on developing core services specifications for Federated Mission Networking (FMN). This work has so far been done primarily by the Technology for Information, Decision and Execution (TIDE) Technology Track, in which we participate. This community develops and improves profiles for how to use a number of core services standards in a federation context.

CWIX, and the SOA focus area in particular, is the primary testing arena for the TIDE Technology Track. During the experimentation at CWIX, valuable feedback on how well the specifications and profiles function as interoperability enablers is captured. This feedback is processed by the TIDE Technology community, which uses this information to improve the specifications and profiles. When the profiles, normally after multiple iterations of testing at CWIX, reach a high degree of maturity they are passed on to the FMN community for potential inclusion in future FMN spiral specifications. The interactions between these two communities are illustrated in Figure 2.1.



Updated specifications and profiles
Input: FMN Core Services Roadmap
TIDE
Develop and improve specifications and profiles
CWIX
Test and validate specifications and profiles
Output: Mature profiles passed on to FMN
Lessons learned and change proposals

Figure 2.1 Interactions between the TIDE Technology Track and the CWIX SOA focus area

During the last three years, FFI has participated at CWIX with a primary focus on the core services specifications for messaging services and web authentication. The main findings from these experiments are included in Chapter 3 below, and described in more detail in [1][2][3].

Experiences from CWIX and TIDE are brought into the FMN processes through our collaboration partners in NCIA, and are also reported in FFI publications. In addition, the experiences are used to support the Norwegian Armed Forces in their FMN work.

2.2 IST-118 – SOA Recommendations for disadvantaged grids in the tactical domain

IST-118 “SOA Recommendations for disadvantaged grids in the tactical domain” is a NATO STO research task group working under the IST-panel. The focus of this group was to provide recommendations on how one can support the various core services required in a service-oriented system when the system is deployed in the tactical domain.

IST-118 provides guidance on which technical modifications should be utilized in several different types of tactical networks which are utilized by NATO member nations. The work of the group was based on the standardization and profiling work done elsewhere in NATO (for instance through TIDE and CWIX as described above), and extends on this work by giving recommendations for tactical adaptations.

The work of IST-118 has been documented in a number of publications, and the group’s final report [4] gives an overview of the results. IST-118 has also arranged a number of demonstrations and workshops, which are described further in Appendix A.

2.3 Coalition Network for Secure Information Sharing II

Coalition Network for Secure Information Sharing II (CoNSIS II) is a multilateral cooperation project based on a signed Memorandum of Understanding (MoU) between the Ministries of Defence of Germany and Norway. The objectives of this project has been to develop, implement, test, and demonstrate technologies and methods that will facilitate the participants’ abilities to share information and services securely in ad-hoc coalitions, and between military and civil communication systems, within the communications constraints of mobile tactical forces.

The external funding that FFI received for CoNSIS II was primarily intended for cooperation with the industry, while FFI contributed with an equivalent amount of money through research work. We originally planned for three phases in CoNSIS II, with one announcement for industry participation per phase. However, as CoNSIS II was later shortened to two years, the number of phases (and announcements) was reduced to two.

In CoNSIS II, our emphasis has been on testing different NATO standards for core services in the tactical domain. As a result, we have gained much experience within some areas (e.g., publish/subscribe) and less in others. Our goal was therefore to cooperate with the industry within areas where our experience was limited, and for the first announcement we wanted a study that focused on the following two areas:

- The use of policies in negotiations as part of invocation of services
- Service discovery in tactical networks

For policies, there were two areas that we wanted surveyed, namely security (authentication, authorization, confidentiality, etc) and adaptations for tactical networks (negotiations between service consumer and service producer). In particular, we wanted an investigation into WS-SecurityPolicy.

The work on service discovery was intended to be closely related to the work on policies, and more concretely, we wanted to find out what information, beyond the service descriptions (WSDLs), that was necessary in order to use policies in conjunction with service discovery. In other words, what information must be included in the service description in order to use policies both for selection of services, and for negotiating a service contract.

The first announcement for industry participation was made in the autumn of 2014, and was won by Saab Technologies Norway AS. As Saab has much experience within both SOA and tactical systems, our goal for the cooperation with Saab was primarily to tap into this experience. At the same time, Saab would get a better insight into systems and standards used by NATO, and thereby have an opportunity to improve interoperability towards NATO.

The work within this first announcement took place from December 2014 until June 2015. FFI and Saab had regular meetings (both telephone and physical) during the period, in order to ensure that the work maintained the correct focus. At the end of the cooperation, a workshop was arranged on June 3 2015 at FFI, where Saab delivered their final report and presented their work. The main results from this report are presented in the CoNSIS II final report [5].

For the second announcement, we wanted to focus the funding on one particular area, namely publish/subscribe. NATO has chosen WS-Notification as their standard for publish/subscribe, but the lack of implementations of this standard is a considerable problem. At FFI we have been using two implementations, microWSN and WS-Nu [32]. Both are developed in-house, and both are prototypes and only meant for experimentation. We therefore wanted to use the funding for the second announcement to provide a more complete implementation of the standard, to be able to perform more comprehensive testing together with our partners.

The second announcement for industry participation was made in the autumn of 2015, and was once again won by Saab Technologies Norway AS. The work started in January 2016, and the implementation was delivered from Saab in time for CWIX 2016 in June. During this period there were regular meetings between FFI and Saab.

The implementation delivered by Saab was based on Apache CXF, and was used by FFI at CWIX 2016. This was described in Section 2.1

2.4 LINE

In November 2015, FFI conducted an experiment using autonomous Unmanned Aerial Vehicles for geo-location of navigation radars. This was an interdisciplinary experiment that included a number of different research communities, and which contributed to a number of different research areas. The experiment was carried out with two UAVs operating out from Ørland main air base in Norway, the INI-lab at FFI acting as the ESM operation center, and with network connection to the Norwegian Joint Headquarters (NJHQ)

The experiment demonstrated how a continuous data flow can be established, from sensors, via an operation center, and all the way to a joint headquarters. In addition, it showed how sensor data from different sources can be integrated. Project 1277 contributed to this work by establishing the necessary services to enable the information flow from the operational area into the operation center, as well as the integration of different functional area services, and the communication from the operation center to the joint headquarters.

For more information about the LINE experiment, we refer to Appendix B.

2.5 Student supervision

In addition to the research performed by the researchers in the SOA part of project 1277, the researchers also engage in supervision of students both at the bachelor and master degree levels. These student activities give a noticeable benefit to the results produced by the project, as many of the student activities have been involved in building prototype systems that have been used to support the project activities.

Title	University	Year	Ref
WS-Nu	NTNU	2014	[32]
Situation Awareness and Incident Reporting	NTNU	2015	-
OKSE - WS-Notification and AMQP publish/subscribe interoperability broker	NTNU	2015	[29]
COPS - Common Operational Picture Secured	HiOA	2015	[33]
Interoperable NATO Track Entry Log	NTNU	2016	[37]
Project Flagpole	NTNU	2016	[38]
OKSE 2.0 Protocol Mediator	NTNU	2016	[39]
CAGED - Communication Application With geographical element data	Westerdals ACT	2016	[40]

Table 2.1 Overview of bachelor degree projects supervised

Table 2.1gives an overview of all the bachelor degree projects that we have supervised, while Table 2.2 shows all the master degree projects. Finally, we also supervised a student, Magnus

Skjegstad, for the degree of Philosophiae Doctor. His dissertation was in 2014, and the title of the work was “Towards Robust and Delay-Tolerant SOA with Web services in Highly Dynamic MANETs”. The work is summarized in [6].

For further details on how these student projects have supported our project activities, we refer to the next chapter, where the student results are presented together with our other results.

Title	Student	Time period	Ref
Efficient SOAP messaging for Android	Eggum, Dag Ove	2013 - 2014	[34]
PISA—The Platform Independent Sensor Application	Krogh, Mikael André	2013 - 2014	[35]
Federated Service Discovery - Interconnecting different Web Service Discovery Mechanisms	Thuen, Andreas	2014 - 2015	[36]
Improving the performance of Web Services in Disconnected, Intermittent and Limited Environments	Lindquister, Joakim J	2015 - 2016	[10]
HCI challenges for smart military situational awareness applications (arbeidstittel)	Frøseth, Ida Marie	2016 – 2017	-

Table 2.2 Overview of master’s degree work related to project 1277

3 Core services

Our work was focused on generating recommendations for a subset of the core services from the NATO C3 taxonomy. The availability of SOA at the tactical level (partly) removes the need to develop and implement separate HQ and tactical versions of the same functionalities, thereby reducing cost, both of research and development, as well as training.

Core services form the basis for other, more special-purpose services (i.e., COI-enabling services, which again form the basis for COI-specific services, and so on). We have looked into applying a subset of the core services to the tactical domain, with the aim of providing recommendations for deployment of said services based on our experiences and experiments.

Specifically, we have chosen to pursue messaging services (request/response and publish/subscribe communication paradigms), service management and control (the service discovery aspect), information assurance (limited to single-sign-on standards) and finally unified communication and collaboration services (the chat and, in collaboration with the University of the West Scotland (UWS), streaming video aspects of such services). These services were chosen because they provide basic and essential functionality, and were also within the time and resource scope of the project to experiment on, either nationally or in multi-national settings. But, that is not to say that other services not included here shouldn’t be employed in the tactical domain.

For each service we give an introduction to the service category, what the main challenges and possible optimizations are, how we have contributed, as well as recommendations and possible ways forward.

3.1 Messaging services

Messaging services are the services that support the basic information exchange between entities in a service-oriented system. They can be implemented using a number of different technologies, and different message exchange patterns can be supported. In this chapter we summarize the work performed in support of both request/response services and publish/subscribe services.

3.1.1 Request/response

Request/response is a messaging pattern in which the entity seeking information, the client, sends a request message to the information source, and gets a response back. This basic messaging pattern is also known as “client-server” or “pull”-pattern.

3.1.1.1 Which standards are used?

In Web Services, as defined by the W3C, request/response messaging is done using the Simple Object Access Protocol (SOAP), which exchanges XML formatted messages between entities in a transport-agnostic manner. The TIDE Transformational Baseline (TTB) [7] points to these same standards, along with the WS-I Basic Profile for interoperability. The current version of the TTB does not address request/response messaging, but the in-progress version 4.0 includes profiles for both SOAP and REST Web Services. We have primarily focused on SOAP-based request/response services, though we have also performed some early performance comparisons between SOAP and Representational State Transfer (REST)-based services.

3.1.1.2 What are the main challenges for this service in the tactical domain?

In Web Services based on SOAP, all messages follow the XML standard, which is text-based, and formats messages so that it is easily readable both for machines and humans. This makes XML fairly verbose, with a significant message overhead.

The SOAP standard is transport agnostic, meaning that its messages can be transmitted using any transport protocol. However, the vast majority of Web service implementations use HTTP over TCP as their transport mechanism. This is partly due to the fact that many development tools only support this standardized SOAP binding. TCP is a connection-oriented protocol, and relying on this as the transport mechanism means that services and clients must be available at the same time, and that a connection between them must be established and maintained. In networks where both disruptions and long delays are common, relying on such end-to-end connections is a limiting factor.

3.1.1.3 Which optimizations are possible?

In order to overcome the issue of XML messaging overhead, the XML messages can be compacted using either a generic loss-free compression mechanism or a binary XML encoding that also reduces the message size. Using alternate data models, which express the same information more compactly is also possible, but might lead to information loss.

The issues stemming from the use of HTTP over TCP as the transport mechanism for SOAP, can be addressed in several ways. This includes tuning the performance of the HTTP and TCP protocols, replacing the standard TCP implementation with other TCP flavors, or replacing the transport mechanism with one that is more suitable for use in tactical networks.

3.1.1.4 Contributions in the field of request/response services

The work done on request/response services is based on the work FFI did in the context of two NATO RTG-IST groups, namely IST-090 (“SOA Challenges for real time and disadvantaged grids”) and IST-118 (see Section 2.2). Here, we recommended that the services optimizations should be done in proxies in order to retain interoperability with standard Commercial off-the-shelf (COTS) services. Then, a partner nation (Poland) investigated the edge proxy concept with AFRO [8], while FFI pursued proxy pairs/network of proxies with DSProxy [9].

Since then, we have implemented a proxy pair adhering to the recommendations from these NATO groups. This proxy pair ensured that COTS services could function in disconnected, intermittent and limited (DIL) environments. The novel part here was that in this proxy version the delay and disruption tolerance was implemented supporting HTTP rather than SOAP. This meant that the proxy approach was shown to function for both SOAP and REST services, which typically both use HTTP for transport. The proxy implementation and evaluation is further described in [10].

Performance tests involving SOAP Web Services (which use XML), compared to REST with XML and REST with JavaScript Object Notation[1] (JSON) show that REST is preferable from a pure performance point of view, whereas SOAP’s strong points are standardization and interoperability [11].

Follow-up work evaluating SOAP and REST on the Android platform showed similar results, in that consuming REST services consumed less power (leading to increased battery life) than consuming SOAP services [12].

[1] JSON is a data-interchange format that is easy to read and write for humans and easy to parse for machines. For more information, see http://www.json.org/

Recommendations for request/response services

General recommendations include using filtering and compression to reduce overhead, and tuning transport protocols and application servers to better fit the underlying transport medium. In order to retain COTS compatibility in both clients and services, we recommend putting proprietary optimizations in proxies between said clients and services.

With respect to which implementation technology to use where, recommendations from our study on Android [12] are as follows:

Overall goal	**Recommendation**
NATO interoperability	SOAP
Machine-to-machine infrastructure services	SOAP (or REST, maybe wrapping the SOAP service)
Functional area services	SOAP (or REST, maybe wrapping the SOAP service)
Smart device clients	REST
Non-smart device clients	SOAP (or REST, if the client is written in JavaScript)

Table 3.1 SOAP vs REST recommendations

3.1.1.5 What is the way forward?

Through this and previous projects (e.g., project 1176 – "Service orientation and semantic interoperability in INI") we have thoroughly studied optimizations for SOAP request/response services. Our recommendations can be used to help deploy systems involving this technology. However, with the increasing popularity of REST services it would make sense to study these further in a similar manner as we have done for SOAP services.

3.1.2 Publish/subscribe

Publish/subscribe is a term used to describe a communication pattern in which clients that are interested in a certain type of information subscribe to information of this type. The clients indicate what type of information they are interested in either by using topics (or keywords), content filters, or both. When new information becomes available, the new information is sent to the interested clients based on the subscriptions. The information is sent either directly by an information producer, or via a broker, which can offload producers from the task of doing both subscription management and notification dissemination. As opposed to the “pull”-pattern, publish/subscribe takes a “push”-pattern approach.

3.1.2.1 Which standards are used?

The SOA Baseline [7] points to the standard WS-Notification from OASIS[2] for publish/subscribe between Web Services, and a SIP has been written for this standard. There is also ongoing work within the TIDE community related to producing a WS-Notification-based profile as part of the TTB. Thus, we have focused primarily on WS-Notification in our optimization work. Note that the implementations used have not been tested for full compliancy with the TTB specification, as that profile is currently awaiting verification through CWIX testing.

3.1.2.2 What are the main challenges for this service in the tactical domain?

When using a broker-based approach to publish/subscribe, all information will go via the broker(s), which means that the availability of the brokers might be a bottle-neck. The impact of the non-availability of a broker depends on the broker deployment topology used; whether one has a single-broker deployment or a multi-broker deployment. In a multi- broker deployment, there are different possible topologies, but deploying brokers close to clients and services might help alleviate the issue of broker availability.

The WS-Notification standard specifies that notifications are to be delivered unicast to each client. When multiple clients, connected through the same broadcast-based communications medium, are interested in the same information, this means that several copies of the same notification are sent over the same network, which leads to sub-optimal use of the often limited network resources.

In many cases, the information producer will be located in a non-resource-constrained network, and might not be aware of the network constraints between itself and the client. Using publish/subscribe means that the transmission of notifications is initiated by the information producer (or broker) rather than by the client. This means that the client has no way of controlling when its communication resources are being used, and how often it receives updates.

3.1.2.3 Which optimizations are possible?

The message exchange between the consumers, brokers and producers is done using standard SOAP messages. The registration of publishers and the creation and management of subscriptions are similar to the request/response message exchange, while the distribution of notification messages can be seen as one-way service calls. This means that the SOAP message optimizations recommended for request/response services can and should be applied to the publish/subscribe message exchanges.

[2] Organization for the Advancement of Structured Information Standards, http://www.oasis-open.org

In addition to the optimizations that can be applied to request/response services, there are a number of optimizations that can be done by the publish/subscribe middleware. Some optimizations done at this level are non-intrusive, i.e. they change neither the content of notifications nor which notifications are delivered to the client. This includes changing the behavior of WS-Notification to use multicast delivery of notifications where applicable and replacement of the transport mechanisms used.

In addition to these non-intrusive adaptations, it is also possible to use optimizations that alter some aspect of the message flow between the information producer and consumer. This includes altering the content of the message (for instance through filtering or transcoding of information), altering how notifications are distributed (for instance aggregating many smaller notification messages into one larger message, and thus altering the timeliness of the delivery of information) and also selective dropping of notifications (also known as frequency filtering) to limit how many messages are transmitted over the network. All of these intrusive adaptations require knowledge of how the information is used by consumers, and must be applied selectively.

3.1.2.4 Contributions in the field of publish/subscribe services

The optimizations of publish/subscribe services have been addressed by FFI in the context of IST-118 in a number of experiments, publications, presentations and demonstrations.

We first tested standard WS-Notification without any optimizations in a wireless broadband radio network. The purpose of this test was to determine whether WS-Notification can be used in such networks without any optimizations, and to measure how much resources this consumes. These tests are documented in [13] and show that while WS-Notification functions in these network types without modification, simple transport optimizations should be used to limit the amount of network resources consumed.

Retaining interoperability while performing tactical optimizations is important, and in [14] we combined our work on WS-Notification in wireless broadband radio networks with an interoperability test. Two independent implementations of WS-Notification were used to transfer information through a network that included a wireless broadband radio network where we performed transport level adaptations. This experiment showed that performing these optimizations did not negatively impact interoperability.

An alternative to performing tactical optimizations of the WS-Notification standard is to replace the standard with a publish/subscribe protocol that is more suited to the constraints of tactical networks. In [15] we performed a comparative performance evaluation of three publish/subscribe protocols.

The different types of networking technologies that are used in tactical networks have very different characteristics. In order to be able to give recommendations for more than one networking technology, we performed experiments with WS-Notification in all 5 network configurations. These experiments [16] were performed in an emulated environment based on the CORE network emulator from US Naval Research Laboratory[3].

In Appendix A, we describe a demonstration and experiment where we combine all our previous efforts on WS-Notification into one larger experiment. Two different implementations of WS-Notification were connected in order to show interoperability, while running over a network consisting of both an emulated tactical network and a real wireless broadband radio network.

In addition to the experiments described in the publications referenced above, IST-118 group members have experimented with combining publish/subscribe with cross-layer mechanisms, where each WS-Notification topic was allocated a given amount of resources it was allowed to consume based on the currently available resources. These optimizations were shown during the demonstration session at the ICMCIS conference in Brussels in May 2016.

3.1.2.5 Recommendations for publish/subscribe services

A publish/subscribe service can, simply put, be seen as a reverse request/response service. As such, publish/subscribe services can benefit from the same optimizations as request/response services: Using compression, filtering, etc. In addition, several optimizations can be made specifically for publish/subscribe services. For example, we have, through demonstrations and experiments in context of IST-118 and also CoNSIS II, shown that the family of WS-Notification standards can benefit from applying cross layer optimizations, message aggregation, and multicast distribution of notifications.

3.1.2.6 What is the way forward?

NATO has chosen WS-Notification for publish/subscribe; hence we focused mostly on that standard. The WS-Notification standard is intended for use both in the NATO enterprise and in federated networks. That being said, WS-Notification may not be the best choice for use in tactical networks even though we have shown the feasibility of applying it to such networks in some of our experiments and demonstrations. Also, WS-Notification is not used much in civilian systems, which means that there are few implementations of the standard out there. Hence, we suggest investigating also other approaches to publish/subscribe (e.g., the Advanced Message Queue Protocol (AMQP) and MQ Telemetry Transport (MQTT)) for which there exists many different implementations. If some other solution than WS-Notification proves more efficient in certain tactical networks then it could be suggested for use there, but then one also needs to look into making said protocol interoperable with WS-Notification when such networks need to share information with NATO.

[3] Common Open Research Emulator, http://www.nrl.navy.mil/itd/ncs/products/store

3.2 CIS Security services

Security properties, such as confidentiality, integrity, and availability (CIA) must be supported in order to handle security requirements of services running in the tactical environment. In particular, they need to manage the security requirements of all relevant security levels, and information flow between security domains. CIS Security Services encompass all communication layers, but here we focus on the security aspects related to protecting core services.

3.2.1 Which standards are used?

There are many standards that can be used for securing core services, as Figure 3.1 below shows:

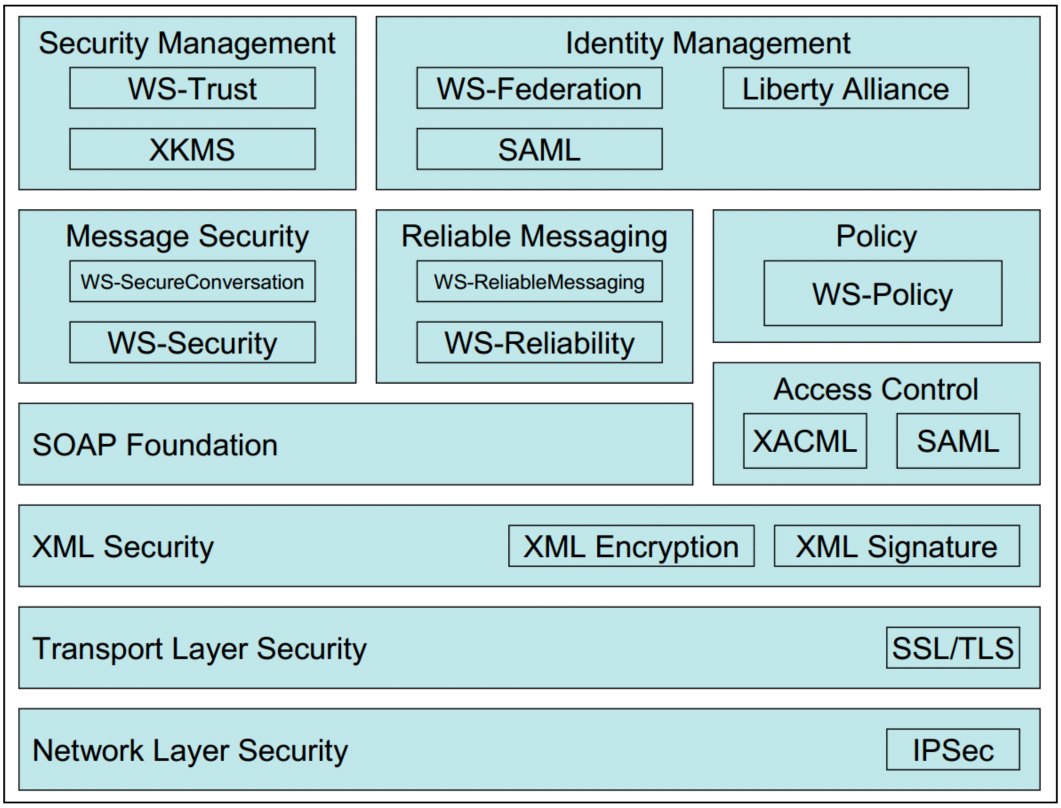


Figure 3.1 Security standards (from [17])

CIS security is a vast field, but, driven by planned CWIX test series, we have focused on a small subset of standards related to identity management and access control. As the figure shows, there are three standards for identity management, of which two are currently considered by NATO: WS-Federation and SAML 2.0. These tie together with the other standards to provide a complete infrastructure for security management, message security, reliable messaging, policies and access control. SOAP is the common protocol and XML the common data format. For an elaborate explanation of how the standards work and tie together, see [18]. We have not considered non-SOAP related standards, and we have not looked into issues with Secure Sockets Layer/Transport Layer Security (SSL/TLS) or IPSec. Also, NATO has recently started looking into securing REST-based services using the Oauth and OpenIDConnect standards, but neither of these has been subject to experimentation within this project.

3.2.2 What are the main challenges for this service in the tactical domain?

The main challenges include using a public key infrastructure (PKI) in DIL environments (certificate distribution, revocation lists, etc.) and the general overhead introduced by adding digital signatures, encryption, and identity management to services. Also, the complex call chains requiring many subsequent synchronous connections to be successful, limit the usability in DIL environments.

3.2.3 Which optimizations are possible?

So far we have only investigated the overhead of security services, which can be deemed considerable. However, we have some suggestions for optimizations that should be pursued: The need for synchronous calls needs to be reduced to a minimum, so one should consider pre-distribution of assets where possible (e.g., certificates), longer timeouts would also help mitigate part of the problem (e.g., increase token validity time). As for the issues of message overhead, one should leverage compression prior to encryption. Also, more compact XML representations of assets that must be distributed (e.g., a more compact signature representation or using an identifier for a certificate that has been pre-distributed rather than including said certificate within every SOAP message) would increase the usability of the security solutions in tactical networks.

3.2.4 Contributions in the field of CIS security services

We focused on a sub-set of the CIS security services, namely aspects related to Single-Sign On (SSO). FFI pursued the SAML 2.0 [19] protocol, whereas a collaboration partner (Poland) investigated WS-Federation [20]. We found that there are issues related to reliance on several synchronous service calls for either protocol to work, and also that there is extra overhead associated with the solutions.

3.2.5 Recommendations for CIS security services

SAML 2.0 seems to be the standard for identity management with best vendor support these days. Hence, we suggest to focus efforts on researching this, as this is most likely to be the standard of choice for SSO for NATO in the future based on results from e.g., CWIX 2015 [21] [22]. Also, we suggest pursuing message-level security in addition to transport or network layer security despite the overhead due to the benefit of achieving multi-hop message level security.

3.2.6 What is the way forward?

An important aspect is the timeframe a security token is valid (“liveness” of the tokens). There needs to be an evaluation of the tradeoff between usability, trust and SSO token liveness. How long should the token be valid? If the token lives forever, the risk of a security breach is increasing as time goes by, and if the token has a time to live through liveness data there has to be an evaluation on how long time it should be valid. Too short gives more overhead as the user might have to re-authenticate often and by this adding traffic and overhead. Other, “classic” challenges of CIS security also remain unsolved, like PKI in DIL environments.

3.3 Service discovery

Before a potential consumer of a service can use the service, it needs to be able to find the services that are available to it, and also discover how to use those services. In Web Services, this translates into the consumer needing to find the machine-readable service description, which describes the interface of the service, and also contains the endpoint address of the service. The process of finding this description is called service discovery. Service discovery can be performed either in design-time, run-time or both. We have focused on run-time discovery, which targets finding available services and consuming them in run-time.

3.3.1 Which standards are used?

There are three SOAP web services discovery standards, all by OASIS:

1. Universal Description, Discovery and Integration (UDDI)

2. electronic business using XML (ebXML), and

3. WS-Dynamic Discovery (WS-Discovery).

Of these, UDDI is mentioned in the SOA baseline and current FMN instructions. Both UDDI and ebXML are registries, suitable for use in stable environment. Of the three, only WS-Discovery targets run-time discovery in dynamic networks. Hence, we have focused on that standard. WS-Discovery offers a multicast-based approach to discovery. The protocol has both a proactive and a reactive mode (the latter is necessary to give an up-to-date view of services in a dynamic environment). The reactive mode allows you to actively probe the network for services and use the result which mirrors the current network state.

3.3.2 What are the main challenges for this service in the tactical domain?

Using a registry is not a good option, because it constitutes a single point of failure. Also, registries rely on services being registered and explicitly deregistered, which is not always feasible in a dynamic environment. Hence, stale data can occur in a registry under such conditions. Broadcast/multicast-based solutions like WS-Discovery overcomes these challenges but introduce new ones: A decentralized protocol consumes more network resources than a centralized registry. It is necessary to limit this overhead for WS-Discovery to be usable (to keep the discovery overhead low in order to maximize the amount of useful payload traffic).

3.3.3 Which optimizations are possible?

Many approaches are possible to optimize service discovery for a given network. Examples here include the usual approaches like enabling compression and using filtering to reduce overhead. Further, it is possible to replace the mechanism itself to a protocol better suited to a certain network's characteristics. For example, using UDDI is fine in an enterprise, but it is ill suited for use in a tactical network. For WS-Discovery, the protocol offers both so-called generic and specific probing of the network. By using specific probes one can search for only the services the client actually needs to know about (limit by Scope and PortType) so that only information that is useful for the client will traverse the network. As different protocols solve different needs we will need to bridge protocols somehow. We have considered different approaches to this, like adaptive protocols, using an abstraction layer, and introducing service discovery gateways.

3.3.4 Contributions in the field of service discovery

In the previous infrastructure project, 1176, we performed several experiments on service discovery. Our findings from that work, and the recommendation to use service discovery gateways remain valid also at the conclusion of 1277. We have focused mainly on WS-Discovery, and experimented with ways to extend the reach of WS-Discovery using peer-to-peer networking [23].

3.3.5 Recommendations for service discovery services

Use service discovery gateways to translate between different protocols to bridge different ownership domains. This approach limits the impact on deployments by keeping the need for mutual agreement to the interoperability points in a federated system. Different networks have different characteristics and need discovery solutions that take the limitations into account. For example, using WS-Discovery instead of UDDI in dynamic networks, such as mobile ad-hoc networks, allows us to discover services without the problems of a registry (stale data in the registry and/or unavailability of the registry itself as it constitutes a single point of failure).

3.3.6 What is the way forward?

We have focused only on discovering SOAP services. As times change, we see an increased use of other technologies and deployment strategies that need addressing. So, for future work we think that discovery in hybrid environments should be pursued in further experimentation. In this sense, we mean "hybrid" in the broadest sense of the word, i.e., encompassing different service technologies (notably both REST and SOAP), different networks (narrowband and broadband tactical networks, etc) and different deployment strategies (your service hosted stand-alone, in a tactical cloud, etc).

3.4 Collaboration services

Collaboration services (known in the C3 Taxonomy as Unified Collaboration and Communication Services) is a group of services that support human-to-human communications, such as e-mail, audio and video-based conferencing and instant messaging. Common for all of these services is that while they are indeed services, they are not realized using Web services technology.

In 1277, we primarily address the adaptation of traditional SOA technologies such as Web services, but we also consider some non-SOA services such as instant messaging and video teleconferencing (VTC). These services have been included, as supporting them is of great importance also in the tactical domain.

3.4.1 Text-based collaboration services

Text-based collaboration services, often called chat, allow users to exchange relatively brief text-based messages in near real-time. The messages can be delivered either between two participants (instant messaging), or between several participants (chat room).

3.4.1.1 Which standards are used?

One of the most prominent solutions in recent years is the XMPP protocol, which is implemented in several instant messaging products, both servers and clients. This protocol has also been chosen for chat by NATO, as it is mentioned in the SOA baseline as one of the protocols to use when implementing the collaboration core services. NATO's JChat client implements XMPP, and has been used with success in many missions. XMPP also supports presence, which is another collaboration service that we have not considered in this experimentation.

3.4.1.2 What are the main challenges for this service in the tactical domain?

XMPP is server-based, making it ill-suited for use in disadvantaged grids where a central server constitutes a single point of failure. Also, there is potential overhead of the presence mechanism, and overhead from the fact that the messages are XML.

3.4.1.3 Which optimizations are possible?

Multicast is an efficient means of distributing one message to many recipients. This can be leveraged in order to decentralize a chat application and do away with the central server. By using gateways and proxies, such a chat solution can be compatible with XMPP clients. We have identified three approaches that are commonly used when attempting to realize chat in tactical networks. Figure 3.2 illustrates these three approaches, from left to right:

1. Attempting to use XMPP directly, but with certain optimizations,

2. Using a proprietary solution in the dynamic environment, but using gateways to achieve interoperability with COTS XMPP clients and servers, and

3. Proprietary client and optimizations, but using a gateway for interoperability with an XMPP server in the backbone network.

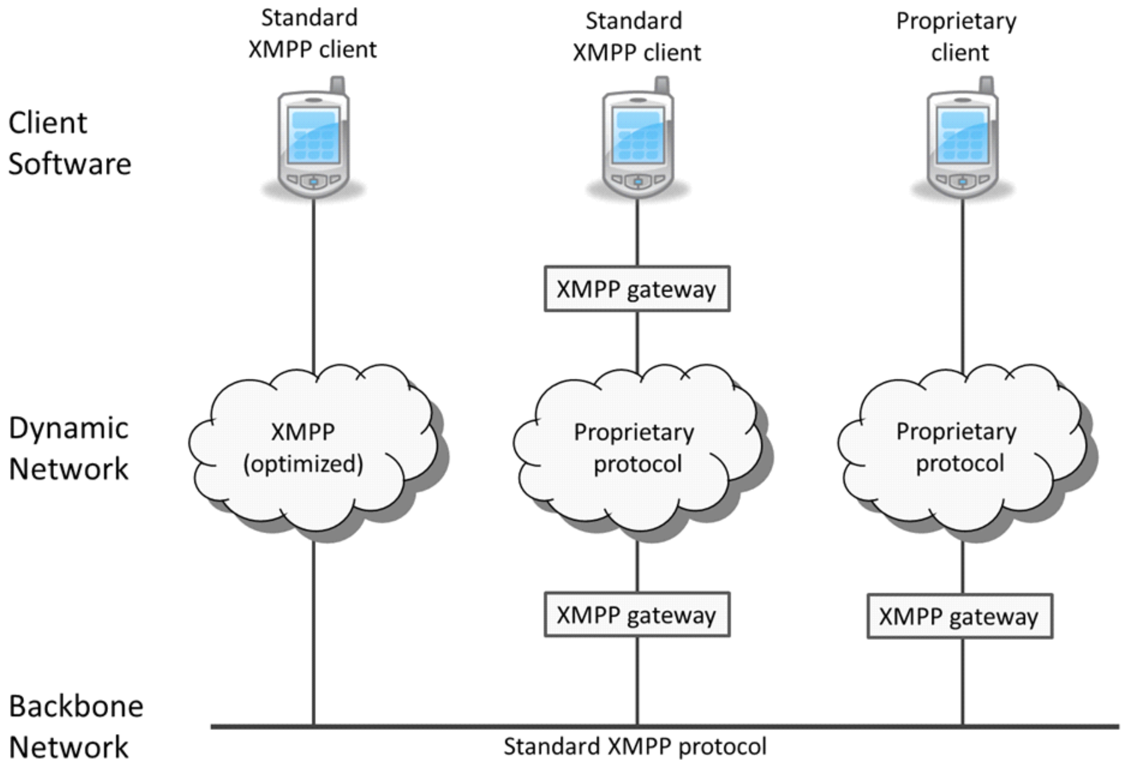


Figure 3.2 Approaches to implementing chat solutions

3.4.1.4 Contributions in the field of text-based collaboration services

In context of IST-118 we have made a prototype solution that we call P_MUL Chat. The motivation for creating this chat solution was to be able to leverage the key properties of ACP142 [24] for instant messaging in disadvantaged grids:

- Reliable multicast messaging
- Designed for bandwidth-constrained networks
- Delayed acknowledgement for EMCON (emissions control – radio silence) environments

Both our ACP142 Java implementation and the P_MUL Chat were released as open source and provided to the NATO STO/IST-ET-070 exploratory team for tactical chat for evaluation. For more information on our work on chat, see [25].

3.4.1.5 Recommendations for text-based collaboration services

The outcome of the NATO STO/IST-ET-070 evaluation was that there is no particular need to investigate tactical chat further. Proprietary enhancements that function well in the tactical domain now exist, and can be used together with corresponding proprietary gateways translating to the XMPP protocol. In this way, interoperability with NATO can also be achieved. We support the conclusions of the STO/IST-ET-070 team.

3.4.1.6 What is the way forward?

Use proprietary optimizations according to recommendation from the exploratory team on tactical chat, and interoperability gateways with XMPP.

3.4.2 Video-based collaboration services

Video based collaboration services may provide two-way video communication between two or more participants, so-called VTC. VTC normally also includes audio communication. VTC services are similar to audio conferencing services in many respects: Users expect real-time behavior, the service must provide an application allowing users to connect to a video conference, and all or only some participants could be allowed to speak and send video. Another use case for video services is one-way streaming, which can also be used for other services, such as getting information from video-based sensors. Full Motion Video (FMV), either for surveillance and intelligence gathering purposes or to provide immediate situational awareness, is becoming an increasingly important part of NATO's collaboration services selection. This latter case has been the focus of extensive experimentation at UWS, with FFI as a collaboration partner.

3.4.2.1 Which standards are used?

STANAG 4609 specifies that all motion imagery in the visible light and infrared spectrums must be contained in MPEG-2 transport streams and, if compression is used, should be employed in one of three commercial formats. Of these three the most commonly used is the H.264 advanced video coding standard first introduced in 2003. This standard is also in the NATO Interoperability Standards and Profiles (NISP). For civilian applications, the more recent H.265 standard is becoming increasingly abundant.

3.4.2.2 What are the main challenges for this service in the tactical domain?

The bandwidth-intensive, delay and loss intolerant nature of high resolution FMV transmission means that there are still challenges in transmitting over DIL networks such as those often found in tactical edge radio networks.

3.4.2.3 Contributions in the field of video-based collaboration services

Through our collaboration with UWS we have proposed a novel H.265-based video service for use as part of a SOA framework for services in DIL tactical networks. The service aims to provide a robust unidirectional video service for FMV for tasks such as video surveillance or provision of real-time situational awareness. The service has been designed to operate effectively in disadvantaged tactical networks by providing error protection and selective dropping mechanism that ensure that delivered video content can be both decoded and interpreted. Results of an empirical investigation show that video quality is maintained despite bandwidth fluctuations and packet loss. This work is described further in [26].

3.4.2.4 Recommendations for video-based collaboration services

For high-bandwidth networks and interoperability with current systems, we recommend using H.264 Scalable Video Coding (SVC). For the future, we recommend that NATO considers H.265 High Efficiency Video Coding (HEVC) for certain applications – it can achieve less network load by trading it for more intensive processing, which in many cases can make it preferable for use in resource-constrained networks where the throughput is the main limiting factor.

3.4.2.5 What is the way forward?

Suggested future work in this area is to concentrate on developing a fully functional Web service for video surveillance over DIL tactical networks that can be used for further experiments and evaluation.

4 Trends

In this chapter, we present what we think are the most important trends to focus on in the coming years, with respect to technologies related to service-oriented architectures.

4.1 Cloud computing

Cloud computing is all the rage in the civilian sector, since it empowers the customers to pay as they go to get exactly the data storage, processing power and software they need to cope with fluctuations in popularity and user mass. There are four main deployment models for cloud:

- Public, i.e., available for all, major vendors here are Amazon, Google and Microsoft,
- Private, e.g., self-hosted,

- Community, i.e., available to a community, for example the Joint Force Training Centre (JFTC) offers a cloud to NATO nations, and
- Hybrid, i.e., a cloud consisting of bridging two or more of the previously mentioned deployment models - an example would be using a public cloud for non-sensitive data and a private cloud for sensitive data.

A cloud can be offered in accordance with one of three service models: IaaS (Infrastructure as a Service), PaaS (Platform as a Service), or SaaS (Software as a Service). Regardless of which model one employs, there is a need for an underlying virtualization infrastructure. It is clear that the Norwegian Armed Forces should consider tapping into the power of the cloud, for ease of management and rapid deployment. In NATO, there are currently proposals for exploratory teams related to tactical cloud computing, though none of the proposals have been actually started at this point. There are, however, initiatives looking at tapping into the power of the cloud, for example MSG-136 ‘Modeling and Simulation as a Service (MSaaS)’, which is investigating using cloud computing for modeling and simulation purposes. From a national perspective it would make sense to investigate the cloud both for strategic, deployed and tactical use.

4.2 REST web services

With the emergence of the cloud, REST web services have gained momentum. The so-called micro services often leveraged in cloud architecture are REST-based, and we also see an increase in businesses choosing REST over SOAP when building their own decentralized systems, whether cloud-based or not. NATO, while thus far mostly invested in SOAP due to the rigid standardization and thereby (more or less) guaranteed interoperability by leveraging that technology, has recently started looking into REST as well. This is due to driving forces in the nations, which themselves start using REST, and also the TIDE community, which has opened up for REST experimentation. REST is considered easier to get started with than SOAP, and so it makes sense to investigate this track further also for the Norwegian Armed Forces. Using technology that is easy to work with and maintain will, in the long term, pay off through lower maintenance costs due to decreased complexity.

4.3 Internet of Things and smart devices

The Internet of Things (IoT) is a buzzword these days, covering aspects which previously were referred to as pervasive computing or ubiquitous computing. The main idea is that small, cheap consumer devices should be connected to the internet, share data and give users benefits though big data analytics and innovative ideas. Applications in the civilian sector include automotive, health care, surveillance, smart homes, and other such useful approaches. NATO is currently investigating possible military applications of IoT through the research task group IST-147 on military IoT. It is evident so far that the IoT approach can possibly be useful in a number of scenarios, such as perimeter surveillance and medevac to mention a few. IST-147 started in

2016, with a duration of three years. 1277 has been following developments in this group, and has recently joined as a member to further pursue this line of research.

An enabler for the IoT boom has been the abundance of smart devices like phones and tablets. These form a cheap yet powerful platform for processing and communicating, and applications on smart devices (so-called ‘apps’) give you a control panel to interact with your IoT devices. Many efforts, both national (see e.g., [27]) and international (see e.g., [28]), look into leveraging smart devices for military purposes. So, it makes sense to maintain a focus also in this area, not only with respect to apps, but naturally also the other aspects of such devices such as machine-to-machine communication issues.

4.4 FMN development

With FMN emerging and future spirals being planned, it is clear that though FMN currently addresses communication between strategic and deployed elements, future spirals will address communication in the tactical domain. It is here 1277 has been focusing much of its efforts, to be at the frontier of FMN-related machine-to-machine communications research. IST-118 work provided input to TIDE, which again will provide input to the FMN process. The successor to IST-118, IST-150 has recently started and will continue this line of work. 1277 was heavily involved in IST-118, and the successor to 1277 will continue its work in the context of IST-150 and TIDE. The culmination of the annual TIDE experimentation is full-blown testing at CWIX, so it is important to also be present at both venues. TIDE as the development and testing of specifications and CWIX as the validation of said specifications.

4.5 Publish/subscribe protocols

Currently, NATO is focused on WS-Notification and is developing its own Web Services Messaging Protocol (WSMP) built on top. The idea is to gain interoperable yet format independent (though limited to XML-based formats) message exchange. Interoperability is key for NATO operations, so the approach does make sense. That being said, WS-Notification is all but dead for civilian use, where standards like AMQP or MQTT are leveraged instead. So, even though IST-118 has shown it to be possible to employ WS-Notification (and then, in theory, also WSMP) in tactical networks, doing so requires several proprietary enhancements (see Appendix A). Hence, since there is a lack of available products, there will be a large cost associated with developing and maintaining own software on a national level to roll this protocol out everywhere. So, it is probably more cost efficient to limit WS-Notification and WSMP support to points of presence and interoperability points towards NATO, and look for other, preferably off-the-shelf solutions that can be employed elsewhere nationally. Then, one could rather bridge the internal solution with WS-Notification towards NATO. This has been shown to be feasible by [29], and warrants further experimentation with alternative protocols for national use, while at the same time pursuing the most recent developments of WSMP in TIDE and at CWIX for interoperability concerns.

4.6 Cross-layer optimization

Cross-layer adaptations have, through IST-118 work [30], been shown by Germany to be beneficial on the middleware-level when one can take network and link-layer information into account to provision middleware resources. FFI has so far performed some theoretical work on cross-layer optimizations for middleware (see, e.g., [31]), but no large scale experiments have been undertaken due to lack of funding. The area of research is active for the time being, and it would make sense to pursue this further in later projects.

5 Conclusion

This report has provided an overview of results and recommendations within the area of service-oriented architectures (SOA) from FFI project 1277 – *Information- and integration services in the information infrastructure*.

The main objective of the project has been to support the Norwegian Armed Forces in its work on developing network-based defence (NBD), by investigating technological solutions that can contribute to the development of a common information infrastructure (INI). SOA is a core technology area within the development of INI and NBD, and it has therefore been an important goal for the project to ensure that FFI maintains a high level of competence in this area. In addition, the project has contributed to further testing and improvement of core services, with the work done within NATO as a starting point.

5.1 Recommendations

As a result of the work on core services within project 1277, we have worked out a set of recommendations for such services. These have been presented in detail in this report, and we provide a short resume here in the conclusion:

- For messaging (both request/response and publish/subscribe), we recommend using filtering and compression to reduce overhead; and tuning transport protocols and application servers to better fit the underlying transport medium. Possible proprietary optimizations should be put in proxies between client and service.

- For CIS security services, we recommend focusing research efforts on SAML 2.0. In addition, we suggest pursuing message-level security in addition to transport or network layer security.

- For service discovery, we recommend using service discovery gateways to translate between different protocols to bridge different ownership domains.

- For text-based collaboration services, we recommend using gateways between XMPP and possible proprietary enhancements for the tactical domain.

- For video-based collaboration services, we recommend using H.264 SVC, but for the future, NATO should consider H.265 HEVC for certain applications

5.2 Trends

There are currently three trends that stand out as particularly important to be watching, and that potentially can have a significant impact on the Norwegian Armed Forces:

- Cloud technology, with its outstanding scalability and flexibility with respect to data storage, processing power and software, is playing an all the more important role in the civilian sector, and is very likely to do so also in the military sector.

- REST has been gaining momentum for a long time, and continues to do so, also in the military sector. Both the low complexity and the close relationship to cloud technology make this an important topic to watch.

- IoT can be useful in a large number of military scenarios, and the topic of military IoT should therefore be followed closely.

- FMN in the tactical domain is emerging and will be an important topic at future TIDE and CWIX events.

- WS-Notification, although being focused on by NATO, is not used in civilian sector, with a lack of products as a consequence.

References

[1] Bloebaum, Trude H., Johnsen, Frank T., “CWIX 2014 core enterprise services experimentation”, FFI-report 14/01510

[2] Trude H. Bloebaum, Frank T. Johnsen and Marianne R. Brannsten, “CWIX 2015 core service experimentation”, FFI-report 15/01334

[3] Trude H. Bloebaum, Frank T. Johnsen and Ketil Lund, “CWIX 2016 core service experimentation” FFI-report 16/02459

[4] Trude H. Bloebaum, Frank T. Johnsen, Peter-Paul Meiler (editors). “SOA recommendations for Disadvantaged Grids in the Tactical Domain.”, Final draft, submitted to NATO STO 2016-12-15 in partial fulfillment of the IST-118 obligations to STO (will become the final report once STO’s editors are finished and the report is officially released).

[5] Coalition Network for Secure Information Sharing II, Task 2 Final Report, Technical Report, 2017 [to appear]

[6] Skjegstad, M., Johnsen, Frank T., Bloebaum, Trude H., Maseng T., “Information-Centric Networking in the Tactical Domain”, IEEE Communications Magazine, Special Issue on military communications, October 2013

[7] NATO ACT, TIDE Transformational Baseline 4.0, available at https://tide.act.nato.int/tidepedia/index.php/TIDE_Transformational_Baseline_v4.0 (requires an account)

[8] Joanna Sliwa and Bartosz Jasiul, “Efficiency of dynamic content adaptation based on semantic description of web service call context”, in IEEE MILCOM 2012.

[9] Ketil Lund et al., “Robust Web services in heterogeneous military networks”, IEEE Communications Magazine, Special issue on military communications, October 2010.

[10] Joakim Johanson Lindquister, “Improving the performance of Web Services in Disconnected, Intermittent and Limited Environments”, Master’s Thesis, University of Oslo, Norway, Spring 2016, http://urn.nb.no/URN:NBN:no-54571

[11] Frank T. Johnsen, Trude H. Bloebaum, and Kristoffer R. Karud, “Recommendations for increased efficiency of Web services in the tactical domain”, IEEE ICMCIS 2015.

[12] Trude H. Bloebaum and Frank T. Johnsen, “Exploring SOAP and REST communication on the Android platform”, IEEE MILCOM 2015.

[13] Christoph Barz, Norman Jansen, Jose-Maria Alcaraz-Calero, Marco Manso, Garik Markarian, Ian Owens, Qi Wang, Peter-Paul Meiler, Trude H. Bloebaum, Frank T. Johnsen, Joanna Sliwa and Kevin Chan, “IST-118 SOA Recommendations for Disadvantaged Grids in the Tactical Domain - SOA Experiments on Wireless Broadband Mobile Networks in the Tactical Domain”, International Command and Control Research and Technology Symposium (ICCRTS), CCRP publication, USA, 2015.

[14] Marco Manso, Jose Maria Alcaraz Calero, Peter-Paul Meiler, Kevin S. Chan, Christoph Barz, Ian Owens, Joanna Sliwa, Norman Jansen, Qi Wang, Trude H. Bloebaum, Garik Markarian, and Frank T. Johnsen, "SOA and Wireless Mobile Networks in the Tactical Domain: Results from Experiments", IEEE MILCOM 2015.

[15] Trude H. Bloebaum and Frank T. Johnsen, "Evaluating publish/subscribe approaches for use in tactical broadband networks", IEEE MILCOM 2015.

[16] Trude H. Bloebaum, Frank T. Johnsen, Marianne R. Brannsten, Jose Alcaraz-Calero, Qi Wang, James Nightingale, "Recommendations for realizing SOAP publish/subscribe in tactical networks", IEEE International Conference on Military Communications and Information Systems (ICMCIS) 2016

[17] Anoop Singhal, Theodore Winograd and Karen Scarfone, "Guide to Secure Web Services", Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-95, August 2007.

[18] Nils Agne Nordbotten, "XML and Web Services Security Standards", IEEE Communications Surveys & Tutorials, Vol. 11, no. 3, Third quarter 2009.

[19] Marianne R. Brannsten, "Federated Single Sign on in Disconnected, Intermittent and Limited (DIL) Networks", IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, Scotland, May 2015.

[20] Joanna Sliwa et al., "Efficiency of the Single Sign On mechanism in a tactical network environment", Military Communications and Information Systems (ICMCIS), Cracow, Poland, May 2015.

[21] Allied Command Transformation (ACT), "CWIX 2015 Final Report Volume I", 18 August 2015

[22] Allied Command Transformation (ACT), "CWIX 2015 Final Report Volume II", 20 August 2015

[23] Trude H. Bloebaum and Frank T. Johnsen, "Enabling service discovery in a federation of systems: WS-Discovery case study", 19th ICCRTS, Alexandria, VA, USA, 2014.

[24] The Combined Communications-Electronics Board (CCEB), ACP142, P_MUL - A PROTOCOL FOR RELIABLE MULTICAST MESSAGING IN BANDWIDTH CONSTRAINED AND DELAYED ACKNOWLEDGEMENT (EMCON) ENVIRONMENTS, http://jcs.dtic.mil/j6/cceb/acps/acp142/ACP142.pdf

[25] F.T. Johnsen, T.H. Bloebaum, K.M. Kittilsen, L. Cetusic, H.K. Flaatten, K. Kjensmo, E. Lothe, O.J. Pettersen, T.M. Schmid and B. Tungesvik, "Collaboration services:

Enabling chat in disadvantaged grids”, 19th International Command and Control Research and Technology Symposium (ICCRTS), Alexandria, VA, USA, 2014.

[26] James Nightingale, Qi Wang, Jose M. Alcaraz Calero, Ian Owens, Frank T. Johnsen, Trude H. Bloebaum, Marco Manso, “Reliable Full Motion Video Services in Disadvantaged Tactical Radio Networks”, IEEE International Conference on Military Communications and Information Systems (ICMCIS), Brussels, Belgium, 2016

[27] Frank T. Johnsen, Trude H. Bloebaum, Marianne R. Brannsten, Ketil Lund, Federico Mancini og Bård K. Reitan. Bakgrunn for og innretning av støtten til EP1667 “SMART”, FFI-RAPPORT 2016/00848, Unntatt offentlighet iht. offentleglova § 21 (in Norwegian)

[28] J. B. Evans, B. J. Ewy, M. T. Swink, S. G. Pennington, D. J. Siquieros, and S. L. Earp. “TIGR: the tactical ground reporting system.” IEEE Communications Magazine, vol. 51, pp. 42-49, 2013.

[29] E. Bertelsen, G. Berthling-Hansen, C. Duvholt, E. Hov, E. Morch, A.H. Weisethaunet, OKSE 2.0 Protocol Mediator, Technical Report, FFI reference number 2016/01171, May 30, 2016

[30] Trude H. Bloebaum, Frank T. Johnsen, Peter-Paul Meiler (editors). “SOA recommendations for Disadvantaged Grids in the Tactical Domain.”, Final draft, submitted to NATO STO 2016-12-15 in partial fulfillment of the IST-118 obligations to STO (will become the final report once STO’s editors are finished and the report is officially released).

[31] Frank T. Johnsen, Joakim Flathagen, Mariann Hauge, Eli Gjørven, Terje M. Mjelde and Frode Lillevold, “Cross-layer design and optimizations”, FFI-rapport 2014/00985

[32] Tormod Haugland (NTNU), Inge E. Halsaunet (NTNU), Frank T. Johnsen, Trude H. Bloebaum, “WS-Nu – open source WS-Notification broker documentation”, FFI-rapport 2015/01250

[33] Julie H. Roa (HiOA), Erik H. Forsén (HiOA), Ole G. Hansen (HiOA), Erlend K. Rognes (HiOA), Frank T. Johnsen og Trude H. Bloebaum, COPS – eksperimentell programvare for situasjonsoversikt, FFI-notat 15/01306

[34] Frank T. Johnsen, Trude H. Bloebaum and Dag Ove Eggum, “Efficient SOAP messaging for Android”, ICMCIS, Krakow, Poland, May 2015

[35] Michael A. Krog, Frank T. Johnsen, Trude H. Bloebaum, Marianne R. Brannsten, Bård K. Reitan, “PISA: Platform Independent Sensor Application”, ICCRTS, USA, June 2015

[36] Andreas Thuen, “Federated Service Discovery – Interconnecting different Web Service Discovery Mechanisms”, Master Thesis, http://urn.nb.no/URN:NBN:no-49044, 2015

[37] Eirik Fosse, Anders Borud, Sigurd Grøneng, Fredrik Gusland, Simeon Georgiev, Michael McMillan, “Interoperable NATO Track Entry Log - A multi data format secure track store for The Norwegian Defence Research Establishment”, Technical Report, FFI reference number 2016/01186, May 30 2016

[38] Ole Berdal, Jørgne Bolli, Sigurd Haaheim, Erik Nyhus, Simon Slyngstad, Torbjørn Soltvedt, “Project Flagpole”, Technical Report, FFI reference number 2016/ 01185, May 30 2016

[39] Eirik Bertelsen, Gabriel Berthling-Hansen, Christian Duvholt, Einar Hov, Eivind Morch, Andreas H. Weisethaunet, “OKSE 2.0 Protocol Mediator”, Technical Report, FFI reference number 2016/ 01171, May 30 2016

[40] Espen Gudmundsen, Kari Helene Bekkelund, Magnus Brurås, “Kommunikasjonsapplikasjon for et felles situasjonsbilde på enkeltsoldatnivå”, Technical Report, FFI reference number 2016/ 01184, May 22 2016

A IST-118 Tactical SOA Demonstration

IST-118 hosted the Tactical SOA workshop during the International Conference on Military Communications and Information Systems (ICMCIS) in May 2016. The workshop was hosted as its own track integrated into the main conference. The workshop, including the keynote given by IST-118 chairman Peter-Paul Meiler, also served as an introduction to the publish/subscribe demonstration that was given after the workshop. In this demonstration, two of the IST-118 member nations, Germany and Norway, showed a number of the publish/subscribe optimizations that IST-118 have investigated.

The setup is shown in Figure A.1, where we had two headquarters, one German (left side) and one Norwegian (right side). Both headquarters had a WS-Notification broker set up, which was used to exchange NFFI tracks between the two nations. At this level, standard WS-BrokeredNotification was used to ensure interoperability. Each nation had its own (emulated) convoy that reported positions back to the national headquarters. In these inter-vehicle networks both nations leveraged their own, proprietary optimizations for WS-Notification.

Germany’s setup involved one laptop for the headquarters and for each of their four (emulated) vehicles one laptop and one tactical router. These tactical routers used WiFi-based radio modules to set up an ad hoc network for inter-vehicle communication. The nodes leveraged cross-layer adaptations where the publication interval of WS-Notification was adjusted to match the available communication resources. So, standard WS-Notification messages were exchanged, but the notification producers had been modified to take the cross-layer information into account before issuing (or choosing not to issue) a given notification. The information was then provided to the German headquarters, where it was also republished as input to Norway’s operational picture.

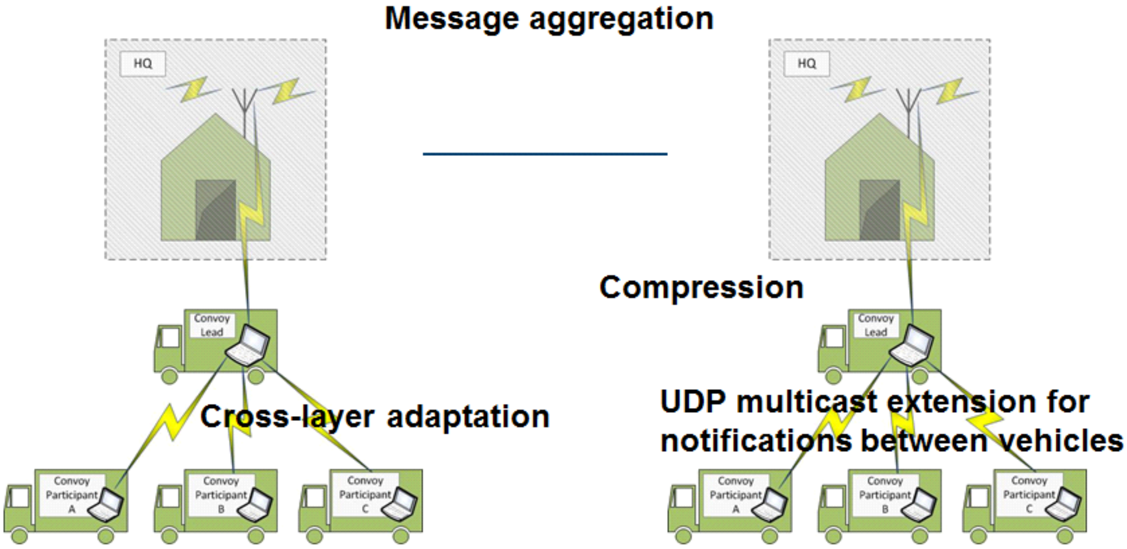


Figure A.1 Demonstration setup, showing where different optimizations were utilized

Norway’s setup consisted of just two laptops: one for the headquarters and one for emulating the convoy. The vehicles were represented with virtual machines (VMs), where each VM was equipped with software for blue force tracking. Here, standard WS-Notification messages were exchanged using some proprietary optimizations: First, compression was added to reduce the overhead of XML. Second, the broker (deployed in the lead vehicle) used UDP multicast to disseminate WS-Notification messages in the vehicular network rather than relying on the point-to-point TCP connections that are normally used. Third, the lead vehicle performed aggregation of messages and applied compression before sending the information across the narrow reach-back link to the Norwegian headquarters. There, the messages were uncompressed, and used to visualize the operational picture. The same (uncompressed) information was then re-published to Germany for visualization there, as input to the operational picture.

In the demo, we successfully showed the exchange of blue force tracking information based on WS-Notification in an efficient and interoperable manner between nations. In addition, we successfully demonstrated the functionality of the tactical level proprietary optimizations and how they could be connected to standards-compliant brokers to ensure interoperability between the nations.

B LINE

In November 2015 the Norwegian Defence Research Establishment (FFI) conducted an experiment using two autonomous Unmanned Aerial Vehicles for geo-location of navigation radars. This was an interdisciplinary experiment that included a number of different research communities, and which contributed to a number of different research areas. This appendix contains a paper describing the experiment, presented at the ICMCIS conference in Brusselse, May 2016.

The paper gives an overview of the experiment, with an emphasis on the information flow. The experiment has demonstrated how a continuous data flow can be established, from the sensors, via an operating center, and all the way to a joint headquarters. In addition, we describe how sensor data from different sources were integrated in order to identify tracks that needed further investigation. Finally, the paper provides some preliminary results from the experiment, both with respect to the radio communication between sensors and ground node, and to the actual geo-location process.

B.1 Introduction

The use of autonomous vehicles is increasing fast in many military areas. One such area is surveillance, and Norway with its long coast line has a particular need for effective maritime surveillance. Using Unmanned Aerial Systems (UAS) for such surveillance operations can save manpower, increase presence and reduce risk, and should therefore be investigated further.

ESM (Electronic Support Measures) is a technique for passive geo-location and identification of radio emitters, and can be an effective means of doing surveillance. LINE UAS (Light Navigation-radar ESM UAS) is a system designed for geo-location of maritime navigation radars and is small enough (3450g total weight and a volume of less than 2 liters) to be carried by a relatively small (less than 20kg) unmanned aerial vehicle (UAV). LINE has been developed at FFI, and is the successful result of an attempt to build a cheap, experimental navigation radar ESM that could function as a low cost supplement in maritime surveillance. This supplement is intended for “gap filling”, as well as for positioning and identity-verification.

The actual ESM concept and Cooperative ESM operations (CESMO) are outside the scope of this paper, and will therefore only be described in sufficient detail to understand the concept. Instead, the paper focuses on how we have built a continuous data flow from the flying sensors, and into the national defense information infrastructure. On its way from sensor to decision maker, the data traverses a number of different networks, from tactical UHF to high-speed fiber networks.

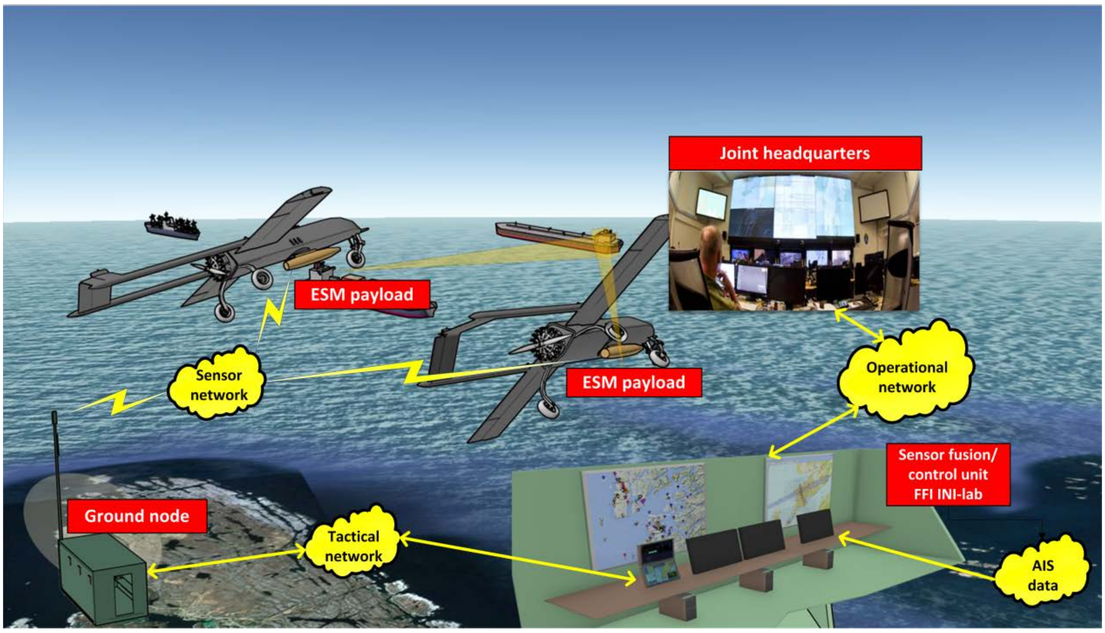


Figure B.1 Overview of the complete system

In addition, we describe how data from different sensors are integrated and used by the operator in order to identify ships that act suspiciously and therefore should be investigated further.

An integrated experiment was carried out in November 2015, with two UAVs operating out from Ørland main air base in Norway, a lab at FFI acting as the ESM operation center, and with network connection to the Norwegian Joint Headquarters (NJHQ), as illustrated in Figure B.1. This paper describes concepts and results from this experiment, with an emphasis on the communication aspects.

The remainder of this paper is structured as follows: Section B.2 provides some background on the experiment, i.e., maritime surveillance, ESM, and UAVs. In Section B.3 we describe the architecture and design of the experiment and the systems used, while Section B.4 presents the actual experiment and the results. Please note that since the paper is meant to give an overview of the experiment, only high-level results are presented. More detailed analyses of the results will be given in separate articles and reports. Finally, in Section B.5 we present related work, before concluding in Section B.7.

B.2 Background

Maritime Surveillance is the effort to gain an effective understanding of anything associated with the maritime domain that could impact security, safety, the economy, or the environment. The purpose of this is to provide political and operational decision-makers with the best basis to make correct and consistent decisions. In this section, we introduce two mechanisms for use in maritime surveillance, namely Automatic Identification System and Electronic Support Measures.

B.2.1 Automatic Identification System

An important mechanism in maritime surveillance is the use of Automatic Identification System (AIS) [1]. This is an automatic tracking system used on ships and by vessel traffic services (VTS) for identifying and locating vessels by electronically exchanging data with other nearby ships and AIS base stations.

The International Maritime Organization (IMO) made AIS compulsory for ships larger than 300 gross ton through the International Convention for the Safety of Life at Sea (SOLAS) in 2000, effectively from 2004.

However, AIS is not a fool-proof system, as the AIS transmitter can be turned off, or the information transmitted can be altered, for instance by transmitting a position that is different from the actual one. Thus, vessels that either turn off their AIS transponder or fake their position are of particular interest to the authorities, both because such actions are illegal, but also because the motivation for doing so may be based on criminal intentions.

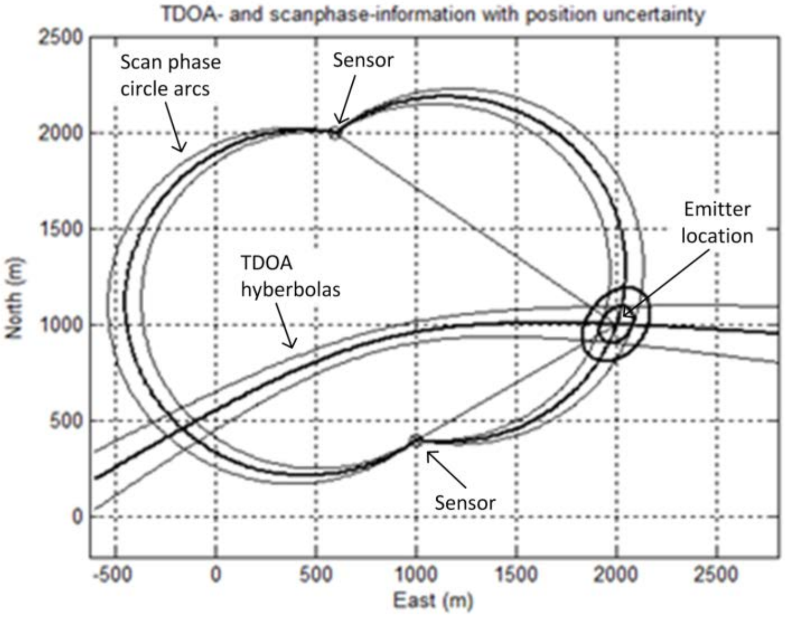


Figure B.2 Illustration of geo-location by TDOA and scan phase with uncertainty

ESM is a concept from the Electronic Warfare community, and involves using special radio receivers for detection of emissions from radars and communication systems. These sensors measure the frequencies and other characteristic parameters of a radar signal, as well as the direction or bearing to the emitter (the latter was not done in this experiment, as this requires quite large antennas). By tracking emitters over time based on bearings from one ESM sensor, it can take a long time to establish target location, and these locations may have limited accuracy.

It is therefore a wide scope for connecting sensors in a network in the ESM context. Two or more sensors can together locate the radar, but require coordination of their recorded information to do so, for example over a network. Geometries (i.e. placement of the sensors relative to the emitter) also play an important part in the geo-location process, and availability of several sensors on the same network can therefore aid the system operator in selecting the sensors likely to form the best geometries relative to the emitter in question.

With cooperating ESM sensors one can process simultaneous observations of an emitter from several ESM sensors, and thereby obtain locations both faster and with better accuracy than is possible with one sensor. It is also possible to use other and better methods that produce a more accurate emitter location. CESMO are mainly concerned with the detection and localization of radar emitters by cooperation between many sensor platforms

LINE EW-UAS is a system designed for geo-location of maritime navigation radars using two UAVs, each carrying their ESM-payload tuned to listen on the X-band (8-12 GHz). The data recorded in the sensors are used to create a near real time (i.e., in the order of 20-30 seconds) picture of visible radars in the area of flight, hence contributing to an increased situational understanding of the maritime domain. Being based on detecting radio waves, ESM and LINE also have the advantage of not being dependent on visible light. This means that surveillance also can be done in darkness or fog.

Two LINE-sensors can, by combining their observations of received radar pulses, obtain Time difference of Arrival (TDOA) and scan phase. A measured TDOA-value implies that the radar is located on a hyperbola with the sensors in the focal points. This is given by the following equation:

$$TDOA = \frac{1}{c}(d_1 - d_2) \qquad \text{(B.1)}$$

In Equation (B.1), c is the speed of light and d1 and d2 are the distances between sensor 1 and the emitter and sensor 2 and the emitter respectively.

Scan phase localization is based on measuring the radar rotation time and the radar main lobe (i.e., the beam of the radar) time difference of arrival at two sensors

A measured scan phase means there is a fixed angle from the radar towards the two sensors, which in turn implies that the radar is located on a circle-arc through the radar starting at the sensors. Figure B.2 illustrates the measurement principles and associated position uncertainty. Note that there are two sets of circle arcs, one on either side of the sensors. To determine which arc is the correct one, the rotation direction of the radar has to be known. Since there are uncertainties in these measurements, neighboring hyperbolas and circle-arcs also may contain the radar. Combining the most likely hyperbola with the most likely arcs determines the position of the radar. For more information on TDOA and scan phase, we refer to [2].

When used in conjunction with AIS data, this becomes a powerful tool for verifying AIS tracks, or ultimately identify those attempting to fake it. This leads to at least two clear advantages in that it adds an extra, redundant layer of surveillance, as well as making life harder for those vessels trying to pass by unnoticed by attempting to fake or turn off their AIS track altogether.

An important goal for the project has been to actively illustrate the advantages such a system can provide, by making use of standardized communication protocols and visualization software that already fits directly into the operational chain of command. NATO has recently ratified STANAG 4658 (CESMO) [3]. This is a standard describing networked exchange of ESM information for geo-location purposes. There are considerable efforts being made within NATO for test and development of CESMO, and this project has made use of the CESMO framework to communicate ESM data from the sensors to the ground node. It is believed that this is the first use case for CESMO in an unmanned platform, and also the first time scan phase messages are implemented in conjunction with the standard.

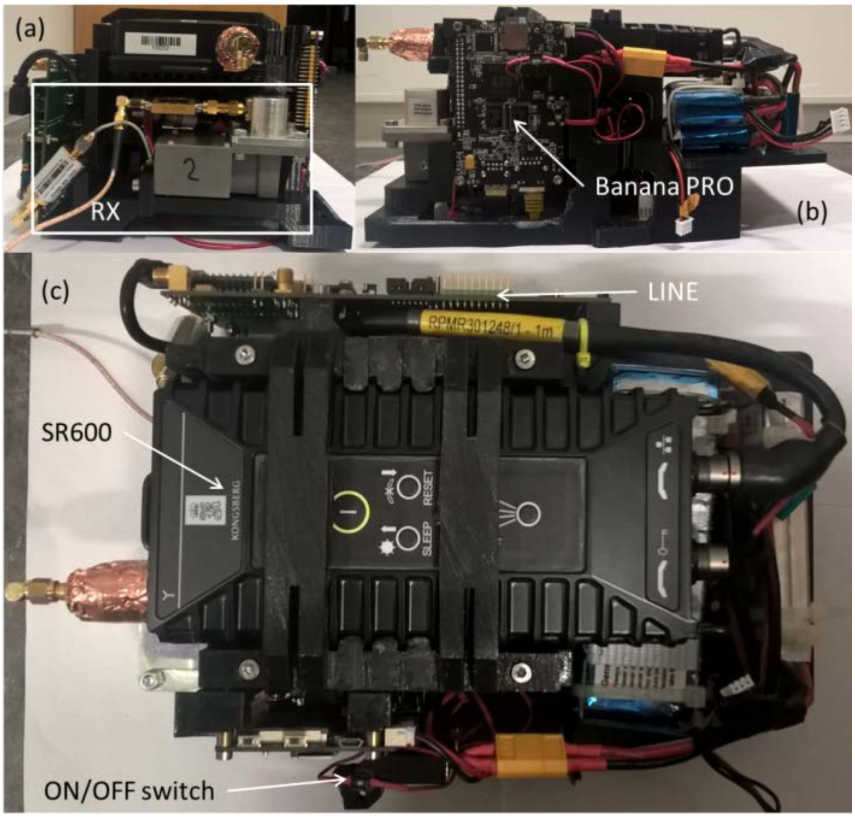


Figure B.3 Payload mounted in a 3D printed rack

B.3 Architecture

An overview of the complete system is given in Figure B-5. Data recorded in the payloads of the two UAVs is sent to the ground node that runs software for handling the message exchange as well as performing the geometry calculations. Processed data is then sent to the operation center at FFI where it is visualized in a map and the actual geo-location of emitters is performed. A verified emitter track is then coupled with live AIS data, leading to a number of track-lists containing information such as; vessels where AIS and radar locations match, vessels with AIS, but no emitter track, and emitter tracks with no AIS information at all.

B.3.1 UAV

The UAVs used in the experiment are two Penguin Bs from UAV Factory [5]. These are fixed-wing UAVs with a wing span of 3.3 meters, a weight of around 20 kg, and a maximum payload of 10 kg. During takeoff and landing, the UAVs were controlled manually, but in the operational area, they flew autonomously.

A significant challenge in this experiment was to fit all necessary equipment into the payload compartment of the UAV. This includes radio, ESM hardware, batteries and computing hardware. A rack was specially designed for the payload compartment of the Penguin B, and then 3D printed. This is shown in Figure B.3.

B.3.2 UAV Payload

The payload on board the UAVs consisted of three main parts, an ESM sensor, a power module and a communication module. These are described below.

ESM sensor

The ESM-sensor collects pulses from navigation radars, digitizes and parameterizes the pulses and then sorts and stores the data. It consists of four parts:

- Antenna: a 9.4 GHz dipole
- Receiver that amplifies and down-converts the incoming pulses
- Pulse processor that digitizes and parameterizes the incoming pulses

ARM processor (Banana Pro [8]) which reads data from the pulse processor, processes this data and communicates and stores the results

The sensor also includes a GPS module, used both for registering the position of the aircraft, and for time stamping the received radar pulses. Note that the flight control system of the aircraft has its own GPS module, separate from the one on the ESM sensor

Power module

To minimize the effect of the payloads on the electronics of the UAVs, the power module had to be completely separated from the UAV systems. The payload therefore needed its own power source. A power module was built using Lithium-Polymer (Li-Po) batteries and a power supply which provided four different voltage levels.

Communication module

The two UAVs communicate with a ground node using UHF radios from Kongsberg Defence Systems, SR600 [6]. This is a modern, software-based radio with an IP interface. The frequency range is 225-440 MHz and it has a bandwidth of 5 MHz. The data rates can be varied, and in this experiment, it was first set to 1024 kbps, and then to 128 kbps. The SR600 has a selectable RF output of 10 mW to 1 W, and for the experiment, the output was set to 1 W (the ground node was a larger version of the radio, and used an output of 5 W). The MAC (Medium Access Control) protocol is CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance), similar to the IEEE 802.11 MAC protocol, with three retransmissions in case of a failed unicast-transmission. Communication with the Banana Pro is done over Ethernet.

The participating radios form an ad hoc network with multi hop capability. This implies that traffic from one UAV may be routed via the other UAV on its way to the ground node. During the experiment, such traffic relaying was observed several times.

The original SR600 antenna is a monopole antenna mounted directly on the radio chassis with a length of 24 cm. The size of the antenna as well as measurements performed, showed that the antenna could not be separated from the radio chassis without affecting the input impedance to a degree that made it unusable. Thus, a new antenna had to be designed. This is shown in Figure B-4.

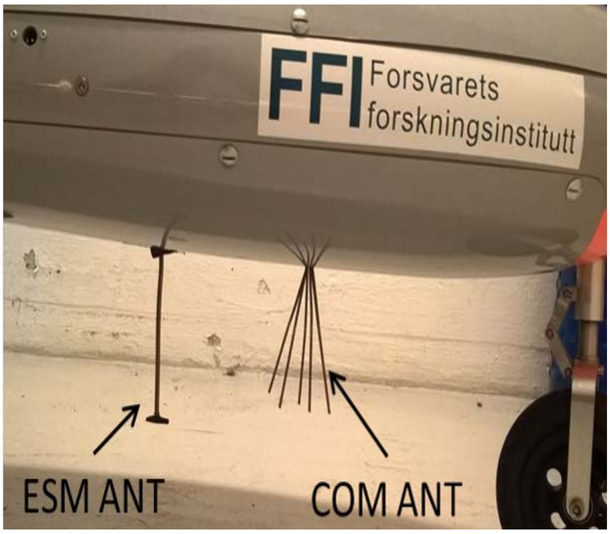


Figure B.4 ESM and communication antennas mounted on the UAV

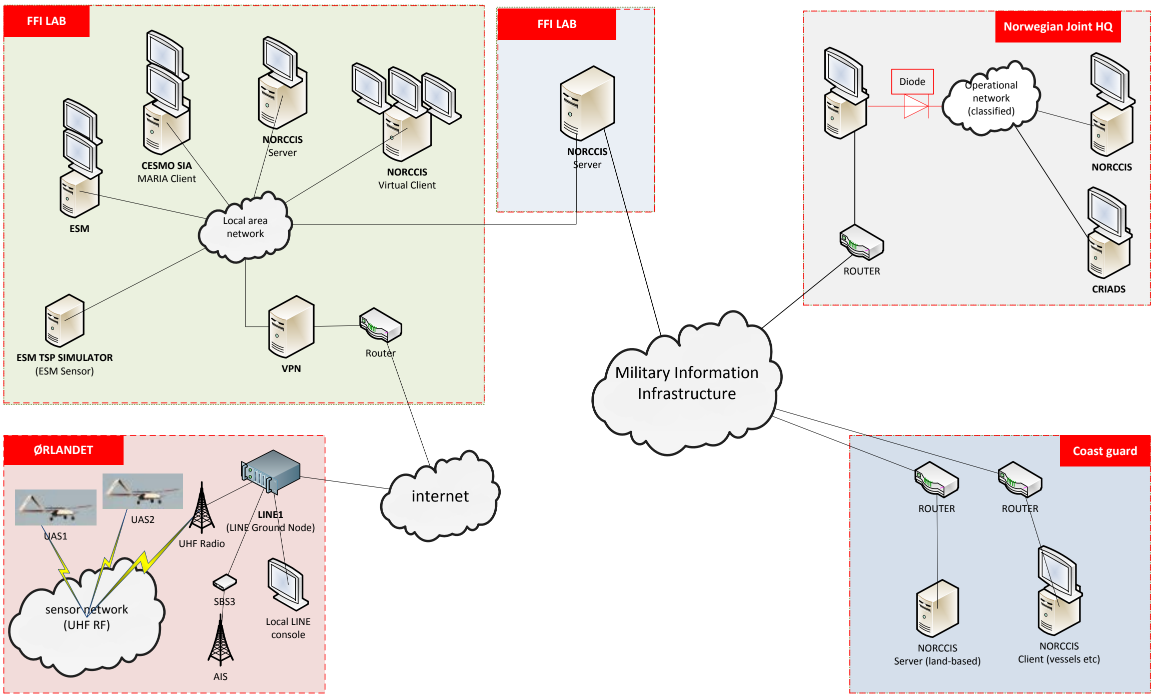


Figure B.5 An overview of the complete system

B.3.3 Communication and data integration

All flow of data to and from the payload is governed by the ground node. The payload system will record ESM data, but no data will be transferred unless specifically queried by the ground node software. This is done as an additional measure to avoid data collision if the two payloads should broadcast at the same time. All communication makes use of the UDP protocol, where there are no mechanisms for error checking or retransmission if a message is lost due to e.g. collisions. The UDP packets from the sensors were therefore modified in two ways, to support link performance monitoring:

1. They were assigned a sequential IP identity number, to detect packets outgoing from the radio that have been lost on the air.

2. They were fitted with an optional IP header (extending the existing IP header,) specifying a timestamp equal to the clock in the radio.

Since both payloads share the same radio channel, a communications scheme was developed to minimize unnecessary data loss and utilize as much as possible of the available bandwidth. Each payload is polled in turn, and assigned a fixed time interval in which it can transmit its data upon receiving a poll. A payload will transmit as many messages from its queue as the bandwidth will allow within a transmit window. With few exceptions, all messages received by a payload will trigger a transmit sequence.

The above scheme was designed to ensure that the system transfers a close-to-continuous stream of data from both payloads. Note that the CESMO standard does not demand a coordinating authority regarding communications, hence accepting a higher probability of package loss.

The data from the UAVs is sent to the ground node in the NATO CESMO format. This means that the data is interoperable with real, operational platforms, both in Norway and in NATO.

From the ground node, the data is sent to the operation center at the FFI lab using a 3G connection secured with Virtual Private Network (VPN). Once received and stored in the operation center, the processed data is visualized in a map and the actual geo-location of emitters is performed based on the TDOA- and scan phase geometries intersection points. The software visualizing the data also receives live AIS tracks from the Norwegian Coastal Administration. These tracks are received as a stream of tracks on the National Marine Electronics Association (NMEA) AIS format over TCP.

By correlating the verified emitter track with the live AIS tracks, the operator is able to produce three different track-lists:

- Vessels where AIS and radar locations match,
- Vessels with AIS track but no emitter track,
- Emitter tracks with no AIS information.

Vessels in the first category are OK, while vessels in the second category may need further investigation. It could be that the navigation radar is turned off, or that the AIS transponder is giving fake positions. In both cases these are illegal actions. For vessels in the last category it could be that the AIS transponder is turned off, which is also illegal.

In addition to these three lists, a fourth list containing the current position of the UAVs is automatically generated. The tracks from these four lists are stored into four different tables in a MySQL database. A service then reads these tables and converts each target into NATO Friendly Force Information format (NFFI – STANAG 5527) [7] with the appropriate symbology code. Each given interval (e.g. 10 sec) the SQL query result will be written to a network stream available to the connected client(s), in this case a local NORCCIS server.

NORCCIS is a Norwegian Command and Control system, widely used throughout the Norwegian Defense. Using software that is recognized by operational personnel was an important part of this experiment, in order to more effectively demonstrate the operational value of our concept.

The local NORCCIS server is set to import the four different TCP streams into its storage and visualization mechanism. Visualizing was done locally by a connected NORCCIS client. In addition, a connection to NJHQ was prepared, which would make it possible to export the tracks there, using NORCCIS internal format (over a TCP stream). This connection used the internal

Norwegian defense information infrastructure, and at the NJHQ side the data would be received by a NORCCIS server in an unclassified area. From this server the data would then be forwarded through a data diode into the classified network. This means that the personnel at the NJHQ would be able to view the same tracks as on the NORCCIS client at FFI.

As shown in Figure B.5, the infrastructure at the FFI lab consists of a mixture of virtual and physical machines, connected over virtual LANs (VLANs). This provides us with great flexibility when it comes to configuring the setup and data flow of the experiment.

B.4 Experiment and results

The actual experiment took place at Ørland air base, just outside Trondheim, in November 2015. The UAVs used in this experiment are defined as Remotely Piloted Aircraft Systems (RPAS), and the system must therefore be approved by the civil aviation authorities in Norway. Further, as the LINE experiments would require Beyond Line of Sight (BLOS) operation of the UAS, a special permission for this had to be issued by the authorities.

The UAVs took off from the runway and then headed into a circling course just off the shore, in order to do an initial check of all systems. Next, they headed further out and entered a circling course with center around 5 km from the runway. The circle was approximately 1.6 km i diameter. Over the next two hours the UAVs first kept this course before entering a more elliptic path. Figure B.6 shows the flight paths of the UAVs.

The preliminary results of the experiment show that, with respect to the geo-location process, the main limiting factor is the manual steps involved. Making a single instantaneous geo-location is time consuming, and tracking a vessel over time becomes tedious work. In addition, data sampled at different points in time introduces an error, and it is difficult to visualize the resulting uncertainty.

After the experiment, a geo-location algorithm based on TMA (Target Motion Analysis) was therefore developed. TMA works on the principle of estimating future position, course and speed based input from multiple sensors. The algorithm works by analyzing relative movement between the sensor(s) and the emitter. A constant input of measurements from a number of sensors is processed continuously. Estimations on the position of the emitters (and course/speed) are calculated periodically and presented as a track of the emitter with uncertainty ellipses. Initial estimations are likely to be quite inaccurate, but these will gradually improve, and within approximately 30 seconds, the estimate is quite accurate (typically with an error margin of less than 300 meters). The net effect is a process that tracks the emitter in near real-time removing any need for manual input.

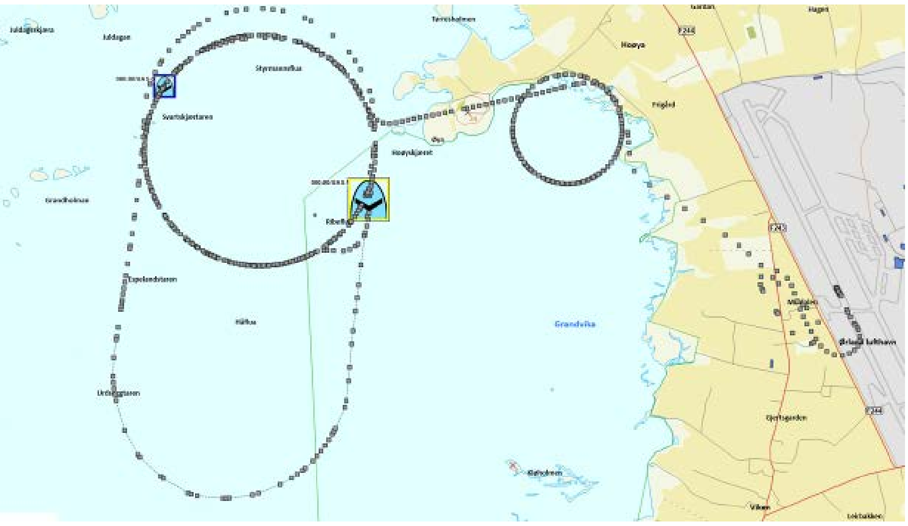


Figure B.6 Flight paths of the UAVs

A TMA algorithm was inserted into the SIA workstation and applied to the measured data from the operational test at Ørland air base. It proved the concept and was able to track moving radars without any operator involvement. The AIS and estimated radar positions were shown independently and then only the final verification against the AIS track was done manually by the operator.

With respect to the communication aspect, the experiment consisted of three distinct parts, chained together in order to demonstrate information flow from sensor to decision maker:

- A tactical mobile ad hoc network between the sensors on board the UAVs and the ground node

- A standard, secured civilian connection between the ground node and the operation center at the FFI lab

- Fixed national defense infrastructure between the operation center and NJHQ

In this paper, we focus on the first step, as no measurements were performed on the other two, other than verifying that the connection had sufficient capacity and was very stable. Also, the last communication step, from the NORCCIS server at FFI to NJHQ was not ready during the experiment. Instead, this connection was established a week later. It has been verified that the connection is operational and that data transfer between the NORCCIS instances is functional, but the actual transfer of tracks from our local NORCCIS installation has not been performed yet.

Due to uncertainty around the robustness of the UHF data link, two different data rates were used for the mobile ad hoc network between the UAVs and the ground node: For the first hour, the radios were set to a data rate of 1024 kbps and a queue length of 1000 packets, while for the last 15 minutes, a data rate of 128 kbps and a queue length of 8 packets was used (the queue length was automatically reduced when the data rate was lowered).

During the high-capacity phase of the experiment (1024 kbps), UAV1 and UAV2 sent 10734 and 20119 packets, with a packet loss of 2.2% and 1.0% respectively. In addition, UAV1 had a considerable number of packets forwarded via UAV2. The data is still being analyzed, and the reason for the big difference between the two UAVs is still not clear. During the low-capacity phase (128 kbps), UAV1 still had lower packet production and higher loss rate, but the differences were smaller.

For both UAVs and for both phases of the experiment, however, the packet loss was most pronounced each time the UAVs were flying towards the ground station. This could be explained by the antenna radiation pattern and a combination of the position of the mounted antenna and the vehicle itself. The nose wheel was positioned right in front of the antenna, breaking the Line-of-Sight (LOS) when the vehicle is headed right towards the ground station.

An important goal for the project has been to actively illustrate the advantages such a system can provide, by making use of standardized communication protocols and visualization software that already fits directly into the operational chain of command.

Using NORCCIS to visualize the different track types was part of this goal, and this turned out to work well. Admittedly, the NFFI format that we used to transfer the track information from the CESMO database to NORCCIS is, as the name implies, meant primarily for blue (friendly) force tracking. However, the data format has sufficient data fields and precision to handle emitter and AIS tracks. Thus, since this is a well-established standard, and we have much experience with it from earlier work, this was a natural choice.

Communication between the different systems, in particular within the operation center at FFI, and the planned communication between the operation center and NJHQ was based on point-to-point connections. According to the NATO Networked Enabled Capability Feasibility Study [12] (which has now been merged into the Federated Mission Networking [13]), instead of using point-to-point connections, information systems should rather be connected to a common information infrastructure. This is a necessary requirement for enabling seamless information exchange between users at all operational levels. However, this would require developing front ends (also known as “wrappers”) for the involved systems, and time did not permit this. The use of front ends is a common technique for service enabling of legacy systems, and we have implemented such front ends on several occasions (see e.g., [14] and [15]).

B.5 Related work

In [4] a similar experiment was performed, with two ESM-sensors, a coordination cell, and a headquarter acting as an information consumer. However, this experiment used traditional (large and expensive) ESM sensors mounted on full-size planes. Also, the experiment only used ESM sensors as information providers, there were no correlation with other information sources

(AIS). On the other hand, the principle of wrapping services with SOA interfaces as done in [4] could be reused in future versions of LINE, though updated with the standards specified by NATO [9].

The paper in [10] investigates the capacity improvements achieved when adding an airborne node to a ground ad hoc UHF-network. The results show that adding an elevated node considerably improves network capacity. These results are confirmed by our work, as the airborne SR600 radios retained connection with the ground node at distances far beyond what we have achieved using ground nodes only [11].

In [14], wireless sensor networks are integrated into an information infrastructure using Web services as front end to the sensor network. This work is complementary to ours, and the principle of wrapping systems with service interfaces is indeed a natural next step for us.

B.6 Future work

There are a number of areas that we will focus on in our further work. This includes improving the ESM sensors, the autonomy of the UAVs, emitter signature recognition etc.

For the scope of this paper, the plans for further activities include a possible extension is to take advantage of the sensor nodes not in use, and use them as communication relays for the “active” ones. This would reduce the need for radio power, resulting in an even more compact system.

In addition, as mentioned in Section B.4, we intend to better integrate the different systems into a service-oriented information infrastructure.

B.7 Conclusion

In this paper, we have presented a proof-of-concept experiment of sensor networking and integration. Sensor data from UAVs is transmitted to a ground node over military UHF radios, and then relayed over a 3G connection into an operation center.

The use case was passive geo-location of vessels by using ESM sensors carried by UAVs to locate the navigation radars of the vessels. The experiment has shown that this is possible, and that the accuracy is sufficiently high to be used for verifying reported AIS positions.

Being an interdisciplinary activity, this experiment contributed to a number of different research areas. The emphasis of this paper has been on the information flow in the experiment, and we demonstrated that it is feasible with a continuous data flow from the sensors, via an operating center, and all the way to the joint headquarters. In addition, we showed how sensor data from different sources were integrated in order to identify tracks that needed further investigation.

B.8 Acknowledgement

This experiment was carried jointly by eight different research communities within FFI. We would like to thank Tore Smestad, Berit Jahnsen, Eivind Bergh Nilssen, Jonas Moen, Øistein T. Hoelsæter, Jan Rune Nilssen, Fredrik Gulbrandsen, Jostein Sander, and Øivind Kure for their contributions to both the experiment and this paper.

B.9 References

[1] ITU Recommendation M.1371-5 (02/2014), Technical characteristics for an automatic identification system using time-division multiple access in the VHF maritime mobile band

[2] G. Høye, “Analyses of the geolocation accuracy that can be obtained from shipborne sensors by use of time difference of arrival (TDOA), scanphase, and angle of arrival (AOA) measurements”, FFI Report 00737, 2010

[3] NATO Standardization Agency, “Co-operative Electronic Support Measure Operations (CESMO), Rev. Edition 1, Version 1.1, March 2014

[4] T. Hafsøe, F. T. Johnsen, N. A. Nordbotten, and E. Skjervold, “Using Web Services and XML Security to Incrase Agility in an Operational Experiment Featuring Cooperative ESM Operations,” 14th International Command and Control Research and Technology Symposium (ICCRTS), Washington, DC, USA, June 2009.

[5] UAV Factory, http://www.uavfactory.com/product/46, accessed December 2015

[6] Kongsberg Defence Systems, “TacLAN UHF radio”, http://www.kongsberg.com/en/kds/products/defencecommunications/taclan/, accessed December 2015

[7] STANAG 5527 Original First Draft, NATO FRIENDLY FORCE INFORMATION (NFFI) STANDARD FOR INTEROPERABILITY OF FORCE TRACKING SYSTEMS (FTS), as of Dec 2007

[8] Lemaker, “Banana Pro”, http://www.lemaker.org/product-bananapro-index.html, accessed December 2015

[9] 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

[10] S.Ö. Tengstrand, S. Linder, K. Fors, and Ulf Sterner, “Capacity Benefits of Airborne Nodes in Ad Hoc Networks with Broadcast Traffic”, 2015 Intl. Conference on Military Communications and Information Systems (ICMCIS), Cracow, Poland, May 2015, pp. 1-6

[11] F.T. Johnsen, 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] P. Bartolomasi, et al., “NATO Networked Enabled Capability Feasibility study”, Version 2.0, NATO Unclassified, October 2005

[13] NATO, “Federated Mission Networking”, http://www.act.nato.int/fmn, accessed March 2016

[14] J. Flathagen, F. T. Johnsen, “Integrating Wireless Sensor Networks in the NATO Enabled Capability using Web services”, Military Communications Conference (MILCOM), Baltimore, MD, USA, Nov. 2011, pp 828-833

[15] F. T. Johnsen, T. H. Bloebaum, K. Lund, E. Skjervold, “Towards operations agility using service oriented integration of prototype and legacy systems”, 17th International Command & Control Research & Technology Symposium (ICCRTS), Fairfax, VA, USA, June 2012

C Publications

C.1 Journal articles

Skjegstad, M., Johnsen, Frank T., Bloebaum, Trude H., Maseng T., “Information-Centric Networking in the Tactical Domain”, IEEE Communications Magazine, Special Issue on military communications, October 2013

Marianne R. Brannsten, Frank T. Johnsen, Trude H. Bloebaum, Ketil Lund, “Towards Federated Mission Networking in the Tactical Domain”, IEEE Communications Magazine, Special edition on military communications, October 2015

C.2 Peer-reviewed conference articles

Morten Avlesen, Skage Spjelkavik, Bjørn Vik, Frank T. Johnsen, and Trude H. Bloebaum, “SPADE: A Test Framework for SOAP Analysis in Dynamic Environments”, 9th International Conference on Web Information Systems and Technologies (WEBIST 2013), Aachen, Germany, May 2013

Trude H. Bloebaum, Frank T. Johnsen, Gunnar Salberg, “Monitoring in Disadvantaged Grids”, 18th ICCRTS, Alexandria, VA, USA, June 2013

Frank T. Johnsen, Trude H. Bloebaum, Peter-Paul Meiler, Ian Owens, Cristoph Barz, Norman Jansen, “IST-118 – SOA recommendations for Disadvantaged Grids in the Tactical Domain”, 18th ICCRTS, Alexandria, VA, USA, June 2013

Frank T. Johnsen, Trude H. Bloebaum, Morten Avlesen, Skage Spjelkavik, Bjørn Vik, “Evaluation of Transport Protocols for Web Services”, Military Communications and Information Systems Conference (MCC) 2013, Saint-Malo, France, October 2013

A. Fongen and T.H. Bloebaum, “Trusted Service Discovery through Identity Management”, MILCOM 2013, San Diego, USA , November 2013

Trude H. Bloebaum, Frank T. Johnsen, “Enabling service discovery in a federation of systems: WS-Discovery case study”, 19th ICCRTS, Alexandria, VA, USA, June 2014

Frank T. Johnsen, Trude H. Bloebaum, K.M. Kittilsen and team, “Collaboration services: Enabling chat in disadvantaged grids”, 19th ICCRTS, Alexandria, VA, USA, June 2014

Frank T. Johnsen, Trude H. Bloebaum and Dag Ove Eggum, “Efficient SOAP messaging for Android”, ICMCIS, Krakow, Poland, May 2015

Frank T. Johnsen, Trude H. Bloebaum and Kristoffer R. Karud, “Recommendations for increased efficiency of Web services in the tactical domain”, ICMCIS, Krakow, Poland, May 2015

Christoph Barz, Norman Jansen, Jose-Maria Alcaraz-Calero, Marco Manso, Garik Markarian, Ian Owens, Qi Wang, Peter-Paul Meiler, Trude H. Bloebaum, Frank T. Johnsen, Joanna Sliwa and Kevin Chan, “IST-118 SOA Recommendations for Disadvantaged Grids in the Tactical Domain”, International Command and Control Research and Technology Symposium (ICCRTS), USA, June 2015

Michael A. Krog, Frank T. Johnsen, Trude H. Bloebaum, Marianne R. Brannsten, Bård K. Reitan, “PISA: Platform Independent Sensor Application”, ICCRTS, USA, June 2015

Trude H. Bloebaum and Frank T. Johnsen, “Exploring SOAP and REST communication on the Android platform”, MILCOM 2015, USA, October 2015

Trude H. Bloebaum and Frank T. Johnsen, “Evaluating publish/subscribe approaches for use in tactical broadband networks”, MILCOM 2015, USA, October 2015

Marco Manso, Jose Maria Alcaraz Calero, Peter-Paul Meiler, Kevin S. Chan, Christoph Barz, Ian Owens, Joanna Sliwa, Norman Jansen, Qi Wang, Trude H. Bloebaum, Garik Markarian, and Frank T. Johnsen, “SOA and Wireless Mobile Networks in the Tactical Domain: Results from Experiments”, MILCOM 2015, USA, October 2015

Marianne R. Brannsten, “Federated Single Sign On in Disconnected Intermittent and Limited (DIL) Networks”, 1st International Workshop on Service-Oriented Computing in Disconnected, Intermittent and Limited (DIL) Networks (SOC-DIL), Glasgow, UK, May 2015.

Trude H. Bloebaum, Frank T. Johnsen, Marianne R. Brannsten, José Alcarez-Calero, Qi Wang, James Nightingale, “Recommendations for realizing SOAP publish/subscribe in tactical networks”, ICMCIS, Brussels, Belgium, May 2016

James Nightingale, Qi Wang, José Alcarez-Calero, Ian Owens, Frank T. Johnsen, Trude H. Bloebaum, Marco Manso, “Reliable FMV Services in Disadvantaged Tactical Radio Networks”, ICMCIS, Brussels, Belgium, May 2016

Ketil Lund, Eirik Skjelbreid Grimstvedt, Morten Aronsen, Erlend Larsen, Robert MacDonald, “Sensor Networking and Integration - A proof-of-concept experiment”, ICMCIS, Brussels, Belgium, May 2016

C.3 FFI reports

Johnsen, Frank T., Bloebaum, Trude H., Lund Ketil, “On caching in military networks”, FFI-report 13/02926

Johnsen, Frank T., Bloebaum, Trude H., Lund, Ketil, “Enabling service discovery in a federation of systems: WS-Discovery case study”, FFI-report 14/01454

Bloebaum, Trude H., Johnsen, Frank T., “CWIX 2014 core enterprise services experimentation”, FFI-report 14/01510

Trude H. Bloebaum, Frank T. Johnsen and Marianne R. Brannsten, “CWIX 2015 core service experimentation”, FFI-report 15/01334

Trude H. Bloebaum, Frank T. Johnsen and Ketil Lund, “CWIX 2016 core service experimentation” FFI-report 16/02459

Trude H. Bloebaum, Frank T. Johnsen, Marianne R. Brannsten and Ketil Lund, “Final report for FFI project 1277 -Information- and integration services in the information infrastructure” FFI report 16/02484

C.4 FFI travel reports

Johnsen, Frank T., Bloebaum, Trude H., 18th ICCRTS, Alexandria, VA, USA, June 2013, Travel report 13/01894

Johnsen, Frank T., Bloebaum, Trude H., MCC 2013 and IST-118 meeting, Saint-Malo, France, October 2013, Travel report 13/02544

Johnsen, Frank T., Bloebaum, Trude H., TIDE Sprint autumn 2013, Travel report 13/02613

Johnsen, Frank T., Bloebaum, Trude H., IST-118 meeting, Hague, Netherlands, February 2014, Travel report 14/00386

Johnsen, Frank T., Bloebaum, Trude H., 19th ICCRTS, Alexandria, VA, USA, June 2014, Travel report 14/01348

Lund, Ketil, Workshop i CIS CaP, IIS-CaT, CES syndikat, 19. – 20. juni 2014, Brussel, Reiserapport 14/01357

Sletten, Geir, Rasmussen, Rolf, Information and Integration Services Capability Team - Data Management Syndicate meeting 4, 24 - 26 juli 2014, Reiserapport 14/01487

Frank T. Johnsen and Trude H. Bloebaum, IST-118 meeting, Paisley, Scotland, August 2014, Travel report 14/01602

Frank T. Johnsen, Trude H. Bloebaum and Marianne R. Brannsten, SSO validation testing workshop at NCIA, the Hague, Netherlands, November 2014, Travel report 14/02302

Frank T. Johnsen and Trude H. Bloebaum, IST-118 meetings in Prague, Paisley, and Lancaster in 2015, Travel report 15/01725

Frank T. Johnsen, Purple Nectar 2015, Travel report 16/00184

Marianne R. Brannsten, Frank T. Johnsen, Inntrykk fra Software 2016, Reiserapport 16/00649

Frank T. Johnsen, Marianne R. Brannsten, Bård K. Reitan, Inntrykk fra IoT-dagen 2016, Reiserapport 16/00650

Frank T. Johnsen and Trude H. Bloebaum, IST-118 public events and final meeting, Travel report 16/02168

Frank T. Johnsen and Trude H. Bloebaum, IST-150 NATO Core Services profiling for Hybrid Tactical Networks kick-off meeting, Travel report 16/02169

C.5 FFI Internal notes

Karud, Kristoffer R, Johnsen, Frank T., Bloebaum, Trude H., Web services performance over tactical communication networks, FFI-notat 14/01490

Eli Gjørven, Bjørn Jervell Hansen og Audun Stolpe, Typer av informasjonskilder for P8156 – tilgjengeliggjøring av sensorinformasjon, FFI-notat 14/01227

Julie H. Roa (HiOA), Erik H. Forsén (HiOA), Ole G. Hansen (HiOA), Erlend K. Rognes (HiOA), Frank T. Johnsen og Trude H. Bloebaum, COPS – eksperimentell programvare for situasjonsoversikt, FFI-notat 15/01306

Tormod Haugland (NTNU), Inge E. Halsaunet (NTNU), Frank T. Johnsen, and Trude H. Bloebaum, WS-Nu – open source WS-Notification broker documentation, FFI-notat 15/01250

Frank T. Johnsen and Trude H. Bloebaum, F. C. Berg (NTNU), K. A. B. Dalby (NTNU), H. Ø. Løvdal (NTNU), A. Skraastad (NTNU), F. B. Tørnvall (NTNU) and T. Walleraunet (NTNU), OKSE – WS-Notification and AMQP publish/subscribe interoperability broker, FFI-notat 15/01325

Marianne R. Brannsten, Trude H. Bloebaum and Frank T. Johnsen, Federated SSO with OpenAM 11.0.2, FFI-notat 15/01328

Julie Hill Roa, Didrik Emil Aubert, Erlend Nodeland Eriksen, Kristoffer Ramberg Karud, Frank T. Johnsen, Trude H. Bloebaum, Marianne R. Brannsten, og Bård K. Reitan, KingsEye – plattformuavhengig situasjonsoversikt, FFI-notat 15/01718

C.6 Other publications

Contribution to VITEN 2/2016 “Teknologien Forsvaret trenger” 16/01028

Contribution to VITEN 3/2016 “Teknologi i fellesoperasjoner” 16/02316

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

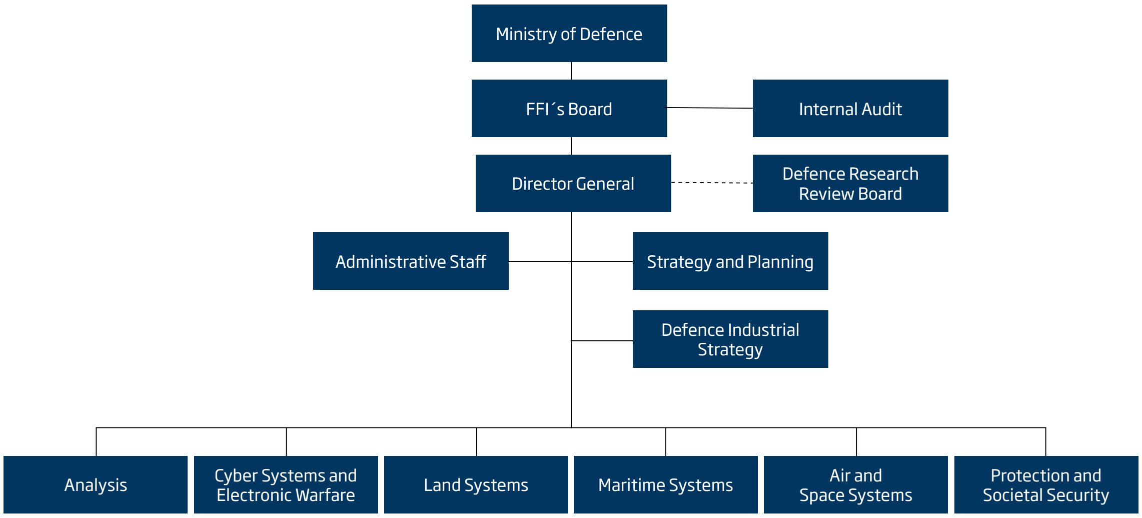
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation


Ministry of Defence

FFI´s Board

Internal Audit

Director General

Defence Research Review Board

Administrative Staff

Strategy and Planning

Defence Industrial Strategy

Analysis

Cyber Systems and Electronic Warfare

Land Systems

Maritime Systems

Air and Space Systems

Protection and Societal Security

Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment