

Chapter 4 – THE DEMONSTRATOR SCENARIO

The demonstration has gathered five nations featuring six platforms in Jørstadmoen Camp in Lillehammer (Norway) during CWID 2006. The names of the participating companies or organisations as well as the demonstration name and Identification number as they were referenced by CWID authorities are listed hereafter:

- EADS for France: EADS demonstrator of the French demonstration Secured Architecture for Information Sharing (SAIS) ID#49;
- FFI for Norway: SecSOA demonstration Secure SOA supporting NEC ID#69;
- NC3A for NATO: IEG Functional Services demonstration #ID104;
- Safelayer for Spain: Advanced Trusted Information Interoperability demonstration ID#106;
- Thales for France: SecSOA of the French demonstration SAIS ID#49; and
- MCI for Poland: Polish SOA WS system demonstration ID#103.

These demonstrators were each located in a separate room according the nationality of company or organisation in the CWID building and were connecting to the CTF-NRF network. This network used the infrastructure of the Combined Federated Battle Laboratories (CFBL) Network (CFBLNet). This network is classified Mission Secret and is also known as the purple Network. (See Figure 4.1)

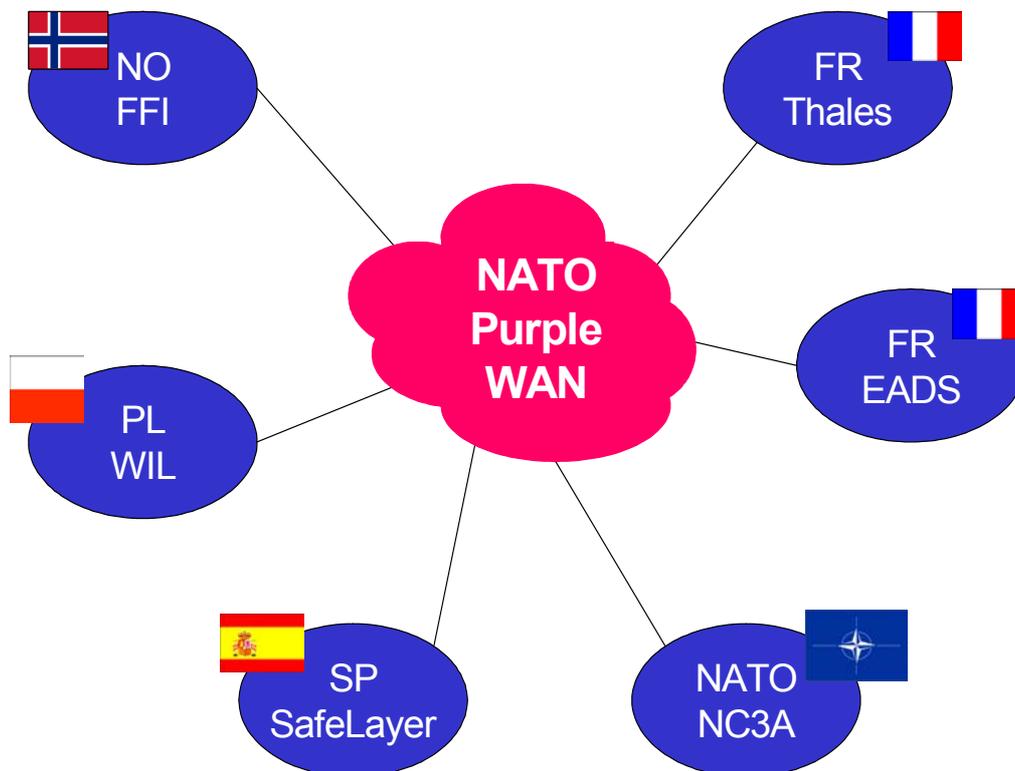


Figure 4.1: Demonstration Participants.

The purpose of the demonstration is to show how nations can share information and capabilities concerning two Communities Of Interest (COI):

THE DEMONSTRATOR SCENARIO

- The C2 COI: Nations expose Operational Picture services through which they provide pictures. Picture services are invoked on demand to retrieve pictures from other nations; and
- The ISR COI: Nations expose ISR services through which they can accept Sensor requests to be executed by their Sensor systems. Processed information from Sensor systems can be shared between platforms.

The area chosen for the demonstration scenario is shown in Figure 4.2. It is located in the south of UK near Southampton and called “Greenport”.

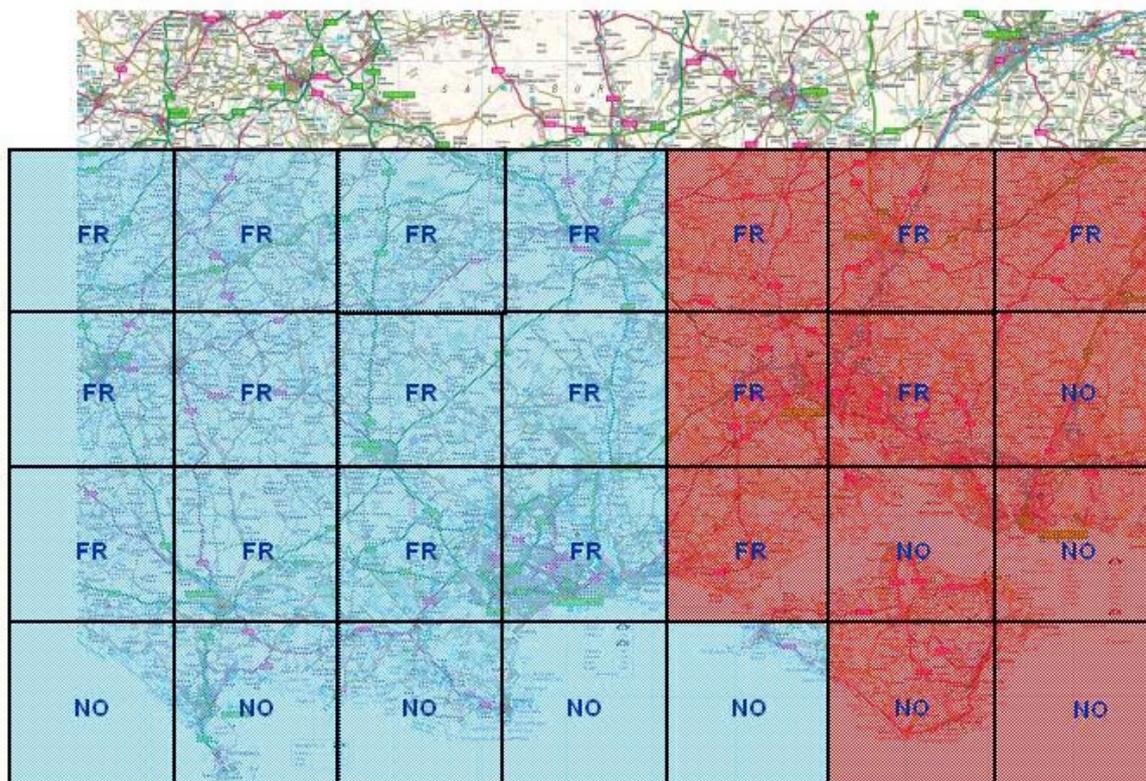


Figure 4.2: Demonstration Area.

The area is segmented in sub-areas that are each under the responsibility of a single nation. The responsible nation positions Blue Forces (in blue squares) and locates Opponent Forces (in red squares) in their sub-areas. Only the responsible Nation is authorised to put elements in its squares. This method has the advantage of not needing a “God’s eyes view” for the simulation. It also precludes the need to synchronize the scenario between nations. A limitation of this method is that it is not possible to perform a fusion of data from different nations, but this was not the focus of the demonstration. (See Figure 4.2)

The interoperability story (the scenario) between the nations could be summarised as follows:

- A Land force (FR) is conducting operations in a coastal area performing detection, location, and identification of opponent forces:
 - C2 COI: LCC provides a Land picture to other forces; and
 - ISR COI: The land ISR assets contribute to the detection of opponent forces. Support is requested from Naval ISR assets.

- A Naval force (NO) is performing littoral surveillance:
 - C2 COI: MCC provides Maritime picture to other forces; and
 - ISR COI: A Naval UAV system provides detection of Land forces. Its base station personnel receives sensor requests (service invocation), processes them and decides on changes in the UAV sensor tasking and/or flight plan.

Figure 4.3 is an example on the dialog between the French platform and the Norwegian platform.

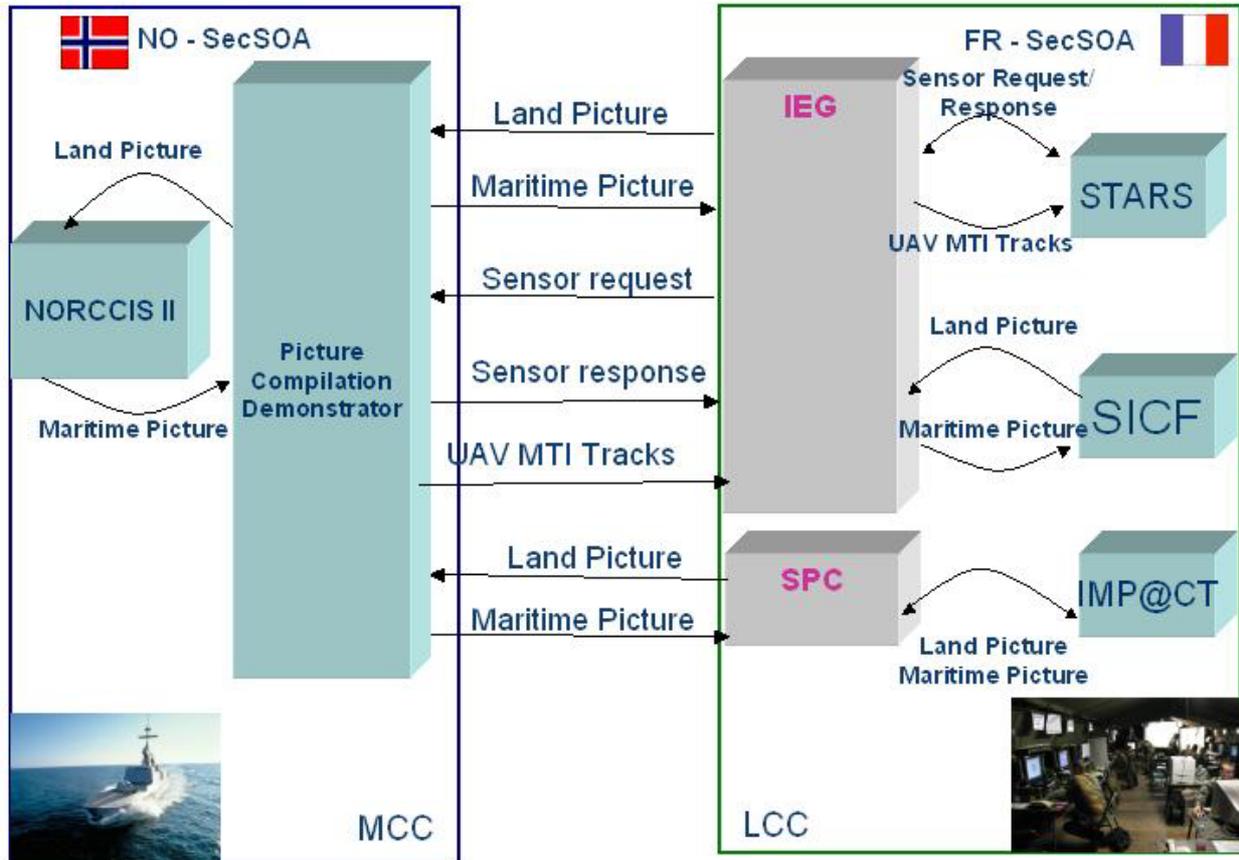


Figure 4.3: Exchange between Norway and France.

Table 4.1 below shows the participants’ intent as providers or consumers of services.

Table 4.1: Services Providers and Consumers

Services	France Thales	France EADS	Norway FFI	Poland MCI	Spain Safelayer	NATO NC3A
Land Picture	P	P	C	C	C	C
Maritime Picture	C	C	P	C	C	C
Sensor Request	C	C	P	C	C	C
UAV MTI Tracks	C	C	P	C	C	C

P: Provider C: Consumer

THE DEMONSTRATOR SCENARIO

Prior Interoperability, Platforms have to connect each other according a three-step process in order to get capabilities of browsing the Service Registry and then Service Invocation:

- 1) **Planning:** Exchange of necessary Security Certificates for directory replication and exchange of addresses of Platform Gateways through trusted files;
- 2) **Assembling:** Platforms replicate Directories of Security Certificates, hence all necessary Certificates, for enabling Service invocation through the Network, have been retrieved; and
- 3) **In operation:**
 - Platforms can publish services that they are willing to expose in the NATO Services Registry. This Registry is hosted on the Norwegian Platform; and
 - Platforms can browse the NATO Services Registry and subscribe to selected services. They will receive updates of information from the services to which they have subscribed.

In the end, the platforms could provide and consume the services as depicted in Table 4.1 Service Providers and Consumers above.

Summarily, the main demonstrated technical components are:

- **Dynamic Service Discovery:** The services are accessible on the Network, platforms do not need prerequisite knowledge of their location except the Services Registry location.
- **Publish-Subscribe Service:** This method allows a service consumer to subscribe to a delivery information service that has been published in the service registry. In the demonstration the Land and Maritime pictures were distributed following this method.
- **Request-response Service:** This method allows a platform to request a service and then to receive the response. The Sensor Request Service uses this method.
- **Services Registry:** A central Services Registry is used for sharing information about services and their publishers.
- **Security Certificates Directories Replication:** Platforms can be synchronised and Certificates can be exchanged.
- **Secured Exchanges:** All exchanges between platforms are performed in a secure way using signature, labeling and ciphering.
- **Security Certificates Revocation:** A certificate can be revoked “on the fly”.
- **Data Exchange Format:** All exchanged Messages are XML-based. The Land and Maritime pictures abide by a sub-set of the C2IEDM-XML Object-oriented Data Model. The UAV MTI Tracks are specified in a proprietary XML schema as there is no standard for sensor data.