A multilevel approach to interoperability in surveillance and reconnaissance

Barbara Essendorfer
Fraunhofer IOSB
Fraunhoferstr. 1
76131 Karlsruhe, Germany
0049-721-6091-0
Barbara.Essendorfer@iosb.fraunhofer.de

Christian Kerth
Fraunhofer IOSB
Fraunhoferstr. 1
76131 Karlsruhe, Germany
0049-721-6091-0
Christian.Kerth@iosb.fraunhofer.de

Gerd Schneider
Fraunhofer IOSB
Fraunhoferstr. 1
76131 Karlsruhe, Germany
0049-721-6091-0
Gerd.Schneider@iosb.fraunhofer.de

ABSTRACT
In the domain of civil and military surveillance and reconnaissance sensors and exploitation systems of different producers are used to achieve an overall picture of a critical situation. In today’s multinational cooperation’s on security and peace keeping it is essential to be able to share data that is produced by one national asset with other systems or even other nations. Therefore interoperability has to be established between those various systems, since each of them is currently dealing with different metadata/data formats and interfaces.

Within the multinational intelligence and surveillance project MAJIIC (Multi-Sensor Aerospace-Ground Joint ISR Interoperability Coalition) various standards have been developed enable sharing data. Those range from common data representation (e.g. imagery or radar data), metadata models and communication protocols to Coalition Shared Data (CSD) servers. The CSD servers provide a decentralized storage facility in which the standardized information is persisted and available to all participants through synchronization. Using standardized client interfaces relevant data can be found and retrieved from the storage facility.

By the approach of standardization, many of the interoperability issues have been overcome on a data representation level, resulting in the ability to share the data. However, to be able to understand the data and translate it into information more work has to be done. The integration of the various systems into a single coherent approach needs to be continued on the process, semantic interpretation and pragmatic level in order to achieve full interoperability. The usage and semantic of the metadata has to be defined as well as user roles and responsibilities. Rules have to be established to enable the correct interpretation and validation of data.

The paper describes the exercise based approach that is used in the project and reflects on the necessity of a multilevel approach to achieve interoperability.

Keywords
MAJIIC, CSD, standardization, metadata, information integration, materialization, virtualization

1. INTRODUCTION
In the past the paradigm within the domain of civil and military surveillance and reconnaissance has been that information has to be strictly restricted to organizational units or persons that have a “need to know”. A reason for this is to ensure information security. However information is always context sensitive and within complex scenarios and operational settings a mix of platforms, sensors and information sources is necessary to get a full situational awareness.

Therefore, systems from different vendors, owners, organizations and even nations have to be able to share data sufficiently, correctly and safely. Information has to be disseminated to the right place, in the right time with sufficient security markings to enable trust. Based on the fielding environment formed by these requirements an interoperable architecture has to be defined.

Interoperability is an achievement on many levels. A technical solution has to provide means to share data. It is required to have a legal base to be allowed to share information. Processes have to be described how data can be shared and semantic definitions have to clarify what a term means in a specific environment.

There is a strong need to improve interoperability on an organizational, system and architectural level between law enforcement authorities of NATO Member States or other organizations that are willing to share information [1].

This will for example
- increase the efficiency of detecting and preventing terrorists, and contraband from entering an area between official ports of entry (POEs)
- improve the reaction time from detection to interception
Based on the requirement to share information within distributed cooperation’s a technical solution is analyzed and proposed in this paper. However a solution needs to be supported by applying various rule sets on the participating systems to drive their capabilities further towards the network enabled joint operations. At the end of the paper, the most important of the various environments in which the approach is being deployed and future prospects are described.

2. ARCHITECTURAL APPROACHES FOR INFORMATION INTEGRATION

The basis for successful interoperability between various systems, acting as information sources and information consumers, is a well-defined integration architecture. This architecture has to be technology independent, thus various technologies can be applied for implementation. To achieve such an integration architecture two general approaches for information integration can be distinguished and applied: either materialized information integration (a priori integration) or virtualized information integration (a posteriori/on demand integration) [3][4][9]. A combination of both is possible and can result in a hybrid approach.

2.1 Materialized approach

The materialized approach is based upon a central, integrated information base. Information provided by various information sources has to be imported to this central information base and information consumers can retrieve the information via this single point of contact [3][9]. Figure 1 depicts this approach [9].

![Figure 1: Materialized information integration](image)

The import process can be realized either by a push or a pull mechanism. The push mechanism is based upon information sources which autonomously provide their information in a predefined exchange format to the central information base. This requires a previous agreement on the exchange format between the participating systems. The pull mechanism on the other hand is initiated by the central information base which collects the information from the sources by use of the sources’ services. In this case the collected information can be in a source-specific format which has to be transformed into an aligned format by the central information base.

The advantages of the materialized approach are as follows [2][5][9]:

- Comparatively easy realization
- High performance
  - Direct access to the central information base
  - Decoupling of slow external systems with limited availability
  - Specific optimization of the central information base
- Data cleansing by the central information base is possible

On the contrary the disadvantages are as follows [2][5][9]:

- Redundant storage of a potentially huge amount of data
- Difficult information update
  - Update initiated by the information sources has to be framed by organizational arrangements (e.g. frequency, exchange format)
  - Update initiated by the central information base is unaware of intermediate changes in the information source
- Originator loses control of the provided information

2.2 Virtualized approach

In contrast to the materialized approach, the virtualized approach is based upon mediator architecture composed of a facilitator for resource/service selection, mediators/service provider for an integrative information model, transformation of the query and merging of the query’s results, and wrappers for information extraction from the various information sources [4][7][12]. Key characteristic is that the information remains at the information source and the information consumer is linked to this source via a virtual integration layer (facilitator, mediator and wrapper). Figure 2 depicts this approach [9].

![Figure 2: Virtualized information integration](image)

Thus, an integrated view of the information does not exist as physical representation. Rather the integrated view will
be provided dynamically by the combination of facilitator, mediator and wrapper. An information consumer’s query will be passed through this virtual integration layer toward the information sources. The result of the query will be provided by these sources as a response.

The advantages of the virtualized approach are as follows [2][5][9]:

- Up-to-dateness
  - Mediated access to the actual information stored at the sources
- Resource consumption
  - Consumption can be distributed to the information sources
- Autonomy of the information source

The disadvantages are as follows [2][5][9]:

- Performance
  - Dependent on the information source and the network load
- Data cleansing
  - A central authority for data cleansing does not exist
- Autonomous modifications of interface and data model by the information sources resulting in an adjustment of the virtual integration layer

2.3 Comparison

The described architectural approaches show various assets and drawbacks which can be summarized as depicted in Table 1. This summary is based upon main characteristics related to both approaches [2][5][9].

<table>
<thead>
<tr>
<th>Table 1: Assets and drawbacks of the information integration strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Materialized</td>
</tr>
<tr>
<td>up-to-dateness</td>
</tr>
<tr>
<td>response time</td>
</tr>
<tr>
<td>complexity</td>
</tr>
<tr>
<td>request expressiveness</td>
</tr>
<tr>
<td>read/write</td>
</tr>
<tr>
<td>memory consumption</td>
</tr>
<tr>
<td>resource consumption</td>
</tr>
<tr>
<td>data cleansing</td>
</tr>
<tr>
<td>information quality</td>
</tr>
<tr>
<td>completeness</td>
</tr>
</tbody>
</table>

+ / positive, o / neutral, - / negative

In general, it is recommended to prefer a materialized information integration approach due to less complexity and independence of modifications of the information sources. Is this approach not sufficient to solve the business requirements the virtualized information integration approach should be considered [7][9].

In conclusion, both information integration approaches have to overcome the following integration aspects similarly [9]:

- System aspects
  - System aspects cover the technical area up to middleware considerations. These issues set the foundation for successful information exchange between various sources and consumers. E.g. aligned use of technologies associated with the ISO/OSI reference model [8] (data link layer: Ethernet, network layer: IP, transport layer: TCP, session layer and above: CORBA).
- Information aspects
  - Framed by the system aspects the information aspects include syntax and structure as well as the semantics of the exchanged information. E.g. syntax and structure can be handled by the use of XML whereas OWL could be the solution for the semantic enrichment of the exchanged information.

3. TECHNICAL SOLUTION

3.1 Description

Out of the various combinations which can be built from the techniques described above, the following has been chosen due to the underlying requirements in the projects’ planned fielding environment:

- Decentralized server topology
- Single point of contact for clients
- Materialized metadata storage
- Virtualized/Materialized hybrid for file storage

The main reason for a decentralized approach was the organizational aspects leading to that kind of infrastructure. Organizations can own the servers and control which information they want to share with the outside world/other servers while providing a wider information content to the local systems, invisible to the outside world.

In addition, decentralization has a positive effect on failure safety as backup systems can easily be added to the infrastructure and be spatially disjointed to minimize the risk of full infrastructure failure caused by local events which is required in the fielding environment to ensure that client systems can rely on a working backbone. Also, a decentralized approach allows the usage of proxy or guarded bridge systems which allow the transfer of information between networks with different security requirements, enabling transparent security application on each networks boundaries based on the network’s information transmission contracts.
server therefore acts as a mediator for all access to the file originally ingested on a remote network segment. The local small parts of the actual data available if the file was cases, the network infrastructure only allows to access localize all information over the wide area network. In most comparatively large, it is not possible to immediately
As the files which are attached to metadata are

“physical copy” is available on the local server. The results of a local copy are both faster access times to information as information transmission times across wide area networks is reduced and lower network traffic as metadata is only transferred once across the wide area network.

As the current client applications usually browse through large parts of the available metadata, most servers create a local copy of all the metadata as soon as it becomes available on remote servers by pulling it with a search. This provides clients with all the information available on the network at a minimal transmission cost on the network infrastructure.

As the files which are attached to metadata are comparatively large, it is not possible to immediately localize all information over the wide area network. In most cases, the network infrastructure only allows to access small parts of the actual data available if the file was originally ingested on a remote network segment. The local server therefore acts as a mediator for all access to the file
data to ensure that large file transmission over the wide area network are kept to a possible minimum. The file storage is therefore initially a virtualized approach. However, to prevent duplicates from being requested from remote servers, all servers attempt to read file data from a local cache before requesting it from its remote location. Thus the local file storage is not a fully virtualized approach, but rather a hybrid solution combining the benefits from both approaches.

With the high level network architecture and information localization strategies defined, one of the first demands risen is interoperability among the various client and server implementations to allow adaption to changes in network topology, hierarchy of information storage/processing and fault tolerance using backup systems. With interoperability between all the systems on the network required, servers have to provide all their information in the same information representation formats through the same interfaces. In addition, their behavior has to be the same when their interfaces are used.

In order to face the problem of interface interoperability, common interfaces have been defined for the server systems which allow all clients to search for existing metadata and attached files, perform metadata modification and ingest new sets of information. To avoid creation of these interfaces from scratch, the “Geospatial and Imagery Access Service Specification” (GIAS) [6] developed by the U.S. “National Imagery and Mapping Agency” (NIMA) has been chosen as a base. Even though the service specification was originally intended for geospatial and imagery data, it was possible to adapt the specification to other product types like organizational documents and derived information like image exploitation products.

The resulting syntactical interoperability on the communication level allows using the same request and response data structures for any server. Partially undefined by the GIAS is the semantics of these data structures which allows the usage of the same interface for different purposes. To ensure that the same understanding/semantics is used by all the participants on the network, the international “Multi-sensor Aerospace-ground Joint ISR Interoperability Coalition” (MAJIIC)[10] has worked on a common semantic definition in the past. The results of the work is semantic interoperability on the communication level which allows for example the integration of server systems with old versions of the data model using automated information conversion. The result is described in various documents and has been incorporated into NATO wide standardization agreements like STANAG 4559 [14] where the “coalition shared data” (CSD) servers – as they are named within MAJIIC – are referred to as “NATO standard ISR library interface” (NSILI).

### 3.2 Data management by metadata

With the communication interfaces, information flow patterns and the localization strategies defined, the next step to interoperability was a common metadata structure by which all the information in the server is categorized.
Aligned with the single point of contact and the materialized metadata storage which allows the clients to access a single source of information without requiring mapping of searches and results, the metadata structure for all product types has been harmonized across all product types so that they are now integrated into a single model structure.

This model structure consists of a “core” which is shared by all product types and “product type specific” content which is only applicable to certain types of products or only to single product types. The metadata shared by all product types covers among others:

- General file information like size, origin and a link to the data itself.
- Releasability markings for the product file and the metadata
- Spatial and temporal location of the described content
- Abstract textual description of file content

The product type specific content describes content as:

- Spectrum of imagery or video data
- Report priority markings
- Operational status of systems

All the attributes from all product types have been sorted into a tree structure so that they are grouped by their meaning. In addition to the easy identification of attributes provided by the hierarchical names of attributes is the ability to use some of these groups multiple times. This allows client systems to describe the individual parts a stored product can persist of - for example a file that consists of multiple images of the same area in different spectral bands produced by the same sensor array.

In order for the available information in the servers to be disseminated to the right people at the right time, the portion of filled metadata needs to be as high as possible. However as not all product types support all the possible information from the core model it is not possible to define all core attributes as mandatory for all product types.

This has resulted in individual flags for each attribute in the model. Using these flags, systems interacting with servers now know which parts have to be provided upon storing new data, and which fields a client system cannot expect to exist for all products.

### 3.3 Shortfalls and Limitations

For complete interoperability between various client systems it is not only required to unify the communication messages, but also the results of each message. The results are uniform product ingestion, metadata update handling, propagation of metadata changes and result sets for queries.

In order to achieve this, the business transactions, the business processes and the mapping of information in the files to their metadata fields need to be defined. The intended result is not only the capability to provide and process the same information, but also to integrate the various systems on their processing level to enable them to work together to achieve their individual goals and the jobs they have been assigned to.

### 4. MODELLING INTEROPERABILITY

A technical solution is - or at least should be - always based on operational needs, business processes and requirement descriptions.

To support an architecture that is built to integrate heterogeneous systems from different vendors, system owners, organizations and even nations it is necessary to have a detailed analysis how this distributed architecture needs to be supported on an organizational, structural and information exchange level.

The technical solution provides the ability to share data over distributed servers. Now it is of interest how this data reaches users with a specific information need.

The focus has to be on different levels of interoperability. On an organizational level the legal and hierarchical framework has to be defined, on a structural level the interoperability of the equipment is in focus and on an information exchange level data has to be filled with meaning.

As described under 3.2 the data is catalogued, and therefore can be discovered by the usage of common and specific metadata. In a distributed architecture with users from different organizations and backgrounds it is necessary to specifically focus on the usage of that metadata and on the semantic it supports.

In the following chapter the different interoperability levels are listed giving an impression of what is necessary to support such a complex organization. A management framework is used to describe those levels.

### 4.1 Organizational Aspects of Interoperability

Operational cooperation at the NATO level aims to strengthen cooperation within collaborative missions. Examples are joint patrols as well as joint intervention and surveillance operations.

Operational cooperation is based on legal aspects like a “Status of Forces Agreement” (SOFA) that defines how an operation is carried out within a specific country or “Military Technical Agreements” under a mandate.

Once the cooperation is agreed to the operational processes have to be inter-coordinated and described.

This includes the command structures of an operation and the work flow.

Operational processes and use cases are defined in specific documents to clarify what information is valid for which user and in what context. These kinds of documents are necessary for the operational users to follow these processes in their specific distributed operational setting.

The specific organizational structure is laid down in organization documents that are exchanged via the CSDs. According to that detached units can setup their systems.
All products that should be shared are labeled according to the defined organizational structure concerning the creator or the unit they belong to. Metadata includes those values, and therefore the organizational layout can be supported within data dissemination and the information can be assigned accordingly.

These definitions on an organizational level are of utmost importance for the next level of interoperability- the structural coordination.

4.2 Structural Aspects
Structural coordination includes the interoperability of equipment, in particular in communications and surveillance technology. This is achieved through the coordination of interfaces and shared products. In the described architecture this is done through the usage of standardized interfaces for data dissemination and retrieval (usage of a shared data storage defined in a STANAG) and the usage of common data formats defined in various STANAGs and specifications. However additionally those standards have to be precisely defined and described. Standards are often only a guideline for usage; specific implementation guides give information about the specific usage of a standard and which (meta) data attributes are used in an environment. After having done this a third level of interoperability has to be taken into account- the level of information exchange.

4.3 Information Exchange
Information exchange implies a common understanding, data formatting, common semantics etc. With a technical solution that provides data distribution hubs, organizational agreements and structures and coordinated formats and interfaces it is now possible to share data. Different systems are now able to read data and users will even know where the data comes from. What is not solved until now is the possibility to share the meaning of that data and therefore provide real information and eventually produce knowledge. What do metadata values mean? To enable this level of interoperability the operational processes have to be defined in technical business rules and use cases that describe how an operational process is supported by technical processes and which information has to be provided to which system to have a consistent information flow. For example it is necessary here to describe which values of the organizational documents (see 4.1) have to be set in the metadata of each product, or which product values should be stored in the metadata.

Additionally the semantic meaning of values has to be described. An example for that is the meaning of the free text field “title” within the CSD metadata. To be able to query for specific products according to the title the way this value is defined has to be described. The same is true for other free text fields like “description”. Is a description a list of specific values or is it plain text?

If an attribute consists of a defined list of values the meaning of the values has to be clarified as well. What means the value “Flash” for a priority? What does the value “Draft” imply for a document? When will a “Draft” be set to “Current” etc.?

Especially when data is shared among different nations and user groups the definition of meanings has to be paid attention to. With users coming from different organizational or cultural contexts one cannot rely on an implicit coherent interpretation.

4.4 Management Framework
The multitude of models, concepts, business rules, agreements and standardizations for both technical and non-technical issues of interoperability in multinational surveillance and reconnaissance require a widely-established management framework for further development and maintenance. For this purpose, the NATO has developed the NATO Architecture Framework [11] which allows the management of technical and non-technical aspects of system-of-systems architectures. Seven different views allow focusing on specific architectural aspects. The NATO All View (NAV) manages for example general military procedures, concepts of operations and agreements. On the contrary, the NATO Systems View (NSV) and NATO Technical View (NTV) assist the management of technical aspects like the specification of participating systems and their interconnection (e.g. use of TCP/IP based upon an Ethernet network). Finally, the NATO Operational View (NOV) defines the command structure, information flows, operational/business processes and business rules between the participating systems. This includes for example the types of the exchanged information specified by STANAGs and the frequency of the exchange. The remaining three views of the NATO Architecture Framework are the NATO Capabilities View (NCV), NATO Service-Oriented View (NSOV) and NATO Programme View (NPV). All three views can be used for further definition and description of the intended system-of-systems architecture.

5. DEPLOYMENT
The previously described architecture was implemented in several trials and exercises. The core component for data dissemination always was a shared database. Data fusion was implemented on varying levels within the different projects.

5.1 MAJHIC
The primary driver for the Coalition Shared Data (CSD) Server was the project of MAJHIC (Multi-Sensor Aero-Ground Joint ISR Interoperability Coalition) [10]. During the last conflicts that German Bundeswehr and allied forces were involved in ISTAR Data (Intelligence, Surveillance, Target Acquisition, and Reconnaissance) could not be shared and exploited among the involved forces because of technical and operational problems which resulted in a loss of human lives and material.

To avoid this in the future the multinational project was introduced. The aim was to strengthen and prove the processes, methods and applications that support interoperability. Interoperability is enforced by standardized data dissemination.

The sensor data that is processed within the sensor workstations in proprietary formats is transformed into
The concept passed its first full-blown test during a major NATO exercise in Norway, Bold Avenger/Trial Quest 2007 [16], which included real-time maneuvers by several thousand air and ground forces. During the exercise joint ISR interoperability was demonstrated in a „Live environment with a multi-sensor, multi-service geographically dispersed set-up”.

5.2 Common Shield
In 2008 the concept was successfully tested during the common Bundeswehr experiment Common Shield and NATO DAT (Defense against terrorism) experiments Technology of ISTAR against Terrorism, Critical Infrastructure Protection, and Harbor Protection Trial [15]. The aim of the Common Shield exercise was to test C2 (Command and Control) processes in a NEC (network enabled capability) environment with integrated ISR (intelligence, surveillance and reconnaissance) and C2 systems. The Common Shield architecture integrated sensor systems, exploitation capabilities, situation awareness tools, common operational picture displays, and C2 systems provided by 27 different producers. Amongst the collection assets there were airborne imaging sensors and ground based imaging sensors; but also ground based radar systems and chemical sensors capable to detect explosives as well as sea-based surface and sub-surface sensors. Exploitation systems provided capabilities to exploit still and motion imagery, radar data, to fuse alarms generated by the chemical explosive detection sensors with imagery, and to fuse alarms and tracks generated by the sea-borne sensors with imagery. The seamless data and information exchange of all the sensor data and exploitation products with a real-time update of the common operational picture was enabled by the employment of a series of CSDs with the capability of storage, query, subscribe and retrieve, and automatic real-time synchronization of metadata.

5.3 SOBCAH
An exemplary implementation of this architecture was realized and successfully demonstrated in the European Project SOBCAH [13]. Within a demonstration at the harbor of Genoa different threat scenarios were exercised. The joint observation of land- and sea-borders with a variety of sensors, among them sonar, radar, video (IR and EO), container and car tracking systems and motion detectors, was tested. The information retrieved from all these sensors was stored in the SOBCAH Shared Database (SSD) that was designed upon the described architecture principles. A situation awareness system subscribed (via a client) to data stored in the SSD and was able to display all relevant information for local decision bodies. As it was possible to store relevant data forensic analysis at a later point in time was possible as well.

The demo showed successfully that data from all kinds of different sensors can be integrated into one system where in a timely manner, i.e. without long delays in time due to the large amount of data a common ground picture of a situation can be extracted.

6. FUTURE RESEARCH
The result of this level of interoperability is a previously not achieved level of failure safety and the capability of the systems to work together on a job. The high level of failure safety is the intrinsic result of the high abstraction level which renders both the network topology and the systems used transparent to the business processes. By replacing faulty systems with currently unused/stayby systems or systems previously assigned to lower priority processes, even time critical job assignments can be fulfilled by exchanging their abortion with those of low priority tasks.

Achieving interoperability in a complex setting like this where multiple nations need to share information and react adequately and being able to integrate legacy systems as well as new technologies still leaves room for improvement and future research. Some efforts are listed below:

- Improve information quality
  To avoid storing invalid combinations in metadata an automated rule set application could enforce additional validation at runtime in future versions of the server. This could be done by using OCL or First Order Logic.

- Analysis of correlation between stored information (business intelligence/data mining)
  In contrary to duplicate detection, the analysis of correlation can be applied to detect reinforcement associations between stored information. E.g. information confirms each other.

- Information fusion
  The analysis of correlation can be used as base to generate aggregated information using information fusion methods like fuzzy logic, bayes’ theorem or artificial neural networks.

- Archiving and metadata lifetime
  In the current server implementations, all the information exists as long as the server exists. This is possible as the servers lifetime is currently rather short (e.g. an experiment). For long term usage however (e.g. many years of operation), the systems will run out of disk space at some point, which puts them into the need to move data out of the system. In future work the process of archiving needs to be defined and applied by all servers to ensure that a common information lifetime is maintained and provided to the client systems.
Integration of services in the current architecture and evolution into a SOA

To apply automated business process execution, business rules enforcement and shared services for metadata and product validation the current architecture has to be able to integrate aspects of a web service based SOA. The advantage of a web service based approach is a sophisticated tool support for configuration and execution of automated tasks and flexible composition of the system landscape.

7. ACKNOWLEDGMENTS

The architecture was part of the projects MAJIIC and SOBCAH that were (partially-SOBCAH) founded by the BMVg and the EU. The authors acknowledge valuable help and contributions from all partners of the projects.

8. REFERENCES


