An Integrated System for Intelligence, Surveillance and Reconnaissance (ISR)

Barbara Essendorfer, Eduardo Monari, Heiko Wanning
Fraunhofer IITB
{essendorfer, monari, wanning}@iitb.fhg.de

Abstract—**Connecting systems that are responsible for gathering information of any kind (e.g., images (optical/infra red/radar), video streams, vehicle tracks, etc.), processing stations (merging images series, stabilizing videos, etc.) and exploitation systems in a large (e.g., multinational) environment is a difficult task. Currently those stations tend to be operating independently irrespective of the vast amount of other systems available.**

As cooperation between different nations and different operating entities (civil and military) is increasingly important the sharing of information to generate a common awareness is vital.

This paper describes a solution towards this goal by introducing a system capable of dealing with the ingestion and distribution of data and the fusion perspectives/possibilities that arise when a multitude of stations report a single event from many viewpoints.

Keywords: client-server architecture, sensor/ exploitation/ information system, information/ data fusion, ISR

1. Introduction

ISR (Intelligence, Surveillance and Reconnaissance) in civil and military environments is often accomplished using separated stove-piped systems, therefore data accumulated from multiple heterogeneous sensors can't be shared and the capabilities to fulfill missions are limited. Services, like data/information collection and analysis, are not performed by the best but by the only system available, resource management is therefore suboptimal. To overcome this problem a concept to share data has been developed and implemented: A Coalition Shared Data (CSD) Server is used to store standardized data. It allows the dissemination according to user requirements, network and security settings. Tasking elements, sensor and exploitation systems store relevant metadata and products in common (standardized) formats in a shared database. The data model and interfaces of the database are based on established military standards (STANAGs). Instead of "only" collecting and distributing data an integrated data processing approach also should evaluate the incoming information, preselect interesting events for the human operator and, by using fusion algorithms, summarize complementary information and sort out redundant data to reduce the amount of information. This fusion aspect will be shown exemplary in the domain of image and video fusion.

The CSD concept was deployed in a rather restricted environment where legacy systems are in place that have to be reliable and secure. These systems are developed by different nations and by different companies. The challenge in such a context is "real" interoperability. To achieve this some constraints were put externally on properties of the final architecture (e.g. using STANAGs for the description of data, meta data and the client-server communication "language"), that our solution had no way to circumvent. Therefore the result and described work here is the output of those design decisions giving in our opinion the best possible solution solving the given problem under the mentioned restrictions. The design and implementation phases were and still are a long continuing process.

This paper is based on a conference paper that focused on border surveillance [1]. Here not only civil applications are taken into account, but the full aspect of civil and military ISR.

It is structured as follows: in Section 2 the task of information sharing within ISR is introduced and described. In the following section, the requirements for standardized data formats, which are highly important for information sharing, are discussed. Next, in Section 4, our system architecture for integrated ISR systems is presented. Finally, exemplary deployments of the developed system, which have been used in different military exercises

and demonstrations on civil security are described.

2. Information Sharing within ISR

ISR are different aspects of information gathering with human and technical sources to enhance situation awareness. This happens on different organizational and administrative levels.

Within (civil) surveillance on a local level, immediate measures have to be found to enable a quick and efficient reaction to an imminent danger. On a regional level relevant information has to be shared to be able to exercise precautionary measures and avoid an escalation of a crisis. If the local authority is not able to handle the crisis, reinforcement has to be provided. If a crisis affects more than one region or even country then national and transnational decisions have to be made and information has to be shared.

Another (military) differentiation is information gathering on a tactical, functional or strategical level. On a tactical level decisions have to be made within operations based on information on current events and immediate decisions on an appropriate reaction have to be made (short term decisions). On a functional level situation awareness is generated to enable the planning of current military operations (mid term decisions). On a strategical level situation awareness is generated with security-relevant information to enable decision makers (on a political and military level) to predict long term developments in critical areas.

The use of a mix of sensor and information systems is key to adequate situation awareness on the different levels.

2.1 Integrated ISR Systems

Within an integrated ISR system, disparate technologies that complement one another are installed, the interaction of the data output is essential.
An integrated ISR system consists of sensors (technical systems and humans), exploitation systems (that might also be deployed as situational awareness displays) and external information systems.
In Figure 1 a critical area, e.g. a border is monitored by a range of different sensor types. Those sensors deliver data to a surveillance unit (SU). However, the areas that are monitored intersect and data that is of interest for one surveillance unit may also be of interest for adjacent units. Our architecture allows the necessary data sharing and accommodation of additional information from external systems resulting in enhanced situation awareness.

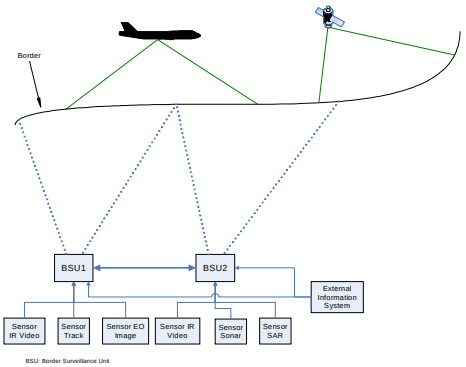

Figure 1: Surveillance System

2.1.1 Sensor Systems

Sensor systems normally consist of the sensor and a ground station that does the primary data processing and possibly some exploitation. Combined sensor systems that consist of different sensors might use some sensors as triggers for others and only the secondary information is passed on to an “outside” exploitation system. Depending on the sensor type and the processing a proprietary (raw) data stream may be created. To observe different types of critical areas it is necessary to make use of different sensor types with differing ranges and tasks [2]:

- Long-range surveillance conducted by space borne and airborne systems is of interest for an all-weather and 24 hour detection of threats that harm a wide area (e.g., oil slicks that indicate an attack on the environment and/or on nations resource supply). The sensors can deliver all kinds of imagery such as IR (infrared), EO (electro optical) and SAR (synthetic aperture radar) as well as motion imagery (video), SIGINT (signal intelligence) or radar data.
- Airborne sensors, including the use of balloons or zeppelins can be used for medium-range surveillance.
- Ground-based or seaborne sensors are mainly used for short-range surveillance. Real time information can be provided on critical areas, objects and people. Seaborne sensors can be installed above (cameras, radar) or under water (e.g., sonar, metal detection).

The display of sensor data in a common picture only makes sense if the operator/analyst is able to interpret

that information correctly. Raw sensor data have to be interpreted by specialists. Therefore sensor data are only provided on system, local or at the most the regional level.

2.1.2 Exploitation Systems

Exploitation Systems are used for the exploitation of preproduced data. Exploitation can be done in different contexts and can be specific to the system, data type, area or task. For exploitation systems that work on products that are produced from multiple sensors it is important that data are available in an inter-coordinated data format (see section 4.2 for how it was implemented in our case). Exploited data normally already contain more enhanced information. Similar to the sensor data it has to be integrated adequately into a common picture. This type of information is of interest for upper decision bodies. Still some special expertise is needed to read and decide upon it. On a national level only the result of an analysis would be provided. The main effort on this level would be to fuse information from different sources. (more on fusion in section 3.3)

2.1.3 Information Systems

Information systems are relevant for the rating/ evaluation of derived data and information. Weather data can give essential advice which product sources are of interest in certain circumstances, systems such as the "Schengen Information System" (SIS) provide data on detected persons or goods and databases/information services freely available on the Internet can provide background information for all kinds of questions (provided it is understood that this is in general low grade intelligence). Public information sources are subject of data protection and the usage of this data has to be legally defined across borders. The system type, structure, language and concepts that are used within those systems differ from region to region and nation to nation. This is why an integration and combined usage of such system information is extremely complicated. Apart from legal regulations, aspects of intelligent data discovery and sharing are subject to research and discussion here.

2.2 Situation Awareness

Situation awareness means that threats and suspicious behavior have to be perceived, the threat has to be understood and an appropriate reaction has to be performed [3]. To perceive threats, products from different sources (information systems, sensors, exploitation systems) have to be available. The data has to be accessible with respect to time and location of the product as well as to other decision-relevant (e.g., urgency) information. Relevant sources of knowledge should be incorporated. Integrated systems achieve enhanced situation awareness by developing a common picture of the tasked area. To support analysts, operators and decision makers it is important to integrate the correct i.e. temporally relevant information in this common picture in a user-friendly manner [4].

2.3 Information Fusion

In general, the usage of multiple and heterogeneous sensors increases the possibilities and functionalities of the superior system and therefore improve the quality of the surveillance task. Especially for security applications (i.e. monitoring) state of the art multi-sensor-systems enable the surveillance of large areas with a reduced amount of manpower.

On the other hand, large sensor networks produce a huge amount of information that the analysts and operators have to monitor. Therefore, automatic data processing and information fusion is an essential part of large distributed and multimodal surveillance systems. The highest benefit of implementing automatic image processing is achieved when the automatism attracts the operator's attention on relevant events and situations only. Hereby, integrated data processing approaches evaluate the incoming information and preselect interesting events for the human operator. Motion detection algorithms for example lead to a reduction of the operator's workload by generating indications of movement automatically and therefore allow the human operator to focus on areas of interest only.

This clearly can be solved more robustly, when sensors of different modalities are incorporated (e.g., video cameras with a visual spectrum during the day and infrared spectrum at night). On the other hand, the usage of different sensor modalities requires the implementation of more complex schemes for information fusion. Implementing theses schemes will result in a higher level of information quality, since automatic sensor data processing and information fusion summarize complementary information and reduce the amount of redundant data.

3. Architectural Aspects of Information Sharing

As stated above, the surveillance of borders or areas of interest requires the co-ordination of many different agencies each with their own personnel, systems, assets and equipment.

The task of information sharing in a time sensitive domain places requirements on the architecture. To be able to share data and information some aspects have to be taken into account:

Information has to be reliable and secure: To be able to make the right decisions and react appropriately, information has to be reliable. Access to classified data has to be limited to entitled agencies and persons. To ensure the security of the data transfer and the protection against cyber attacks encryption and authentication techniques must be implemented. Also, user roles that include access levels can be used to restrict data access to authorized persons only. In addition it allows the display of only the relevant data to the right personnel (analyst, decision maker on a regional/national level etc.) avoiding information overload.

Information has to be provided in time and at the right place: An adequate data transmission network is required (i.e. distributed architecture and standardized mechanisms to access data). At the first step databases at different locations only synchronize their meta data ("video clip from location x, time y, sensor z, showing i") and not the full data (the video file itself) as this would mean shifting unnecessary data loads through out the network causing congestions.

To integrate information systems with different semantics, intelligent methods of information retrieval have to be established. The annotation of information with metadata and ontologies enables semantic interoperability between the systems.

To be able to access data in time at the right place data transmission between more than two systems has to be enabled. This leads to a distributed architecture and standardized mechanisms to access data. Databases at different locations have to be able to synchronize their information, without synchronizing the data as this would mean to shift unnecessary data loads through the network.

To grant an easy and adaptable data access standardized data formats and data sharing mechanisms should be used. The data formats have to provide the right type of information which implies a detailed analysis of the application domain.

3.1 Data formats for the ISR domain

The previously described particularities of the domain make an adequate handling of the data necessary.

Surveillance has to be weather, season and daytime independent. Sensor systems have to consider the various landscapes and it has to be possible to detect all kinds of threats. Thus different sensor types providing different data types have to be deployed.

A mix of sensors has to be implemented. To survey an area at night time thermal sensors like infrared (passive or active) have to be installed, contrariwise these sensors are not built for hot weather. Metal detectors have to be deployed to register weapons and for gas or explosives olfactory sensors are of interest.

To get an overall picture and assign surveillance products to an area and put them in a chronological context as well as to fuse data, it is important to provide metadata with the product. The requirements at that point depend on the overall architecture and the display, exploitation and fusion capabilities. Information on chronological and areal allocation of the product, the source and the coverage of the sensor as well as the product type and size should be mandatory. If the data is confidential congruent metadata has to be defined.

Standardization agreements exist in the military domain as well as in the commercial world. NATO standards are of interest for ISR because of the dual use within military and civil ISR. Nations with heterogeneous information and sensor technology need to combine their efforts and achieve a common situational awareness. Most of the information is time sensitive and in both domains there are areas of graded interest.

In the commercial world there are a number of standardization agreements but most of them are less binding and the commitment to those standards is dependent on the application domain.

- ***Military standards***

For the storage and dissemination of digital data STANAG (Standardization Agreement) 4559 NSILI (NATO Standard ISR (Intelligence, Surveillance, Reconnaissance) Library Interface) is the standard interface for querying and accessing heterogeneous product libraries maintained by various nations. "The interface provides electronic search and retrieval capabilities for distributed users to find products from

distributed libraries in support of, but not limited to, rapid mission planning and operation, strategic analysis, and intelligent battlefield preparation. The overall goal is for the users, who may be intelligence analysts, imagery analysts, cartographers, mission planners, simulations and operational users from NATO countries, to have timely access to distributed ISR information..." [5].

For data types like image, video, radar or tracks standardized formats exist and are in use (e.g., STANAG 4545 [6], STANAG 4609 [7] and STANAG 5516 [8]). For secondary information like the textual analysis of surveillance products report standards are defined.

- ***Commercial Standards***

The OpenGIS® Catalogue Service [9] defined by the OGC (Open GIS Consortium) is a standard for data dissemination that concentrates on geospatial data, related services and resources. It was not designed for the surveillance area, but could be adapted. The functionalities are similar to the ones defined in the STANAG 4559 [5].

For digital image conservation or video compression there are many standards available. The usage depends on user and domain needs. For video the codices and container formats defined by the MPEG (Moving Pictures Experts Group) consortium are among the most popular ones. Here standards for video compression (MPEG-2/ MPEG-4) and the management of corresponding audio and collateral data (MPEG-4) as well as the handling of metadata (MPEG-7) are defined. For tracks the ASTERIX (**A**ll Purpose **ST**ructured **E**urocontrol Su**R**veillance **I**nformation E**x**change) Standard that is defined by Eurocontrol [11] is of interest. In the maritime sector the NMEA (National Marine Electronics Association) defined a standard that handles navigation data [10].

It is necessary to consider using "the best of both worlds".

3.2 Data transmission

The choice which medium (wired ethernet/ wireless) to use depends on: the number of connected sensors/sensor ground stations, their location in space, their mobility and the kind of transmitted data. Generally, if the required overall data rate is very high, wireless communications might have problems before a landline's limit would be reached. Also, security aspects deserve closer attention when using a wireless connection, since it is easier for the man in the middle to listen in, provide false information or disrupt communication. The usage of cables which can be shielded much easier than the complete area of radar coverage bears a smaller risk in this regard.

For the implementation an architecture was chosen with wired connections wherever possible, only a few sensors are connected via a radio link due to the vast distances covered and the prohibition to lay cables everywhere.

4. An architecture for ISR

As ISR systems need to consist of many components it is necessary to build a flexible and adaptive architecture. Once the system components (sensors, exploitation and information systems) are decided upon, it is necessary to establish a way of connecting them. This chapter will detail the "how" of data transfer, what network layout to use. It will explain what happens to the data, once they have left the originating sensor, and in what way they arrive at the desired destination (i.e. the analyst).

For the integrated sensors and information sources converters have to be developed that translate the incoming data into a common data format. As can be seen in Figure 2 different proprietary data formats are converted into a standardized one, so that inquirers do not have to know the type of source (e.g., sonar, radar or infrared) the information is coming from, but can focus on the information itself. The architecture described here is based on these formats (resp. STANAG 4559) [5].

The standardized data is then transferred over the network to a local data server. Connected to the same network are exploitation systems taking in a filtered set of the provided information (depending on the tasking). By fusion and analysis they generate new additional information (e.g. reports) that is also stored in the data server(s). Situational awareness systems are able to display selected intelligence and can ask for additional information from sensors, exploitation or information systems to support decision makers. A detailed description of data dissemination with the shared database is explained within 4.1.

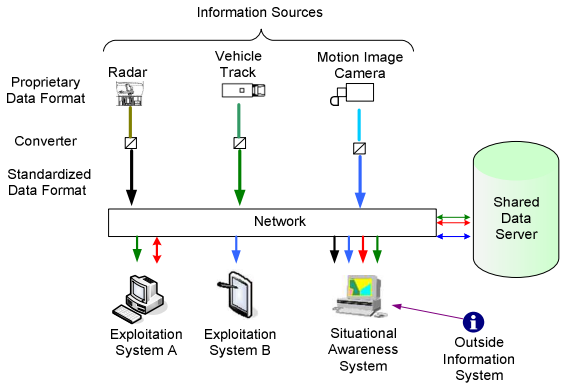

Figure 2: Information sharing within a local architecture

4.1 The Shared Database

The middleware CORBA for the client-server communication was chosen due to its providing transparency in regards to object location, language, and implementation and its established and widespread proven stability and performance. The clients access the server using interfaces for the ingestion or retrieval of data (see Figure 3). If a product is stored in the database, the client hands over the metadata and the product itself to the database via the CreationMgr. To retrieve a product the client asks for the metadata via the CatalogMgr and is able to order the product if it is of interest for the user. Within the metadata all (for the domain) relevant aspects of the product are defined and queryable. Those parameters could be for example: location, time, speed, size, friend/foe, weather condition, certainty of the info, product type.

There are two different ways of retrieving data:

- With the interactive query the user searches the database on aspects of the product (e.g. time, space, product type). A summary of the results is presented in list form on the screen and the relevant data sets can be marked for download in the next step.
- With the subscription method the data query is transferred to the server once and continues running for a set time interval whereby the client is automatically notified whenever new incoming data sets fit the query parameters.

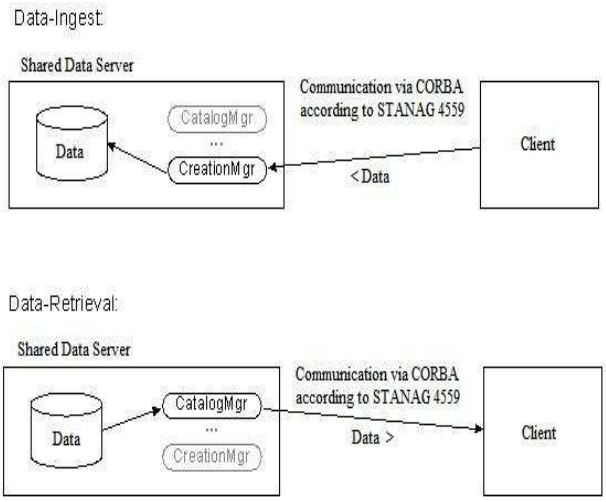

Figure 3: Data ingest and retrieval with the client

Synchronization of information is necessary to be able to share information along different levels and locations. To distribute information from the local network to all interconnected nodes, thereby reducing bandwidth usage and increasing stability, a decentralized setup is used. Here (see Figure 4) the regional servers/local network hubs (in white) collect the data from their directly connected information sources (in black), respectively the converters.

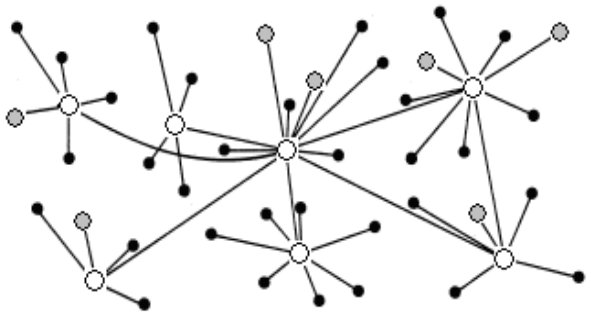

Figure 4: Decentralized network

Note, that sometimes (preferably always) several possible connections between regional servers exist, so that connection loss on one link does not mean the cut off of data sharing. This is especially important, since the connections are of varying quality and reliability (ranging from fluctuating small band wireless to high-speed cable).

The regional servers synchronize their respective

metadata content among each other in times of otherwise low network usage but in a set minimum interval using the mentioned subscription method whereby server A plays the role of client when receiving data from server B. The original product data (e.g., images, movie clips of possibly high data volume) are kept only on the originating server. When a situation awareness system (in grey) wants to collect data from different sources scattered throughout the whole network, it uses its client to send a query to its local server which delivers the results by looking only at its own data base. Only when one or more of the results are specifically requested, a connection to the originating server is initiated where the potentially large files (e.g. videos) are transported across the network.

This setup has the advantage of reducing the amount of data traffic on the overall network, because bigger data packets are only transferred on demand, not every time they are created. Also, the local servers serve as a backup in case of network or server failures.. That "complete reliance upon a single point is not always required" [12] was the idea that started the ARPANET (Advanced Research Projects Agency Network) in the 1960s, which later evolved into the Internet.

This system is fully scalable, i.e. the size of each 'subnet' including its server can be understood to be either belonging to a certain sensor type in a small region or at the other extreme they could also consist of all sensors of a nation participating in a European network. Also, several layers of subnets are possible.

In addition to accumulation, storage and distribution of data, other tasks of the servers can be the processing and generation of new data out of the received information. Examples are:

- Data fusion (combine the information obtained from a daylight and infrared camera pointing at the same location resulting in new knowledge unobtainable from each single sensor individually)
- Data clarification/extraction (motion imagery processing like image stabilization, mosaicing, object tracking, noise reduction)
- Object recognition (e.g., 3-D object recognition using several 2-D images [13])

To allow hierarchical information access according to different levels of authority further data fields (metadata) are necessary for each product.

On the server – querying client connection side user roles have to be supported, i.e. clients need an account specifying their access rights and statuses. For restricted information, a login and user password has to be supplied before each connection to guarantee the authenticity and the right of access. Additionally, the usage of certificates raises the security of the system to a satisfactory level.

To circumvent unauthorized access to sensitive data from a third party and ensure a secure transmission the data transfer should be encrypted (for example by using a private key infrastructure (PKI)). Using secure lines alone only saves one from intruders outside the network of permitted nodes, but not everyone within the network should be able to read all data from everyone and everywhere. A further complicating situation arises when "friends become foes" within coalitions: a partner who you share data with in one area might be a competitor/adversary in another area or at another time. A more detailed analysis of this "Dynamic Coalition Problem (DCP)" with an emphasis on the military domain can be found in [14].

4.2 Image and Video Processing

In surveillance systems, image and video processing modules are incorporated for three basic reasons: The first one concerns the human machine interface, more precisely the enhancement of video stream visualization. The second one concerns automatic or semi-automatic scene understanding to disburden the operator or analyst. The third one concerns aspects of efficient data storage, e.g. for recording the happenings for offline reconnaissance.

Visualization of sensor data streams may be improved by diverse methods of automatic image processing. The purpose thereby is, to manipulate the video streams such that the video material is optimized for the perception of a human observer, e.g., realized by automatically optimizing contrast or color values of the images.

Another way of improving visualization requires some basic methods of automatic scene understanding: Highlighting moving or otherwise relevant objects or persons in the video streams help the human observer to focus his mind on relevant situations. The same procedure can be implemented, when aspects of data storage are addressed: Instead of recording all sensor data all the time, the recording functionality can be switched off, whenever the scene

does not show any (relevant) alteration.

More complex forms of automatic scene understanding can be established in order to generate alarms that call the observers attention to an abnormal situation. Since this kind of high-level situation awareness highly depends on the specification of the specific abnormality and – in addition – presumes more scene information, these methods are less portable to scenarios other than specified.

A system was built that includes a module for (semi-) automatic video processing and sensor data fusion. The module is able to process heterogeneous video sensors (e. g. EO, IR) from different video providers and redistribute extracted information to all participants using the shared database capabilities. Additionally, the image processing module uses sensor information provided by non-video sensors (e. g. sonar, radar, etc.) for automatic control of movable video sensors.

For interaction with the integrated algorithms, a user interface for image processing and analysis was created. The so-called Image Processing Unit has access to all available video streams in the sensor network, is able to receive alarms from all (video and non-video) sensor systems over the shared database and is additionally able to request stored imagery data for offline processing of historic video data from all video providers.

The Image Processing Unit acts as a fusion module between different video sensors and non-video data sources providing three basic processing modes: single-sensor video processing, multi-sensor video fusion and video-sensor remote control (by non-video sensors). In “single-sensor video processing”-mode the Image Processing Module provides generic sensor independent algorithms, applicable to all video sources available in the network. Using the GUI of the Image Processing Module the user is able to select an arbitrary video sensor provided by any participating subsystem and process the video data by miscellaneous algorithms, like “automatic motion detection”, “video-based moving target indicator”, “multi-object-tracking” or “real-time video mosaicing”. The processed video streams are sent back to the sensor network (to provide results to all participants) and important information (detections / alarms etc.) is additionally archived in the database. Of course, if an automatic image processing algorithm detects suspicious behavior it generates alarms like any other subsystem, and broadcasts the information using the common track data and the shared database.

4.3 The Fusion Perspectives

As motivated in 2.3, automatic image processing by means of analyzing distributed and multimodal sensor-data, requires the implementation of sensor fusion techniques, which can be solved by various types of fusion techniques.

In the context of (semantic) sensor data analysis, information fusion can be characterized under several aspects. One of these aspects focuses on the level of information aggregation, where the fusion takes place: “early fusion” indicates that information is fused before semantic descriptions are derived. This might be realized by extracting (abstract) features from each of the sensors, which then are concatenated to a common description, i.e. in terms of a high dimensional vector. The analyzing step then is solved on the common description and results in a multimodal description of events, situations etc.

“Late fusion” on the contrary indicates, that semantic concepts are derived from unimodal sensor data and the fusion step (that often coincides with a kind of decision or detection) is implemented on these semantic descriptions.

Both techniques are applicable in surveillance systems. While early fusion is predestined to be applied on sensor data, that is acquired within a locally limited area where redundant information has to be expected, late fusion techniques should be preferred, when events have to be evaluated in a more global manner.

Another method of sensor fusion, that is relevant for surveillance tasks, is to assign each type of sensor a sensor specific task, e.g., using PIR motion detection sensors as trigger for detailed automatic or semiautomatic analysis in EO- or IR-cameras. This approach is even more efficient, when the cameras are mounted on pan/tilt units: Triggered by non-video sensors cameras can be sighted towards the detected event. This kind of active vision not only results in reduced computational effort, but also allows the reduction of the amount of sensors, that have to be installed. Moreover, this method provides an interaction-free view on the point of interest in a high image resolution.

Finally, the direct fusion of video streams for visualization is a worthwhile technique in the context of surveillance systems: When the number of video streams that have to be displayed in order to monitor a scene is high, multiple sensor streams can be fused

into one common video stream. This is even more profitable, when cameras of different modalities are directed onto the same location of the scene, since there exist image fusion techniques that accentuate the sensor specific information. E.g., for two cameras, one of them in the visual and the other one in the thermal spectrum, these approaches deliver images, that show visible structures and thermal structures as overlays.

5. Deployment of the Architecture

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 differentiating levels within the different projects.

5.1 MAJIIC

The primary driver for the Coalition Shared Data (CSD) Server was the project of MAJIIC (Multi-Sensor Aero-Ground Joint ISR Interoperability Coalition) [15]. 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 standardized formats and shared over standardized interfaces.

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 (Defence against terrorism) experiments Technology of ISTAR against Terrorism, Critical Infrastructure Protection, and Harbour Protection Trial [17]. 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 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 providing MTI 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, MTI 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 [18]. Within a demo 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. Conclusion and Future Work

Within MAJIIC detailed processes to share information within the ISR domain have been developed, implemented and tested. The focus of this work was on multinational information sharing within a coalition with (mainly) satellite and airborne IMINT sources. The usage of an architecture as previously defined proved to be applicable for the information exchange between different nations.

Within the Bundeswehr experiment Common Shield adaptability of that architecture to different sensor types and surveillance needs was successfully tested. Although the adaptation of some of the STANAGS was necessary it was possible to integrate new systems in this type of architecture relatively easily.

Within SOBCAH the usage of such an architecture in a civil environment was demonstrated. Data fusion techniques as described above were of great use to help the operator focus on relevant events.

For future work within CIMIC the seamless integration such an architecture with the means of converters and services should be further developed.

Standardized mechanisms of data dissemination in civil and military security applications should be enforced as this enables an agile plug and protect system. Sensor and information systems can be integrated and thus different sources of information can be fused if necessary.

The integration of other data/information sources (e.g. human intelligence, electronic intelligence) in such an architecture has to be evaluated and planned. To be able to cooperate on a semantic level the mapping of data models and ontologies from the different domains (civil and military, ISR and C2 etc.) has to be enforced and integrated in an intelligent situation awareness system.

7. References

[1] Essendorfer, B., Monari, E., Wanning, H.(2009). An Integrated System for Border Surveillance. GlobeNet ICN 2009, International Conference on Networks. 28.02.-05.03.2009. Cancun, Mexico.

[2] Jaeger, T., Hoese, A., Oppermann, K. Transatlantische Beziehungen. Sicherheit-Wirtschaft- Oeffentlichkeit. Verlag für Sozialwissenschaften. 2005

[3] Endsley, M. R. Situation awareness global assessment technique (SAGAT). Proceedings of the National Aerospace and Electronics Conference (NAECON). (New York: IEEE), 789-795. 1998

[4] Endsley, M.R., Garland, D.J. Situation Awareness Analysis and Management. Lawrence Erlbaum Associates. 2000

[5] STANAG 4559 NATO Standard ISR Library Interface. Edition 2. http://www.nato.int/structur/AC/224/standard/4575/ag4_4575_E_ed2_nu.pdf. 27.07.2009

[6] STANAG 4545 NATO Secondary Imagery Format (NSIF). http://www.nato.int/structur/AC/224/standard/4545/4545_documents/4545_ed1_amd1.pdf. 27.07.2009

[7] STANAG 4609 NATO Digital Motion Imagery Format. http://www.nato.int/structur/AC/224/standard/4609/4609_documents/4609Eed01.pdf. 27.07.2009

[8] STANAG 5516 Tactical Data Exchange- Link 16.

[9] OGC (2005). Open GIS Consortium. OGC catalogue service specification. http://portal.opengeospatial.org/files/?artifact_id=5929&version=2. 27.07.2009

[10] NMEA 0183 Interface Standard. NMEA 0183 Interface Standard

[11] Eurocontrol standard document for surveillance data exchange. Part 1. All Purpose Structured Eurocontrol Surveillance Information Exchange (ASTERIX). http://www.eurocontrol.int/asterix/gallery/content/public/documents/pt1ed129.pdf. 27.07.2009

[12] Baran, P. (1964) On Distributed Communications Network. IEEE Transactions on Communications [legacy, pre - 1988], 12, 1

[13] Dutta Roy, S., Chaudhury, S. and Banerjee, S. (2004). Active Recognition through Next View Planning: A Survey. Pattern Recognition, 37, 3, pp. 429 – 446

[14] Phillips, C. E., Ting, T.C., Demurjian, S. A. (2002). Information sharing and security in dynamic coalitions, Proceedings of the seventh ACM symposium on Access control models and technologies, June 03-04, 2002, Monterey, California, USA

[15] MAJIIC (2007). http://www.nato-otan.org/docu/update/2007/pdf/majic.pdf. 27.07.2009

[16] Trial Quest (2007). Key NATO reconnaissance technology passes major test. www.nato.int/docu/update/2007/12-december/e1210d.html.27.07.2009

[17] Stockfisch, D. (2008): Common Shield 08. TechDemo 08/Harbor Protection Trials. Strategie & Technik, October 2008

[18] SOBCAH. Surveillance of Borders, Coastlines and Harbors, http://ec.europa.eu/enterprise/security/doc/project_flyers_2006/766-06_sobcah.pdf.27.07.2009