2009 Fourth International Conference on Systems

An Integrated System for Border Surveillance

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

***Abstract*—Borders are extremely vulnerable and prone to terrorist attacks, smuggling and illegal immigration. To achieve enhanced situation awareness it is necessary to fuse sensor and information data. By automated fusion of referenced and associated data an aggregation of raw sensor data is achieved.**

Within the project SOBCAH (Surveillance of Borders, Coastlines and Harbors), an architecture was developed and tested that supports the sharing of information from heterogeneous sources. Additionally techniques of data fusion within video data were used to enhance information and provide operators with relevant details of an event.

1. Introduction

Effective control and surveillance of the European border is a matter of the utmost importance both to member states and to the European Union itself [1].

At present border surveillance is often accomplished through separated stovepiped systems. Data that might be of interest for not only one but many surveillance units can't be shared and thus the capabilities to secure the border are limited. To overcome these limitations, interoperable transnational surveillance systems, capable of including all relevant data sources and sharing them among border related law enforcement bodies are needed. Within the project SOBCAH (Surveillance of Borders, Coastlines and Harbors) [2], an architecture was developed and tested that supports the sharing of information from heterogeneous sources. An experimental system based on this architecture was developed, set up and evaluated during the final demonstration in July 2007 at the harbor of Genoa, Italy. The experimental system for the demonstration successfully handled event information from about 15 sensors generated by 10 subsystems provided by participating companies
from 7 nations. This paper provides an overview over the systems architecture and the principle of data sharing. It gives an insight into methods used to enable information fusion and automatically process images and image series.

2. Levels of Information Sharing

The surveillance of borders happens on different organizational and administrative levels. On a local level, immediate measures have to be found to enable a quick and efficient reaction to the imminent danger. On a regional level relevant information has to be shared to be able to exercise precautionary measures and avoid an escalation of the 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.
Depending on the level (spatial and decision wise) the degree of information has to be adaptable. Information has to be at the right place within the right time and with the right granularity.
The use of a mix of sensor and information systems is key to adequate situation awareness on the different levels.

2.1 Situation Awareness

Situation awareness in transnational surveillance 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

978-0-7695-3551-7/09 $25.00 © 2009 IEEE
DOI 10.1109/ICONS.2009.27

IEEE computer society

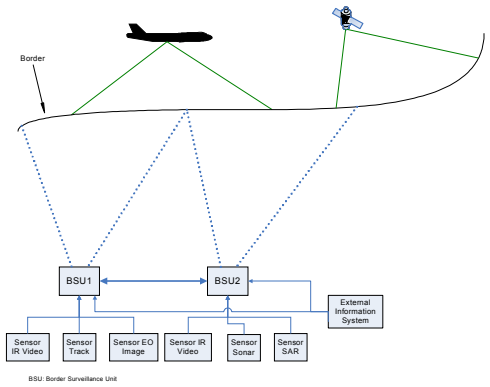

Figure 1: Border Surveillance System

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].

2.2 Integrated Surveillance Systems

Border surveillance makes use of a number of systems that detect threats and conspicuous behavior. Within an integrated surveillance system, disparate technologies that complement one another are installed, the interaction of the data output is essential.
An integrated surveillance system consists of sensors, exploitation systems (that might also be deployed as situational awareness displays) and external information systems.
In Fig. 1 a border is monitored by a range of different sensor types. Those sensors deliver data to a border surveillance unit (BSU). 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

2.2.1 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 land and sea borders it is necessary to make use of different sensor types with differing ranges and tasks [5]:

- Long-range border 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 border 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.

2.2.2 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 3.1 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 4)

2.2.3 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 (see also [6]).

3. System Overview

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 three main 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 possibly 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.

Since the information is originating from different locations arriving in different formats and the exploiting stations expect their own respective format an intelligent distributed data access is necessary

3.1 An Architecture for Transnational Surveillance Systems

As surveillance 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. 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 Fig. 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. There are military standards on relevant formats for the surveillance domain and data exchange. The architecture described here is based on these formats (resp. STANAG 4559) [7].

The standardized data is then transferred over the network to a local data server. Fig. 2 shows an example of a regional network with (via converters) connected information suppliers such as sensor stations, criminal registers, etc. 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.

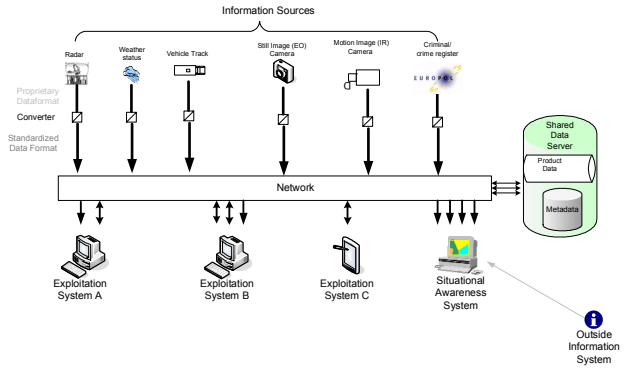

Figure 2: Information sharing within a local architecture

3.2 The SOBCAH Shared Database (SSD)

The key component of the architecture is the data server. Data in the common format is stored in the SSD and can be accessed by clients via CORBA. To retrieve a product a client (working on a system) asks for the metadata and is able to order the product if it is of interest to 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, friend/foe, weather condition, certainty/quality of the info, product type.

The user can either use an interactive query where the database is searched once or a subscription method where 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.

Considering the security of the data user roles should be supported, i.e. clients need an account specifying their access rights and statuses. For restricted information a login and user password have 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.

In a larger system, several regional servers can be used that synchronize their respective metadata content among each other in times of otherwise low network usage but with a set minimum interval. The original product data (e.g. images, movie clips of possibly high data volume) are held only on the originating server. When a system wishes 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 merely at its own data base. Only when one or more of the results are specifically requested, a connection to the originating server is initiated and the potentially large files (e.g. videos) are transported across the network.

3.3 Deployment of the Architecture in SOBCAH

Within the project SOBCAH the previously described architecture principles were used to be able to disseminate alarms, tracking information and videos from sensors to a situation awareness system. For tracks and alarms a common data format was developed. The data generated by the sensor systems were transmitted to the SOBCAH Shared database. Through subscription to the server, track and alarm data were retrieved from the situation awareness system or other system providers. Based on this information, products from other systems (e.g. videos) were queried upon or sensors were directed to an alarm location.

4. Information Fusion

The usage of multiple heterogeneous sensors increases the possibilities and functionalities of the whole system and improves the quality of the surveillance task. Especially for security applications (e. g. monitoring) state of the art multi-sensor-systems enable the surveillance of large areas with a reduced number of manpower.

Unfortunately, large sensor networks produce a huge amount of information that the security staff has to process. Therefore, automatic data processing and information fusion becomes an essential part of large distributed multi-sensor surveillance systems. Hereby integrated data processing approaches evaluate the incoming information and preselect interesting events for the human operator. Additionally automatic data fusion algorithms summarize complementary information and sort out redundant data to reduce the amount of information for the human operator. Motion detection algorithms as used in SOBCAH for example are able to reduce the workload on the security staff by generating indications of movement automatically. For the human operator it is now possible to focus only on areas of interest.

Therefore, on the one hand by fusing heterogeneous data the operator receives pre-processed information (higher quality) for optimal analysis and evaluation. On the other hand sensor fusion makes automatic control of sensors for a better data acquisition possible.

In SOBCAH, different sensors like PIR motion detection sensors, laser range finder, etc. automatically trigger Pan/Tilt cameras if a movement is detected. The cameras turn to the area of interest for further analysis (by human or automatic image processing). The advantage for the human operator is that the system provides the view of interest without interaction from the user. In doing this, the operator can manage multiple events simultaneously.

For that reason, we focus the fusion in SOBCAH on the described reduction of the cognitive workload on the operator's side.

5. The Image Processing Module

Our experimental system 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 SSD 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 SOBCAH sensor network, is able to receive alarms from all (video and non-video) sensor systems over the SSD and is additionally able to request stored imagery data for offline processing of historic video data from all video providers.

As shown in Fig. 3, 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 SOBCAH 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

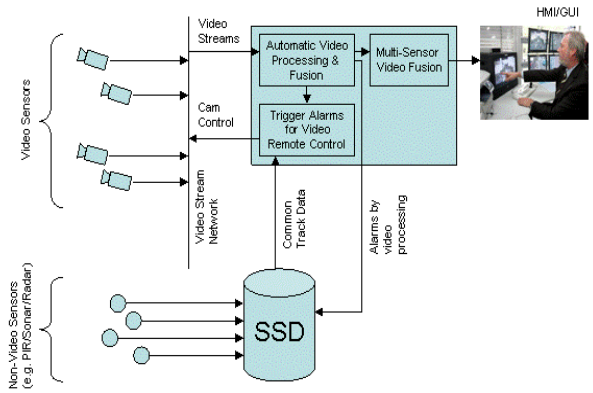

Figure 3: Internal architecture of the SOBCAH Image Processing Module.

are sent back to the sensor network (to provide results to all participants) and important information (detections / alarms etc.) is additionally archived in the SSD. 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 SSD.

The "multi-Sensor video fusion" functionality is an approach for the visual enhancement of heterogeneous video sources. In the SOBCAH system the human operator of the Image Processing Module has to overlook all video sources available in the surveillance systems. To reduce the number of displays to watch, redundant information from different video streams is fused to a common video stream (e.g. providers of EO/IR image streams).

The third mode is the so-called "video-sensor remote control". Hereby, the Image Processing Unit acts as an interface to combine information/alarm data provided by external subsystems (which use video or non-video-sensors) and active video sensors. We integrate the functionality to re-set the camera-orientation of available Pan/Tilt-cameras if an incoming alarm is in range of the field of view of an active camera. In this case the cameras slew automatically to the position of the detected event, activate a motion detection algorithm and in case of suspicious behavior start providing additional alarms to confirm previous alarms. In doing so, the Image Processing Unit provides a control assistance and automatic information fusion functionality.

6. Demo Results and Conclusion

An exemplary implementation of this architecture was realized and successfully demonstrated in the European Project SOBCAH. 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.

For a flexible data transfer it is necessary to convert proprietary data formats into a common format. As in a heterogeneous environment, many systems are supposed to share data, the format should be predefined and reusable. For adequate (motion) image processing and to reduce the workload on the operator, it is necessary to have additional collateral/meta data describing sensor settings and other collateral information. The available standards for some data types (e.g. the ASTERIX [8] standard for radar data) were either not defined for the surveillance domain and/or do not focus especially on security but on safety aspects.

As securing borders and infrastructure against terrorist attacks is a military task as well, the cooperation of military and civil surveillance and reconnaissance systems will be of greater importance in the future. For that the integration of military standards has to be considered.

7. Acknowledgments

The architecture is part of the project SOBCAH, partially funded by the European Commission under the Preparatory Action for Security Research (PASR) 2005 program. The authors acknowledge valuable help and contributions from all partners of the project.

[1] Townsend, A. Guarding Europe. In: Jaeger, T., Hoese, A., Oppermann, K. *Transatlantische Beziehungen.* Sicherheit- Wirtschaft- Oeffentlichkeit. Verlag für Sozialwissenschaften. 327- 346. 2005

[2] SOBCAH. Surveillance of Borders, Coastlines and Harbours, http://ec.europa.eu/enterprise/security/doc/project_flyers_2006/766-06_sobcah.pdf. 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] Peterson, J.K. Understanding surveillance technologies: spy devices, privacy, history & applications. Auerbach Publications. 2007

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

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

[8] 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